Detecting the Originality of Biometric Details Using Image Quality Assessment

S.SWARTHY[1], A.AMALI ANGEL PUNITHA[2]
Scholar[1], Assistant Professor[2],
Department of Computer Science and Engineering[1,2]
Ultra College of Engineering and Technology for Women, Madurai, India

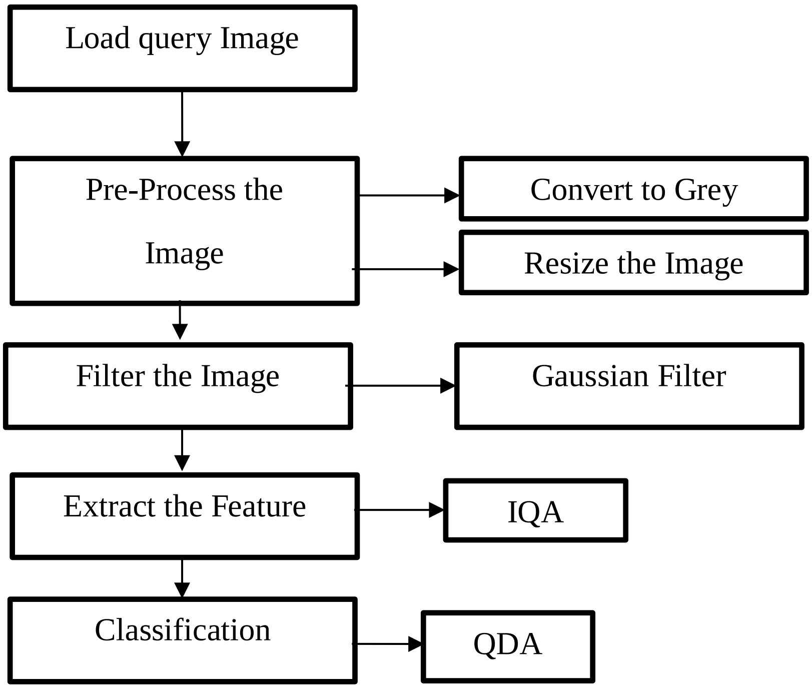
Abstract—Image and biometric details of man is designed artificial by using some software it is called spoofing. Spoofing is one of the most problems in developing security world. In spoofing, process is done by so many software and skilled person. In future, world security is the important one for every person. The biometric data will help in all fields for identification process. So it is needed to develop new method to find and rectify the spoofing data's. 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. The proposed approach presents a very low degree of complexity, which makes it suitable for real-time applications, using general image quality features extracted from one image (i.e., the same acquired for authentication purposes) to distinguish between legitimate and impostor samples.

I. INTRODUCTION

Image processing is any form of signal processing for which the input is an image, such as a photograph or video frame the output of image processing may be either an image or a set of characteristics or parameters related to the image. Most image processing techniques involve treating the image as a two-dimensional signal and applying standard signal processing techniques to it. Image processing usually refers to digital image processing, but optical and analog image processing also are possible. This article is about general techniques that apply to all of them. The acquisition of images (producing the input image in the first place) is referred to as imaging. Closely related to image processing are computer graphics and computer vision. In computer graphics, images are manually made from physical models of objects, environments, and lighting, instead of being acquired (via imaging devices such as cameras) from natural scenes, as in most animated movies. Computer vision, on the other hand, is often considered high-level image processing out of which a machine/computer/software intends to decipher the physical contents of an image or a sequence of images (e.g., videos or 3D full-body magnetic resonance scans).In modern sciences and technologies, images also gain much broader scopes due to the ever growing importance of scientific visualization in biometrics. Biometric refers to metrics related to human characteristics and traits. Biometric authentication (realistic authentication) is used in computer science as a form of identification and access control. It is also used to identify individuals in groups that are under surveillance. Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals .Biometric identifiers are categorized as physiological versus behavioural characteristics. Physiological characteristics are related to the shape of the body. Examples include, but are not limited to finger print, palm veins, Face recognition, Palm Print, Hand Geometry, iris recognition retina. Behavioural characteristics are related to the pattern of behaviour of a person.

Besides other anti-spoofing approaches such as 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. Non-invasive, the technique should in no case be harmful for the individual or require an excessive contact with the user. They are user friendly, people should not be reluctant to use it; fast, results have to be produced in a very reduced interval as the user cannot be asked to interact with the sensor for a long period of time; low cost, a wide use cannot be expected if the cost is excessively high performance, in addition to having a good fake detection rate, the protection scheme should not degrade the recognition performance (i.e., false rejection) of the biometric system



A novel software-based multi-biometric and multi-attack protection method which targets to overcome part of these limitations through the use of image quality assessment (IQA). It is not only capable of operating with a very good performance under different biometric systems (multi-biometric) and for diverse spoofing scenarios, but it also provides a very good level of protection against certain non-spoofing attacks (multi-attack) software-based techniques are in general less expensive (as no extra device is needed), and less intrusive since their implementation is transparent to the user. Furthermore, as they operate directly on the acquired sample (and not on the biometric trait itself), software-based techniques may be embedded in the feature extractor module, which makes them potentially capable of detecting other types of illegal break-in attempts not necessarily classified as spoofing attacks. For instance, software based methods protects the system against the injection of reconstructed or synthetic samples into the communication channel between the sensor and the feature extractor using Image Quality Measures.

II IMAGE QUALITY MEASURES

A.Error Sensitivity Measures:

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. Although their efficiency as signal fidelity measures is somewhat controversial, up to date, these are probably the most widely used methods for IQA as they conveniently make use of many known psychophysical features of the human visual system , they are easy to calculate and usually have very low computational complexity. The features have been classified here into five different categories according to the image property measured.

B. Pixel Difference measures:

These features compute the distortion between two images on the basis of their pixel wise differences. Here it include: Mean Squared Error (**MSE**), Peak Signal to Noise Ratio (**PSNR**), Signal to Noise Ratio (**SNR**), 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 implementation, *R* = 10.In the LMSE *h (***I***i, j)*= **I***i*+1*, j* +**I***i*−1*, j* + **I***i, j*+1 + **I***i, j*−1 − 4**I***i, j* .

C. Correlation-based measures:

The similarity between two digital images can also be quantified in terms of the correlation function. A variant of correlation based measures can be obtained by considering the statistics of the angles between the pixel vectors of the original and distorted images. These features include Normalized Cross Correlation (**NXC**), Mean Angle Similarity (**MAS**) and Mean Angle- Magnitude Similarity (**MAMS**). In the MAS and MAMS αi, j denotes the angle between two vectors, defined as, *αi*, j =2π arcos _**I***i, j* ,ˆ**I***i, j* _||**I***i, j* ||·||ˆ**I***i, j* ||, where _**I***i, j* ,ˆ**I***i, j* _ denotes the scalar product. As it is dealing with positive matrices **I** and ˆ**I**, it is constrained to the first quadrant of the Cartesian space so that the maximum difference attained will be π/2, therefore the coefficient 2*/π* is included for normalization.

D. Edge-based measures:

Edges and other two-dimensional features such as corners, are some of the most informative parts of an image, which 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 tightly linked with its edge degradation, here it have considered two edge-related quality measures: Total Edge Difference (TED) and Total Corner Difference (TCD). In order to implement both features, the Sobel operator to build the binary edge maps IE and ˆIE, the Harris corner detector to compute the number of corners Ncr and ˆNcr found in I and ˆI.

E. Spectral distance measures:

The Fourier transform is another traditional image processing tool which has been applied to the field of image quality assessment .It is considered as IQ spectral-related features: the Spectral Magnitude Error (**SME**) and the Spectral Phase Error (**SPE**), (where **F** and ˆ**F** are the respective Fourier transforms of **I** and ˆ**I**), and arg *(***F***)* denotes phase.

F. Structural Similarity Measures:

Although being very convenient and widely used, the afore mentioned image quality metrics based on error sensitivity present several problems 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 one. Among these recent objective perceptual measures, the Structural Similarity Index Measure (**SSIM**), has the simplest formulation and has gained wide spread popularity in a broad range of practical applications. In view of its very attractive properties, the SSIM has been included in the feature parameterization.

III BENIFITS

- It has very low complexity,
- It is very well suited to operate on real scenarios.
- It does not deploy any trait-specific property .
- General image quality measures are fast to compute.
- Very simple classifiers are used.
- The performance speed is high.

These are the steps involved in detecting the fake traits.

A.PREPROCESSING

The input image is collected. The spoofing image is created by photo editing software. That input images are loaded and shown in the GUI. The pre-processing step is important in image processing. In this process the noise is removed and the image is resized and some process is done for output.

*Convert to Grey***:**

In pre-process step the first step is converting the input image to grey image. In image processing all the images are in grey scale. In the grey scale image the RGB is removed .Because some process is done in without RGB image. So the RGB is removed from the given input image.

Resize the image:

It is the second step in pre-processing. The image size is modified as the input images may be of different size. It affects the time consuming and output quality. So the image size is changed to our comfortable range.

B.FILTER

In Filter process Gaussian filter is applied to input image. Gaussian filter is often used to remove the noise from the image. Wiener function to remove the noise from the input image. Gaussian filter is windowed filter of linear class, by its nature is weighted mean. weights in the filter calculated according to Gaussian distribution.

The Gaussian Smoothing Operator performs a weighted average of surrounding pixels based on the Gaussian distribution. It is used to remove Gaussian noise and is a realistic model of defocused lens. Sigma defines the amount of blurring. The radius slider is used to control how large the template is. Large values for sigma will only give large blurring for larger template sizes. Noise can be added using the sliders.

Gaussian filtering g is used to blur images and remove noise and detail. In one dimension, the Gaussian function is:

$$G(x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{x^2}{2\sigma^2}}$$

Where σ is the standard deviation of the distribution. The distribution is assumed to have a mean of 0. Shown graphically, we see the familiar bell shaped Gaussian distribution.

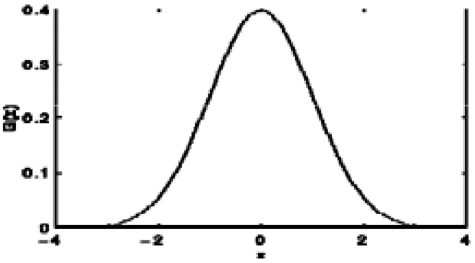


Fig. Gaussian Distribution

The Gaussian function is used in numerous research areas:
– It defines a probability distribution for noise or data.
– It is a smoothing operator.
– It is used in mathematics.
The Gaussian function has important properties which are verified with The Gaussian function has important properties which are verified with respect to its integral:

$$I = \int_{-\infty}^{\infty} \exp\left(-\mathrm{x}^2\right) dx = \sqrt{\pi}$$

In probabilistic terms, it describes 100% of the possible values of any given space when varying from negative to positive values. Gauss function is never equal to zero because it is a symmetric function. When working with images we need to use the two dimensional Gaussian function. This is simply the product of two 1D Gaussian functions (one for each direction) and is given by:

$$G(x,y) = \frac{1}{2\pi\sigma^2} e^{-\frac{x^2+y^2}{2\sigma^2}}$$

A graphical representation of the 2D Gaussian distribution with mean (0,0) and σ=1 is shown to the right.

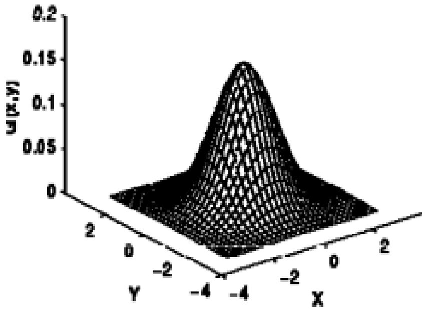


Fig . 2D Gaussian Distribution

The Gaussian filter works by using the 2D distribution as a point-spread function. This is achieved by convolving the 2D Gaussian distribution function with the image. It needs to produce a discrete approximation to the Gaussian function. This theoretically requires an infinitely large convolution kernel, as the Gaussian distribution is non-zero everywhere. Fortunately the distribution has approached very close to zero at about three standard deviations from the mean. 99% of the distribution falls within 3 standard deviations. This means we can normally limit the kernel size to contain only values within three standard deviations of the mean. An integer valued 5 by 5 convolution kernel approximating a Gaussian with an σ of 1.

*GAUSSIAN FILTER ALGORITHM***:**

- Given window size $2N+1$ calculate support points $x_n=3n/N$, $n=-N$, $-N+1$, ... , N;
- Calculate values G''_n;
- Calculate scale factor $k'=\sum G''_n$;
- Calculate window weights $G'_n=G''_n/k'$;
- For every signal element:
  .1 Place window over it;
  .2 Pick up elements;
  .3 Multiply elements by corresponding window weights;
  .4 Sum up products — this sum is new filtered value.

C.FEATURE EXTRACTION

The Image Quality Assessment (IQA) is applied over the filtered image. The input grey-scale image **I** (of size $N \times M$) is filtered with a low-pass Gaussian kernel in order to generate a smoothed version ˆ**I** .Then, the quality between both images (**I** and ˆ**I**) is computed according to the corresponding full-reference IQA metric. It assumes that the loss of quality produced by Gaussian filtering differs between real and fake biometric samples. There are so many image quality measures some of the image quality measures that are applied over the image that are Mean square error (MSE),Peak Signal to Noise Ratio (PSNR),Signal to Noise Ratio (SNR), Structural Content (SC), Maximum Difference (MD), Average Difference (AD), Normalized Absolute Error (NAE), Normalized Cross-Correlation (NXC),Total Edge Difference (TED),Total Corner Difference (TCD) ,Structural Similarity Index (SSI). The selected image quality to extract the image features. 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. Although their efficiency as signal fidelity measures is somewhat controversial up to date, these are probably the most widely used methods for IQA as they conveniently make use of many known psychophysical features of the human visual system they are easy to calculate and Usually have very low computational complexity. Several of these metrics have been included in the feature parameterization. For clarity, these features have been classified here into five different categories according to the image property measured. These features compute the distortion between two images on the basis of their pixel wise differences. Here it includes: Mean Squared Error (MSE), Peak Signal to Noise Ratio (PSNR), Signal to Noise Ratio (SNR), Structural Content (SC), Maximum Difference (MD), Average Difference (AD), Normalized Absolute Error (NAE).The term peak signal-to-noise ratio (PSNR) is an expression for the ratio between the maximum possible value (power) of a signal and the power of distorting noise that affects the quality of its representation. Because many signals have a very wide dynamic range, (ratio between the largest and smallest possible values of a changeable quantity) the PSNR is usually expressed in terms of the logarithmic decibel scale.

D.CLASSIFICATION:

The Quadratic Discriminant Analysis is used to classify the image is either original or fake. Quadratic discriminant analysis is a common tool for classification A standard approach to supervised classification problems is quadratic discriminant analysis (QDA), which models the likelihood of each class as a Gaussian distribution, then uses the posterior distributions to estimate the class for a given test point (Hastie et al., 2001). The Gaussian parameters for each class can be estimated from training points with maximum likelihood (ML) estimation. The simple Gaussian model assumption is best suited to cases when one does not have much information to characterize a class, for example, if there are too few training samples to infer much about the class distributions. Unfortunately, when the number of training samples nis small compared to the number of dimensions of each training sampled, the ML covariance estimation can be ill-posed.

IV.CONCLUSION AND FUTURE WORK :

The biometric systems against different types of attacks has been a very active field in future. This has enhanced the field of security technologies for biometric-based applications.. Simple visual inspection of an image of a real biometric trait and a fake sample of the same trait shows that the two images can be very similar and even the human eye may find it difficult to make a distinction between them after a short inspection. Yet, some disparities between the real and fake images may become evident once the images are translated into a proper feature space.

In this context, it is reasonable to assume that the image quality properties of real accesses and fraudulent attacks will be different. It have explored the potential of general image quality assessment as a protection tool against different biometric attacks (with special attention to spoofing). Some of the feature space of image quality measures has been combined with simple classifiers to detect the difference between the real and fake access attempts. The novel protection method has been evaluated on three largely deployed biometric modalities such as the iris, the finger print and 2D face, using publicly available databases with well-defined associated protocols. It adapts the different biometric details by high performance method, they are able to analyse multi biometric details, using this modalities performance efficiency is high. This methodology of software based detection of fake biometric details is simple, The accuracy obtained from this detection method is about 84% and the complexity involved in this detection method is less when compared with other hardware based detection methods that includes sensor which is of high cost In future some enhancement is made for improving security and accuracy in biometric authentication. By hybriding the software based system over the hardware based biometric system the efficiency of the system can be improved, by hybriding the software based system with the hardware, the accuracy of the system can be improved up to 89% for authentication. It enhances the determination of fake authentication and increases the performance of the process. In future it can be used as an authentication system which involves the biometric details for authentication in Banks, ATM centers, Office, Investigation Departments.

V.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] (2012). BEAT: Biometrics Evaluation and Testing [Online]. Available: http://www.beat-eu.org/

[4] A. Hadid, M. Ghahramani, V. Kellokumpu, M. Pietikainen, J. Bustard, and M. Nixon, “Can gait biometrics be spoofed?” in Proc. IAPR ICPR, 2012, pp. 3280–3283.

[5] Z. Akhtar, G. Fumera, G. L. Marcialis, and F. Roli, “Evaluation of serial
and parallel multi biometric systems under spoofing attacks,” in Proc. IEEE 5th Int. Conf. *BTAS*, Sep. 2012, pp. 283–288.

[6] K. Bowyer, T. Boult, A. Kumar, and P. Flynn, Proceedings of the IEEE Int. Joint Conf. on Biometrics. Piscataway, NJ, USA: IEEE Press, 2011.