Biometric Vulnerability Analysis Based On Image Quality And Distortion : Application To Iris, Fingerprint And Face Recognition

Abstract

This paper presents a novel software-based fake detection method that can be used in multiple biometric systems to detect different types of fraudulent access attempts. The objective of the proposed system is to enhance the security of biometric recognition frameworks, by adding liveness assessment in a fast, user-friendly, and non-intrusive manner, through the use of image quality assessment. To ensure the actual presence of a real legitimate trait to a fake self-manufactured synthetic or reconstructed sample is a significant problem in biometric authentication, which requires the development of new and efficient protection measures. The proposed approach presents a new method for detecting vulnerabilities of biometric systems against different types of attacks. For this purpose the proposed system consider 25 image quality measures which combined with simple classifiers to detect real and fake access attempts which makes it suitable for real-time applications. The experimental results was done based on the images in the dataset and it is taken as with high and low quality images of both original images and fake images. The image quality is estimated by 25 quality assessment features. The analysis of the general image quality of real biometric samples reveals highly valuable information that may be very efficiently used to discriminate them from fake traits.
1. Introduction

Identity management using biometrics becomes reality. Then the increase in the interest of security evaluation in biometric system is also increasing day-by-day. For this, some laptops such as Lenovo, Toshiba etc. provide built in authentication like fingerprint authentication, Iris recognition, etc. But these systems are vulnerable to different attacks like spoofing attacks. One of the important characteristics in biometric system is the fake detection and several biometric characteristics are used in various applications. Each biometric has its strength and weaknesses, and the choice typically depends on the application. No single biometric can effectively meet their requirements of all applications, none is optimal.

Among the different threats analysed, understand that the spoofing attacks have motivated the biometric community to study the vulnerabilities against the type of fraudulent actions in modalities such as the iris, the fingerprint, the face, the signature, or even the gait and multimodal approaches. In these attacks, the intruder uses some type of synthetically produced artifact (e.g., Gummy finger, printed iris image or face mask), or tries to mimic the behavior of the genuine user (e.g., gait, signature), to fraudulently access the biometric system. As these types of attacks are performed in the usual digital protection mechanisms such as encryption, digital signature or watermarking are not effective. Besides other anti-spoofing approaches the use of multi-biometrics or challenge-response methods, special attention has been paid by researchers and industry to the liveness detection techniques, which use different physiological properties to distinguish between real and fake traits. Liveness assessment methods represent a challenging engineering problem as they have to satisfy certain demanding requirements and it is discussed in the later section.

1.1 Liveness Detection

Liveness detection methods are mainly classified into two: both hardware-based and software-based techniques. A hardware based technique adds some specific device to the sensor in order to detect particular properties of a living trait (e.g., fingerprint sweat, blood pressure, or specific reflection properties of the eye). In software-based techniques, the fake trait is detected once the sample has been acquired with a standard sensor. Therefore, hardware-based strategies typically present some sort of higher detection rate, the actual software-based methods include the main advantage of currently being less costly, as well as less intrusive for the user. In general, a variety of both kind of anti-spoofing schemes for improving the security level of biometric systems [3].

2. Existing System

There are two ways to evaluate the image quality. The most reliable way of assessing the quality of a image is the subjective approach because human beings are the ultimate receivers in most applications. But this approach presents some disadvantages. That is why, in the last few years, new objective image and image quality metrics have been proposed. The objective quality metrics can be classified in three categories. An important criterion used in the classification of image quality measures is the type of information needed to evaluate the distortion in degraded images. Measures that require both the original image and the distorted image are called full reference or nonblind methods. Measures that do not require the original image are called no-reference or blind methods. Measures that require both the distorted image and partial information about the original image are called reduced reference methods.

The evaluation of quality may be divided into two classes, subjective and objective methods.
3.1 Subjective Methods

Intuitively, one can say that the best judge of quality is the human himself. That is why subjective methods are said to be the most precise measures of perceptual quality and to date subjective experiments are the only widely recognized method of judging perceived quality. In these experiments humans are involved who have to vote for the quality of a medium in a controlled test environment. This can be done by simply providing a distorted medium of which the quality has to be evaluated by the subject. Another way is to additionally provide a reference medium which the subject can use to determine the relative quality of the distorted medium.

3.2 Objective Methods

This is another quantitative approach where intensity of two images, reference and distorted type are used to calculate a number which indicate the image quality. The objective Image Quality Assessment (IQA) can be classified into full-reference, reduced-reference and no-reference. IQA based on the availability of the reference image. The goal of objective image quality assessment models is to automatically estimate the perceptual quality of images, in a way correlated with the human appreciation. The three models of objective method on the basis of reference images are categorized as given below.

3.2.1 No Reference (NR) Models

It is also called blind methods, in which the QA algorithm has access only to the distorted signal and must estimate the quality of the signal without any knowledge of the 'perfect version'. NR methods can be used in any application where a quality measurement is required because they do not require any reference information.

3.2.2 Reduced Reference (RR) Models

In this partial information regarding the 'perfect version' is available. A side-channel exists through which some information regarding the reference can make available to the QA algorithm. RR QA algorithms use this partial reference information to judge the quality of the distorted signal of the scene.

3.2.3 Full Reference (FR) Model

In this method quality assessment algorithm have access to a 'perfect version' of the image or video against which it can compare a 'distorted version'. The 'perfect version' usually comes from a high-quality acquisition device, before it is distorted by compression artifacts and transmission errors. There are in general two classes for objective quality assessment approach, statistical error metrics and human visual system based metrics.

4. Proposed System

The proposed system is a fake biometric detection problem. It can be seen as a two-class classification problem where an input biometric sample has to be assigned to one of two classes: real or fake. The key point of the process is to find a set of discriminant features which permits to build an appropriate classifier and features are extracted from set of given features. The present work proposes a novel parameterization using 25 general image quality measures.
A general diagram of the protection approach proposed in this work is shown in Fig. 1. 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). Furthermore, as the method operates on the whole image without searching for any trait-specific properties. Also, it does not require any pre-processing steps (e.g., fingerprint segmentation, iris detection or face extraction) prior to the computation of the IQ features. These characteristic minimizes its overall computational load. Once the feature vector has been generated the sample is classified as real (generated by a genuine trait) or fake (synthetically produced), using some simple classifiers. In particular, the proposed system conducted experiments in SVM classifier.

Figure 1: General diagram of the biometric protection method based on Image Quality Assessment (IQA) proposed in the present work.

Figure 2: Classification of the 25 image quality measures implemented in the work.
4.1 Full-Reference IQ Measures

Full-reference (FR) IQA methods were based on the availability of an 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 and for steganalysis, is implemented here.

As shown in Fig. 1, the input gray-scale image $I$ (of size $N \times M$) is filtered with a median filter in order to generate a smoothed version $I'$. Then, the quality between both images ($I$ and $I'$) is computed according to the corresponding full-reference IQA metric.

4.1.1 FR-IQMs: Error Sensitivity Measure

Traditional perceptual image quality assessment approaches are based on measuring the errors (i.e., signal differences) between the distorted and the reference images, and attempt to quantify these errors in a way that simulates human visual error sensitivity features.

(a) Wavelet Based Measures

The wavelet-Fourier analysis (WFA) for the characterization used as a mathematical model to analyse image features. In wavelet transform (WT), usually the image is represented in terms of the frequency of content of local regions over a range of scales. This representation provides a framework for the analysis of image features, which are independent in size and can often be characterized by their frequency domain properties. In the current system, discrete wavelet transforms (DWT) using a fourth-order. Also, DWT is a multi-scale analysis method, in which analysis can be performed on various scales. Each level of the transformation provides an analysis of the source image at a different resolution, resulting in its independent approximation and detailed coefficients.

In the WFA, the fast Fourier transform (FFT) is the detailed coefficients. The resultant Fourier amplitudes are combined with the normalized approximation coefficients of the DWT to create a set of features. Though providing valuable insight into the analysis of images using mathematical generalization. DWT features need to be extracted to represent an image that is as discriminative as possible in the transform domain. The DWT captures both the spatial and frequency information of a signal. The proposed system uses two well-known wavelet filters, the daubechies (db3), the symlets (sym3), filters. Then symlets wavelet is used to extract features and analysis discontinuities and abrupt changes contained in the signals. Then the filters calculate the averages of the detailed horizontal and vertical coefficients and wavelet energy signature from the detailed vertical coefficients.

Here also include some other features to find the error sensitivity measures such as: Structural Content (SC), Maximum Difference (MD), Average Difference (AD), Normalized Absolute Error (NAE), R-Averaged Maximum Difference (RAMD) and Laplacian Mean Squared Error (LMSE). In the RAMD, $max_r$ is defined as the $r$-highest pixel difference between two images. For the present implementation, $R = 10$. In the LMSE,

$$h(i, j) = I_{i+1, j} + I_{i-1, j} + I_{i, j+1} + I_{i, j-1} - 4I_{i, j}$$

(b) Distortion Based Measures

These methods were designed primarily to counter printed photo attacks, displayed photo attacks, or replayed attack. Suppose when an image is recaptured, images tend to show a different color distribution compared to colors in the genuine images. This is caused by the imperfect color
reproduction property of printing and display media. This chromatic degradation was explored in for detecting recaptured images, but its effectiveness in spoof face detection is unknown. Since the absolute color distribution is dependent on illumination and camera variations, then proposed system to create a devise invariant feature to detect abnormal chromaticity in spoof faces. For this, first convert the normalized facial image from the RGB space into the HSV (Hue, Saturation, and Value) space and then compute the mean, deviation, of each channel as a chromatic feature. Here, it will be represented as $HMEAN$, $VMEAN$, $SST$. Since these two features are equivalent to the two statistical moments in each channel, they are also referred to as chromatic moment features.

(c) Edge-Based Measures.

Edges and other two-dimensional features such as corners play a key role in the human visual system and in many computer vision algorithms including quality assessment applications. Since the structural distortion of an image is fully linked with its edge degradation, here we have considered two edge-related quality measures: Total Edge Difference (TED) and Total Corner Difference (TCD). In order to implement both features, which are computed according to the corresponding expressions: 

(i) the Sobel operator to build the binary edge maps $IE$ and $IE^\ast$; 
(ii) the Harris corner detector to compute the number of corners $NCR$ and $NCR^\ast$ found in $I$ and $I^\ast$.

(d) Spectral Distance Measures.

The Fourier transform is a no other traditional image processing tool, which has been applied to the field of image quality assessment. In this work, consider IQ as spectral-related features: the Spectral Magnitude Error (SME) and the Spectral Phase Error (SPE), (where $F$ and $F^\ast$ are the respective Fourier transforms of $I$ and $I^\ast$), and arg($F$) denotes phase.

(e) Gradient-Based Measures.

Gradient measures can convey important visual information which can be of great use for quality assessment. Many of the distortions that can affect an image are reflected by a change in its gradient. Therefore, using such information, structural and contrast changes can be effectively captured. Two simple gradient-based features are included in the current biometric protection system: Gradient Magnitude Error (GME) and Gradient Phase Error (GPE), (where $G$ and $G^\ast$ are the gradient maps of $I$ and $I^\ast$ defined as $G = G_x + iG_y$, where $G_x$ and $G_y$ are the gradients in the $x$ and $y$ directions).

4.1.2 FR-IQMs: Structural Similarity Measures

There are several problems based on an error sensitivity measure which are evidenced by their mismatch (in many cases) with subjective human-based quality scoring systems. In this scenario, a recent new paradigm for image quality assessment based on structural similarity was proposed following the hypothesis that the human visual system is highly adapted for extracting structural information from the viewing field. Therefore, distortions in an image that come from variations in lighting, such as contrast or brightness changes (non-structural distortions), should be treated differently from structural ones.

4.1.3 FR-IQMs: Information Theoretic Measures

The quality assessment problem may also be understood, from an information theory perspective, as an information-fidelity problem (rather than a signal-fidelity problem). The core idea behind these approaches is that an image source communicates to a receiver through a channel that limits the
amount of information that could flow through it, thereby introducing distortions. The goal is to relate the visual quality of the test image to the amount of information shared between the test and the reference signals, or more precisely Under this general framework, image quality measures based on information fidelity exploit the (in some cases imprecise) relationship between statistical image information and visual quality. In the present work, consider two of these information theoretic features: the Visual Information Fidelity (VIF) and the Reduced Reference Entropic Difference index (RRED). Both metrics are based on the information theoretic perspective of IQA but each of them takes either a global or a local approximation to the problem, as is explained below.

The VIF metric measures the quality fidelity as the ratio between the total information (measured in terms of entropy) ideally extracted by the brain from the whole distorted image and the total information conveyed within the complete reference image. This metric relies on the assumption that natural images of perfect quality, in the absence of any distortions, pass through the human visual system (HVS) of an observer before entering the brain, which extracts cognitive information from it. For distorted images, it is hypothesized that the reference signal has passed through another distortion channel before entering the HVS. The VIF measure is derived from the ratio of two mutual information quantities: the mutual information between the input and the output of the HVS channel when no distortion channel is present (i.e., reference image information) and the mutual information between the input of the distortion channel and the output of the HVS channel to the test image. Therefore, to compute the VIF metric, the entire reference image is required as quality is assessed on a global basis. the mutual information between them.

4.2 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. Presently, NR-IQA methods generally estimate the quality of the test image according to some pre-trained statistical models. Depending on the images used to train this model and on the a priori knowledge required, the methods are coarsely divided into one of three trends:

4.2.1 Distortion-Specific Approaches
These techniques rely on previously acquired knowledge about the type of visual quality loss caused by a specific distortion. The final quality measure is computed according to a model trained on clean images and on images affected by this particular distortion. Two of these measures have been included in the biometric protection method proposed in the present work. The JPEG Quality Index (JQI), which evaluates the quality in images affected by the usual block artifacts found in many compression algorithms running at low bit rates such as the JPEG. The High-Low Frequency Index (HLFI), which was inspired by previous work which considered local gradients as a blind metric to detect blur and noise. Similarly, the HLFI feature is sensitive to the sharpness of the image by computing the difference between the power in the lower and upper frequencies of the Fourier Spectrum.

4.2.2 Training-Based Approaches
Similarly to the previous class of NR-IQA methods, in this type of techniques a model is trained using clean and distorted images. Then, the quality score is computed based on a number of features
extracted from the test image and related to the general model. However, unlike the former approaches, these metrics intend to provide a general quality score not related to a specific distortion. To this end, the statistical model is trained with images affected by different types of distortions. This is the case of the Blind Image Quality Index (BIQI) described in, which is part of the 25 feature set used in the present work. The BIQI follows a two-stage framework in which the individual measures of different distortion-specific experts are combined to generate one global quality score.

4.2.3 Natural Scene Statistic Approaches
These blind IQA techniques use a priori knowledge taken from natural scene distortion-free images to train the initial model (i.e., no distorted images are used). The rationale behind this trend relies on the hypothesis that undistorted images of the natural world present certain regular properties which fall within a certain subspace of all possible images. If quantified appropriately, deviations from the regularity of natural statistics can help to evaluate the perceptual quality of an image. This approach is followed by the Natural Image Quality Evaluator (NIQE) used in the present work. The NIQE is a completely blind image quality analysis based on the construction of a quality aware collection of statistical features (derived from a corpus of natural undistorted images) related to a natural scene statistical model.

4.3 Classification
In the existing system, the classification was done by LDA. But it lacks accuracy in some cases. Therefore, to improve the accuracy the proposed system using another classifier named, Support Vector Machine (SVM) to classify the images.

5. Experiments And Results
The experiment is done based on the images in the dataset. The dataset contains the 18 images and it is taken as with high and low quality images of both original images and also fake images. The image quality is estimated by 25 quality assessment features. The experiments have been designed with two main objectives: First, evaluate the —multi-biometric —protection. That is, its ability to achieve a good performance, compared to other trait-specific approaches, under different biometric modalities. For this purpose three of the most image-based biometric modalities have been considered in the experiments: iris, fingerprints and 2D face. Second, evaluate the —multi-attack‖ protection. That is, its ability to detect not only spoofing attacks (such as other liveness detection specific approaches) but also fraudulent access attempts carried out with synthetic or reconstructed samples. In order to achieve these objectives the performance of the proposed system need to change. So we change some features in the existing system so as to improve the performance of the current system. Then the important changes made-up in the proposed system are :i) initially, replace the Gaussian filter with median filter so as to improve the quality, then ii) remove pixel wise difference and co-relation in the previous system and add wavelet features and distortion analysis without the loss of quality because both pixel-wise and co-relation have poor results compared to subjective test results. Then, finally change the classifier for better prediction, so here we use SVM classifier instead of LDA.

The classification performance using support vector machine is promising. It yields detection rates of 86% on a new benchmark dataset consisting of 60 images, and 83% on 50 images that were collected from the Internet. The experiments show that there is a great difference in the LDA (Linear
Discriminant Analysis) estimates of the images compared to SVM (Support Vector Machine) when they are fake. This is because, while editing the image, the manipulator performs different functions to make the image look more like the original one. This can alter the edge features of the image. Therefore, in all cases, results are reported in terms of: the false genuine rate (FGR), which accounts for the number of false samples that were classified as real; and the false fake rate (FFR), which gives the probability of an image coming from a genuine sample being considered as

The half total error rate (HTER) is computed as,

\[
\text{HTER} = \frac{\text{FGR} + \text{FFR}}{2}
\]

<table>
<thead>
<tr>
<th></th>
<th>FAR</th>
<th>FRR</th>
<th>HTER</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDA</td>
<td>0.283</td>
<td>0.66</td>
<td>0.174</td>
</tr>
<tr>
<td>SVM</td>
<td>0.1</td>
<td>0.016</td>
<td>0.058</td>
</tr>
</tbody>
</table>

Figure 3: FAR for proposed system and existing system LDA

Figure 4: FRR for proposed system and existing system LDA
From fig 3 and 4 it is clear that SVM has a lower rate of FAR and FRR. Hence we can say that the proposed method much better than the existing system.

6. Conclusion

In this work, present a new method for detecting vulnerabilities of biometric systems against different types of attacks. For this purpose the proposed system considered a feature space of 25 image quality measures which combined with simple classifiers to detect real and fake access attempts. Moreover the novel protection method has been evaluated on three largely deployed biometric modalities such as the iris, the fingerprint and 2D face, using publicly available databases with well-defined associated protocols.

Several conclusions may be extracted from the proposed method such as it is able to consistently perform at a high level for different biometric traits (multi-biometric), to adapt to different types of attacks providing for all of them a high level of protection(multi-attack), to generalize well to different databases, acquisition conditions and attack scenarios; also the error rates achieved by the proposed protection scheme are in many cases lower than those reported by other trait-specific state-of-the-art anti-spoofing systems which have been tested in the framework of different independent competitions; and in addition to its very competitive performance, and to its multi-biometric and multi-attack characteristics.

8. References


[4] Di Wen, Member, IEEE, Hu Han, Member, IEEE, and Anil K. Jain, Life Fellow, IEEE “Face Spoof Detection With Image Distortion Analysis”


