ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition

Kottur Harshika
PG Scholar,
Department of ECE,
Sudheer Reddy College of Engineering and Technology for Women.

P Sayanna
Associate Professor,
Department of ECE,
Sudheer Reddy College of Engineering and Technology for Women.

Abstract

In this paper, to ensure the actual presence of a real legitimate trait, in contrast to a fake self-made/self-manufactured synthetic or reproduced sample is a real problem in biometric authentication. This requires the development of new and very efficient protection technique. Here we present software based fake biometric detection technique that can be used in biometric systems for detecting various types of fakeaccess attempts. The objective of the technique is to enhance the security of biometricrecognition system, by adding liveness assessment in a user-friendly, fast, and non-intrusive manner, using image quality assessment. The proposed technique presents a very low degree of complexity that makes it suitable for all the real time applications, using generalimage quality features extracted from one image to differentiate between legal and fake samples. The experimental results, taken from publicly available databases (available online) of fingerprint, iris, and 2D face, shows that theproposed technique is highly competitive compared with other approaches and that the analysis of the general image quality of real biometric samples reveals highly valuable information that may be very efficiently used to differentiate them from fake traits.

Keywords: ***Image Quality assessment, Fake Biometric, self-manufactured synthetic, fingerprint recognition, security, attacks.***

1. Introduction

Images samples may be 2D, such as a photograph, screen display, and as well as a 3D, such as a statue. Images can be captured by electronicdevices – such as cameras, telescopes, microscopes, mirrors, lenses, etc.

Image is also can be of any 2D figure such as a graph, a map,a chart, or a painting. In this wider sense, images can also be rendered manually, such as by drawing, the art of painting, carving, rendered automatically by printing or modified using computer graphics , or developed by a combination of multiple methods.

A volatile image is one that exists only for a short period of time. This may be a reflection of an object by a mirror, a projection of a camera obscure, or a scene displayed on a cathode raytube. A fixed image, also referred as a hard copy, is one that has been recorded on a material object, like paper or textile by photography or the other digital method.

A still image is a single static image, as distinguished from a kinetic image. This sample is used in photography, television media and the computer industry to emphasize that one is not talking about movies, or in very precise or technical writing such as standards, papers etc.

A film still is a photograph captured on the set of a television or movie program during production, used for promotional purposes.

There are many different aspects of human chemistry, physiology or behavior may be used for biometric authentication. The selection of a particular method for

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

use in a specific application needs a weighting of several factors identified, such factors will be used when assessing the suitability of any trait for use in biometric authentication. Meaning of Universality is every person using a system should possess the trait. Meaning of Uniqueness is the trait should be sufficiently different and distinguished from one person to another. In addition, collected data should be in a form that permits subsequent processing and extraction of the relevant feature sets. Performance relates to the robustness, accuracy, and speed of technology used. Acceptability relates to how well individuals in the relevant population accept the technology such that they are willing to have their biometric trait captured and assessed. Circumvention relates to the ease with which a trait might be imitated using an artifact or substitute. Presently there is no single biometric system that can meet all the requirements of every possible biometric application.

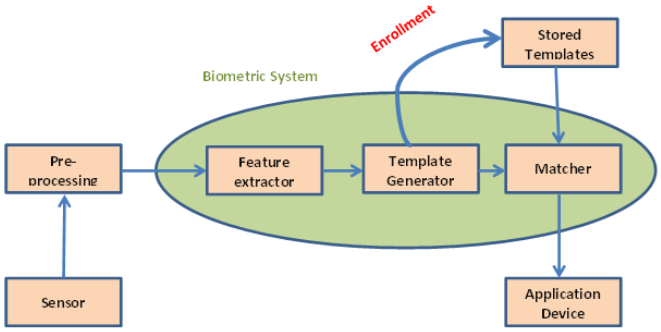

Fig 1. Basic biometric system

The block diagram shown above (Fig.1) explains the two basic modes of a biometric system.[1] First, in authentication(or verification) mode the system performs a one-to-one comparison of a captured biometric with a specific template stored in a biometric database in order to verify the individual is the person they claim to be. There are 3 steps are required in the verification of a person.[2] First, reference models for all the individual are captured and stored in the model database. Second, few samples are matched with reference models to generate the genuine and impostor scores and calculate the threshold. Third step is the testing step. This process may use auser name, identification number (e.g. PIN) or any smart card to indicate what type of template should be used for comparison.

In identification mode the biometric system performs a one to many comparisons against available database in attempt to generate the identity of an unknown person. The system will succeed in identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold.

Identification technique can be used either for “negative recognition“ or for “positive recognition” of the person, where the system establishes whether the person is who she/he denies to be. [3] The latter function can only be achieved through biometrics since other methods of personal recognition such asPINs, passwords or keys are ineffective.

The first time an individual registration into a biometric system is called enrollment. During the enrollment, biometric information of an individual is captured and stored in the database. In subsequent uses, biometric information is compared and detected with the information stored at the database. It is very important to keep storage and retrieval of such systems themselves be secure if the biometric system is to be robust. The first block (sensor) is the interface between the system and real world; it has to acquire all the necessary data. Most of the times it is an image captured system, but it can change according to the required application. The 2nd block performs all the required pre processing, it has to extract artifacts from the sensor, to enhance the input (e.g. removing noise from the background), to use some kind of normalization, etc. In the 3rd block required features are extracted. This is a main step as the correct features need to be extracted in optimal way. An image with particular properties or a vector of numbers is used to create a template.

At the time of enrollment, the template can be stored somewhere (on a computer system or on a card, within a database or both). During the matching phase, the template is passed to a matcher that will compare it with

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

other available templates, estimating the differences between them using any algorithm. The matching program will analyze the template with the input. This will then be output for any purpose or specified use (e.g. entry in a secure location).[2] We should consider Robustness, Circumvention, Acceptability, Performance, Size, Population coverage, Identity theft deterrence in selecting a particular biometric. Selection of biometric based on user requirement considers Device availability, Sensor availability, reliability, Computational time, Cost, Sensor area and power consumption.

2. IMAGE QUALITY ASSESSMENT FOR LIVENESS DETECTION

The use of image quality assessment for liveness detection is motivated by the assumption that: "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."

Expected quality differences between real and fake samples may include: degree of sharpness, color and luminance levels, local artifacts, amount of information found in both type of images (entropy), structural distortions or natural appearance. For example, iris images captured from a printed paper are more likely to be blurred or out of focus due to trembling; face images captured from a mobile device will probably be over- or under-exposed; and it is not rare that fingerprint images captured from a gummy finger present local acquisition artifacts such as spots and patches. Furthermore, in an eventual attack in which a synthetically produced image is directly injected to the communication channel before the feature extractor, this fake sample will most likely lack some of the1 properties found in natural images.

Following this "quality-difference" hypothesis, in the present research work we explore the potential of general image quality assessment as a protection method against different biometric attacks (with special attention to spoofing). As the implemented features do not evaluate any specific property of a given biometric modality or of a specific attack, they may be computed on any image. This gives the planned methodology a brand new multi-biometric dimension which isn't found in previous protection schemes.

3. THE SECURITY PROTECTION METHOD

The problem of fake biometric detection will be seen as a 2 class classification problem whenever an input biometric sample must be assigned to at least one of two classes: real or fake. The key purpose of the method is to seek out a collection of discriminant features which allows creating an appropriate classifier which provides the better probability of the image "realism" given the extracted set of features. In the present work we propose a unique parameterization using twenty five general image quality measures.

A general diagram of the protection approach proposed in this work is shown in Fig. 2. In order to keep its generality and simplicity, the system needs only one input: the biometric sample to be classified as real or fake (i.e., the same image acquired for biometric recognition purposes).

In our experiments we have used standard implementations in Matlab of the Quadratic Discriminant Analysis (QDA) and Linear Discriminant Analysis (LDA) classifiers [4].

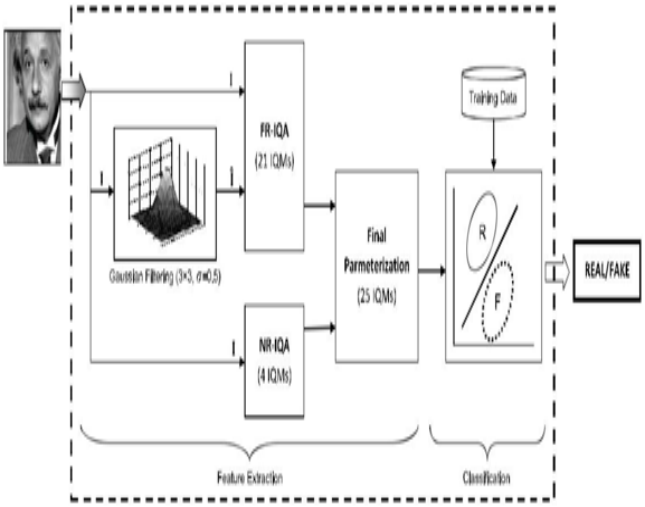

Fig.2 Biometric protection method using Image Quality Assessment (IQA)

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

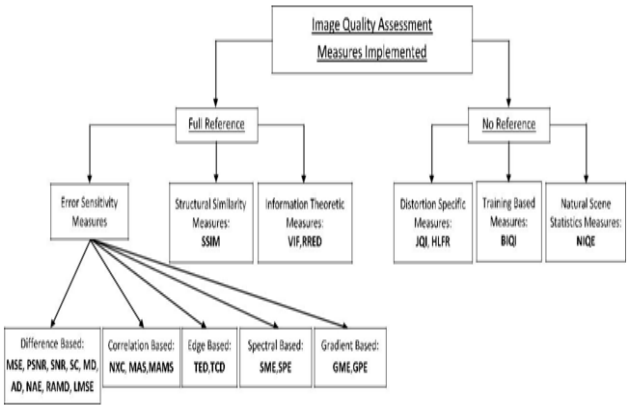

Fig.3 Classification of the image quality measures

Full-Reference IQ Measures:

Full-reference (FR) IQA methods rely on the availability of a clean undistorted reference image to estimate the quality of the test sample. In the problem of fake detection addressed in this work such a reference image is unknown, as the detection system only has access to the input sample. In order to circumvent this limitation, the same strategy already successfully used for image manipulation detection in [8] and for steganalysis in [9], is implemented here.

No-Reference IQ Measures

Unlike the objective reference IQA methods, in general the human visual system does not require of a reference sample to determine the quality level of an image. Following this same principle, automatic no-reference image quality assessment (NR-IQA) algorithms try to handle the very complex and challenging problem of assessing the visual quality of images, in the absence of a reference. NR-IQA methods are divided into one of three trends [5], 1) Distortion-specific approaches, 2) Training-based approaches and 3) Natural Scene Statistic approaches [10].

4. EXPERIMENTS AND RESULTS

The evaluation experimental protocol has been designed with 2 objectives:

- First, evaluate the "multi-biometric" dimension of the protection method.
- Second, evaluate the "multi-attack" dimension of the protection method.

With these goals in mind, and in order to achieve reproducible results, we have only used in the experimental validation publicly available databases with well described evaluation protocols. The task in all the scenarios and experiments described in the next sections is to automatically distinguish between real and fake samples.

Fig. 4. Typical real iris images (top row) and their corresponding fake samples (bottom row)

Image database of above will be available from the ATVS-FIr DB used in the iris-spoofing experiments. The database is available at http://atvs.ii. uam.es/.

A. Results: Iris

For the iris modality the protection method is tested under two different attack scenarios, namely: 1) spoofing attack, and 2) attack with synthetic samples. For each of the scenarios a specific pair of real-fake databases is used. Databases are divided into totally independent (in terms of users): train set, used to train the classifier; and test set, used to evaluate the performance of the proposed protection method. In all cases the final results are obtained applying two-fold cross validation.

Results: Iris-Spoofing

The database used in this spoofingscenario is the ATVS-FIr DB which is taken from the Biometric Recognition Group. The database consists of real and fake iris images samples (printed on paper) of 50 individual randomly selected from the Bio Sec baseline corpus [11]. The acquisition of both real and fake samples was carried out

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

using the LG Iris Access EOU3000 sensor with infrared illumination which captures bmp grey-scale images of size 640 × 480 pixels. In Fig.4 we show some typical real and fake iris images that may be found in the dataset. As mentioned above, for the experiments the database is divided into a: train set, comprising 400 real images and their corresponding fake samples of 50 eyes; and a test set with the remaining 400 real and fake samples coming from the other50eyes available in the dataset.

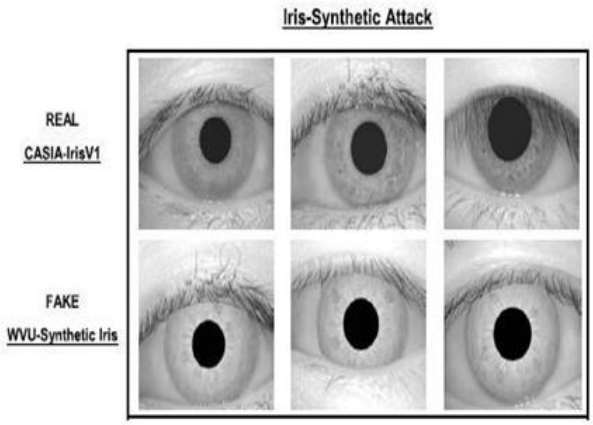

Fig. 5. Typical real iris images CASIA-IrisV1 (top row) and fake samples

Above sample images (in Fig.5) are taken from WVU-Synthetic Iris DB (bottom row), used for the iris-synthetic experiments, these databases are available at http://biometrics.idealtest.org and http://www.citer.wvu.edu/.

The Liveness detection results achieved by the proposed approach under this scenario is able to correctly classify over 97% of the samples. This was measured on a standard 64-bit Windows7-PC with a 3.4 GHz processor and 16 GB RAM memory, running MATLAB. This method not only outperforms the previously available techniques, but also, as it does not require any iris detection or segmentation, the processing time is around 10 times faster.

Results: Iris-Synthetic: In this scenario attacks areperformed using synthetically generated iris samples which are used as input in the communication channel between the feature extraction module and the sensor (Fig. 1). The real and fake databases used in this method are:

- **Real database:** CASIA-IrisV1. This dataset is publiclyavailable through the Biometric Ideal Test (BIT) platform of the Chinese Academy of Sciences Institute of Automation (CASIA). It contains 7 grey-scale 320×280 images of 108 eyes captured in two separate sessions with a self-developed CASIA close-up camera and are stored in bmp format.
- **Synthetic database:** WVU-Synthetic Iris DB. This samples ofdatabase that contains only fully synthetic data, so it is not subjected to any legal constraints and is publicly available (online) through the CITeR research center.

B. Results: Fingerprints

For the fingerprint modality, the performance of the planned protection technique is evaluated using the LivDet 2009 DB [6] comprising over 18000 real and fake samples. As in the iris an experiment, the database is divided into a: train set, used to train the classifier; and test set, used to evaluate the performance of the protection method. In order to generate totally unbiased results, there is no overlap between both sets (i.e., samples corresponding to each user are just included in the train or the test set). The same QDA classifier already used in the iris related experiments is used here.

Results: Fingerprints-Spoofing LivDet:

The LivDet2009 DB [6] comprises three datasets of real and fake fingerprints captured each of them with a different flat optical sensor: 1) Biometrika FX2000 (569 dpi), 2) Cross Match Verifier 300CL (500 dpi), and 3) Identix DFR2100 (686dpi). The database contains over 18,000 samples coming from more than 100 different fingers. Some typical examples of the images that can be found in this database are shown in Fig.6, where the material used for the generation of the fake fingers is specified.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

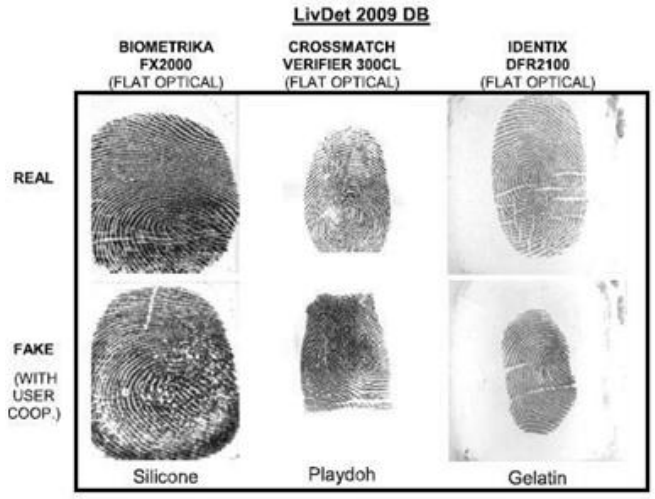

Fig.6. Typical examples of real and fake fingerprint images

These images can be found in the public LivDet09 database used in the fingerprint anti-spoofing experiments. The database is available at http://prag.diee.unica.it/Liv Det09/.

Experimental results show that our method gives better performance than contestants in LivDet 2009 in two of the datasets (Biometrika and Identix). The classification error rates of our approach are also lower than those reported in for the different liveness detection solutions tested.

C. Results: 2D Face

The performance of the IQA based protection technique has also been used to assess on a face spoofing database: the REPLAY-ATTACK DB, which is accessible publicly from the IDIAP Research Institute. The database contains short videos of both spoofing attack and real-access attempts of 50 different subjects, acquired with a 320 × 240 resolution web-cam of a 13-inch.

In addition, access attempts in the three attack subsets (print, mobile and high def) were recorded in two different modes depending on the strategy followed to hold the attack replay device (paper, tablet or mobile phone): 1) hand-based and 2) fixed-support. Such a variety of fake and real acquisition scenarios and conditions makes the REPLAY-ATTACK DB a unique benchmark for testing anti-spoofing techniques for face-based systems. As a consequence, the print subset was selected as the evaluation dataset in the Competition on Counter Measures to 2D Facial Spoofing Attacks [7]. Some typical images (frames extracted from the videos) from real and fake (print, mobile and high def) access attempts that may be found in the REPLAY-ATTACK DB are shown in Fig.7.

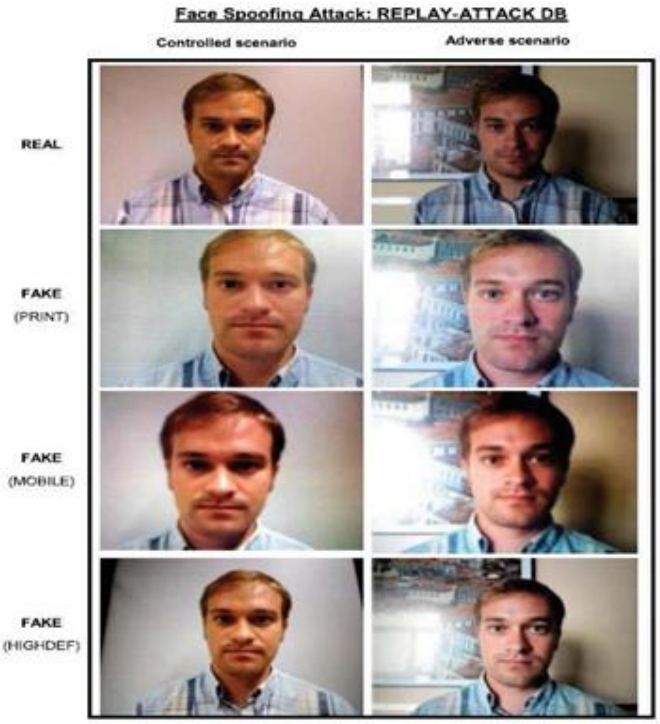

Fig. 7. Typical examples of fake and real (print, mobile and high def) face

Images shown (in Fig.7) that can be found in the public REPLAY-ATTACK DB used in the face anti-spoofing experiments. Images were extracted from videos acquired in the two considered scenarios: controlled and adverse. The database is available at https://www.idiap.ch/ dataset/replayattack.

Results obtained by the different participants in the competition compared to the performance of our method without doing the cropping and normalization of the videos. We can observe that, even though many of the

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

contestants were using a sequence of frames to classify each video (with the complexity and speed decrease that this entails), our proposed IQA-based method performs similarly to the top ranked systems.

5. CONCLUSION

Image quality assessment (IQA) for Liveness detection method is used to detect the fake biometrics. Due to Image quality measurements it is easy to find out fake and real users because fake samples/identities always have some different features than original. It always contain different color and luminance levels, general artifacts, quantity of sharpness, and quantity of information, found in both type of images, structural distortions or natural appearance. Multi-Biometric system is challenging system. It is more secure than uni-biometric system.

In this paper studied about the three biometric systems that are iris recognition, fingerprint recognition, face recognition, and the attack on these three biometric systems. In general, Multi biometric system is used for various applications. And in future for making this system more secures adding the one more biometric system into this system and trying to improve the system. In this context, it is reasonable to assume that the image quality properties of fraudulent attacks and real accesses will be different. Following this quality-difference, in the present paper we have explored the potential of general image quality assessment as a protection tool against different biometric attacks. For this purpose we have considered a feature space of 25 complementary image quality measures which we have combined with simple classifiers to detect real and fake access attempts.

The novel protection methodology has been tested on 3 largely deployed biometric techniques like the iris, the fingerprint and 2D face, using publicly accessible databases with well defined associated protocols. This way, the results are reproducible and may be fairly compared with other future analogue solutions. The present work also opens new possibilities for future work, including: 1) extension of the considered feature set with new image quality measures; 2) further evaluation on other image-based modalities; 3) use of video quality measures for video attacks; 4) analysis of the features individual relevance.

REFERENCES

[1] Jain, Anil K.; Ross, Arun (2008). "Introduction to Biometrics". In Jain, AK; Flynn; Ross, A. Handbook of Biometrics. Springer. pp. 1–22. ISBN 978-0-387-71040-2.

[2] Sahoo, SoyujKumar; MahadevaPrasanna, SR, Choubisa, Tarun; MahadevaPrasanna, SR (1 January 2012). "Multimodal Biometric Person Authentication : A Review". IETE Technical Review 29 (1): 54. doi:10.4103/0256-4602.93139 (inactive 2015-01-04). Retrieved 23 February 2012.

[3] S. Prabhakar, S. Pankanti, and A. K. Jain, ―Biometric recognition: Security and privacy concerns,‖ IEEE Security Privacy, vol. 1, no. 2, pp. 33–42, Mar./Apr. 2003.

[4] T. Hastie, R. Tibshirani, and J. Friedman., The Elements of Statistical Learning. New York, NY, USA: Springer-Verlag, 2001.

[5] 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.

[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] M. M. Chakka, A. Anjos, S. Marcel, R. Tronci, B. Muntoni, G. Fadda, et al., "Competition on countermeasures to 2D facial spoofing attacks," in Proc. IEEE IJCB, Oct. 2011, pp. 1–6.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[8] S. Bayram, I. Avcibas, B. Sankur, and N. Memon, "Image manipulation detection," J. Electron.Imag., vol. 15, no. 4, pp. 041102-1–041102-17, 2006.

[9] I. Avcibas, N. Memon, and B. Sankur, "Steganalysis using image quality metrics," IEEE Trans. Image Process., vol. 12, no. 2, pp. 221–229, Feb. 2003.

[10] 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.

[11] J. Fierrez, J. Ortega-Garcia, D. Torre-Toledano, and J. Gonzalez-Rodriguez, "BioSec baseline corpus: A multimodal biometric database," Pattern Recognit., vol. 40, no. 4, pp. 1389–1392, 2007.