Multimodal Biometric and Multi Attack Protection Using Image Features

Archana G S , Sajin Salim

PG Student, TKMIT, archanags001@gmail.com

Abstract— Biometric system uses physiological, behavioral characteristics for automatic personal recognition. Multimodal biometrics is an integration of two or more biometric systems. It overcomes the limitations of other biometrics system like unimodal biometric system. Multimodal biometric for fake identity detection using image features uses three biometric patterns and they are iris, face, and fingerprint. In this system user chooses two biometric patterns as input, which will be fused. Gaussian filter is used to smooth this fused image. Smoothed version of input image and input image is compared using image quality assessment to extract image features. In this system different image quality measures are used for feature extraction. Extracted image features are used by artificial neural network to classify an image as real or fake. Depending on whether image is real or fake appropriate action is taken. Actions could be showing user identification on screen if image is classified as real or raising an alert if image is classified as fake. This system can be used in locker, ATM and other areas where personal identification is required.

Keywords— Biometrics, Multimodal, Image quality assessment, IQM, SSIM, Security, Feed Forward Neural Networks.

INTRODUCTION

Biometrics refers to the automatic identification of a person based on his or her physiological or behavioral characteristics. Biometric recognition offers a reliable solution to the problem of user authentication in identity management systems. Any human physiological or behavioral trait can serve as a biometric characteristic as long as it satisfies the requirements of universality, distinctiveness, permance and collectiabilty. Different types of fraudulent access attempt are present in biometric systems. 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. Image quality assessment is used to protect the biometric system from these attacks. Image quality assessment is following the quality difference hypothesis. In quality difference hypothesis assume 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. Biometric systems are traditionally used for three different applications such as physical access control for the protection against unauthorized person to access to places or rooms, logical access control for the protection of networks and computers, and time and attendance control.

Traditional personal identification systems are based on something that you have (Key) or something that you know (Personal Identification Number [PIN]), but biometrics relies on something that you are. Biometric systems used in real world applications are unimodal. Unimodal biometrics has several problems such as noisy data, intra class variation; inter class similarities, nonuniversality and spoofing which cause this system less accurate and secure. To overcome these problems and to increase level of security multimodal biometrics is used. Multimodal biometrics refers to the use of a combination of two or more biometric modalities in a Verification or Identification system [1]. Three fusion levels in multimodal biometrics: feature level fusion, matching score level fusion and decision level fusion. Different methods such as PCA, ICA and image quality assessment are used for feature extraction. Image quality assessment must be accurate, easy to use, fast and relaiable. Different classification methods are used to distinguish between legitimate and imposter samples. In biometric system mainly consist of enrollment, verification, identification.

Biometrics offers greater security and convenience than traditional methods of personal recognition. In some applications, bio-metrics can replace or supplement the existing technology. One emerging technology that is becoming more widespread in such organizations is bio-metrics, automatic personal recognition based on physiological or behavioral characteristics. The term comes from the Greek words bios (life) and metrikos (measure)[2]. Unimodal biometrics uses a single source of biometric system for personal identification. Unimodal biometrics has several problems such as noisy data, intra class variation, inter class similarities, nonuniversality and spoofing which cause this system less accurate and secure. Multibiometrics is a combination of one or more biometrics. In multibiometrics the noise in any one of the biometrics will lead to high false reject rate (FRR) while identification [3]. All these problems are addressed by Multimodal biometrics. Multimodal biometrics is the integration of two or more types of biometrics system. Multimodal biometrics operates in two phases that is enrollment phase and authentication phase [4]. In enrollment phase, biometric traits of a user are captured and these are stored in the system database as a template for that user and which is further used for authentication phase. In authentication phase, once again traits of a user captured and system uses this to either identify or verify a person.

METHODOLOGY

Multimodal biometric increases the security of the biometric system and avoids spoofing attacks. Human physiological characteristics like Iris, fingerprint and face, which satisfies biometric characteristics such as universality, distinctiveness, permanence and collectability, are used as input to this system. Image quality assessment is used for feature extraction from these inputs as it is a low complexity process compared to other feature extraction methods. If the positioning or angle of user input (face, iris, finger-print) is incorrect then system identifies this user as fake even if he/she is a real user. This can be avoided by using ANN.

1. BASIC BLOCK DIAGRAM

General diagram of the biometric protection method based on Image Quality Assessment is shown Figure 1. For a multimodal biometric system, selecting the proper biometric traits is one of the main tasks. There is no single biometric trait that is the best. The appropriate biometric type for a given application depends on many factors including the type of biometric system operation (identification or verification), perceived risks, types of users, and various need for security. Each biometric trait has associated advantages and limitations. It is often the case that a single biometric trait is not capable of satisfying above mentioned requirements needed by different applications.

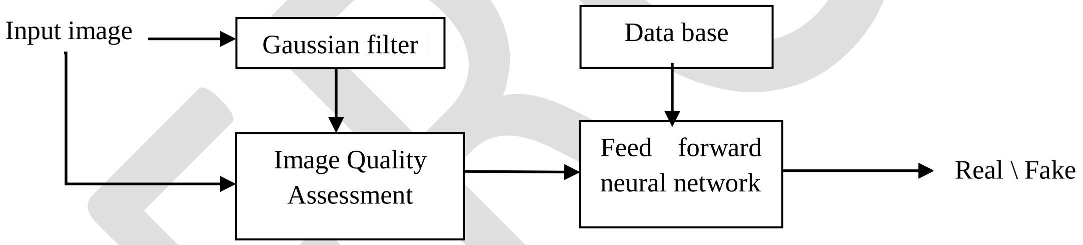


Fig. 1: Block diagram of Multimodal Biometric for Fake Identity Detection using image features

In this method use face, iris and fingerprint biometric traits for this purpose. All of these biometric traits are from the similar region of the human body. The human face plays an important role in our social interaction, conveying peoples identity. Using the human face as a key to security, biometric face recognition technology has received significant attention in the past several years due to its potential for a wide variety of applications in both law enforcement and non-law enforcement. Face recognition serves the crime deterrent purpose because face images that have been recorded and archived can later help identify a person. Iris is a unique characteristic of a person. The primary visible characteristic of iris is the trabecular mesh work that makes possible to divide the iris in a radial fashion. Considered to be one of the exact methods of biometrics. Iris is protected by eyelid, cornea and aqueous humour that makes the likelihood damage minimal makes the likelihood damage minimal.

Fingerprints vary from person to person (even identical twins have different prints) and don’t change over time. Fingerprinting is an authentication technique that has helped law enforcement officials identifies potential criminals for decades, but recently it has started to gain wider usage. The technique is emerging as the most popular form of biometrics, and much of the budding interest is coming from government agencies looking to enhance physical security, such as access to buildings.

2. GAUSSIAN FILTER

The input image I is filtered with a low-pass Gaussian filter in order to generate a smoothed version Î. The Gaussian smoothing operator is a 2-D convolution operator that is used to ‘blur’ images and remove detail and noise. In this sense it is similar to the mean filter, but it uses a different kernel that represents the shape of a Gaussian (‘bell-shaped’) hump. For designing Gaussian filter is h = f special (῾Gaussian᾿,hsize, sigma) which returns a rotationally symmetric Gaussian lowpass filter of size hsize with standard deviation sigma.

3. IMAGE QUALITY ASSESSMENT

Image Quality is a characteristic of an image that measures the perceived image degradations that occurs within the imaging system. Image quality measurement is very important for various image processing applications such as recognition, retrieval, classification, compression, restoration and similar fields. The images may contain different types of distortions like blur, noise, contrast change etc. There are two ways for measuring image quality like Subjective and Objective. If the quality is judged by a group of observers then it comes under subjective quality assessment techniques. Subjective measures are usually inconvenient, time consuming and expensive. On the other hand objective quality measurements automatically predict the perceived image quality based on computational metrics. Objective quality measures can be classified as Full reference (FR), No reference (NR) and Reduced Reference (RR). Full reference image quality assessment demands that a complete reference image is to be known, while no reference image quality assessment means that the reference image is not available. Reference image is partially available and is in the form of a set of extracted features for reduced reference image quality assessment.

2.1 Full Reference (FR) Image Quality Assessment

Full-reference (FR) IQA methods rely on the availability of a clean undistorted reference image to estimate the quality of the test sample. Full reference image quality assessment (FR-IQA) is mainly classified into three; they are Error Sensitivity Measures, Structural Similarity Measures, and Information Theoretic Measures.

2.1.1 Error Sensitivity Measures: An image or video signal whose quality is being evaluated can be thought of as a sum of a perfect reference signal and an error signal. Assume that the loss of quality is directly related to the strength of the error signal. Therefore, a natural way to assess the quality of an image is to quantify the error between the distorted signal and the reference signal, which is fully available in FR quality assessment. Error sensitivity measures have been classified here into five different categories according to the image property measured. They are Pixel Difference measures, Correlation-based measures, Edge-based measures, Spectral distance measures, Gradient-based measures.

2.1.2 Structural Similarity Measures: The principle hypothesis of structural similarity based image quality assessment is that the HVS is highly adapted to extract structural information from the visual field, and therefore a measurement of structural similarity (or distortion) should provide a good approximation to perceived image quality. The luminance of the surface of an object being observed is the product of the illumination and the reflectance, but the structures of the objects in the scene are independent of the illumination. Consequently, to explore the structural information in an image, to separate the influence of the illumination. Define the structural information in an image as those attributes that represent the structure of objects in the scene, independent of the average luminance and contrast. Since luminance and contrast can vary across a scene, use the local luminance and contrast for definition.

First, the luminance of each signal is compared. Assuming discrete signals, this is estimated as the mean intensity:

$$\mu_x = \frac{1}{N}\sum_{i=1}^{N} x_i \qquad (1)$$

The luminance comparison function $l(x, y)$ is then a function of μ_x andμ_y.

Second, remove the mean intensity from the signal. In discrete form, the resulting signal $X - \mu_x$ corresponds to the projection of vector X onto the hyper plane defined by

$$\sum_{i=1}^{N} x_i = 0 \qquad (2)$$

Third, the signal is normalized (divided) by its own standard deviation; so that the two signals are being compared have unit standard deviation. The structure comparison $s(x, y)$ is conducted on these normalized signals $\frac{(X-\mu_x)}{\sigma_x}$ and$\frac{(Y-\mu_y)}{\sigma_y}$.

Finally, the three components are combined to yield an overall similarity measure:

$$S(x, y) = f(l(x, y), c(x, y), s(x, y)) \qquad (3)$$

Information Theoretic Measures: The quality assessment problem is viewed as an information-fidelity problem rather than a signal-fidelity problem. 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 output of the image source is the reference image, the output of the channel is the test image, and 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, the mutual information between them. Although mutual information is a statistical measure of information fidelity, and may only be loosely related with what humans regard as image information, it places fundamental limits on the amount of cognitive information that could be extracted from an image. For example, in cases where the channel is distorting images severely, corresponding to low mutual information between the test and the reference, the ability of human viewers to obtain semantic information by discriminating and identifying objects in images is also hampered. Thus, information fidelity methods exploit the relationship between statistical image information and visual quality.

2.2 No-reference (NR) Image Quality Assessment

Objective quality assessment is a very complicated task, and even full-reference QA methods have had only limited success in making accurate quality predictions. Therefore tend to break up the problem of NR QA into smaller, domain specific problems by targeting a limited class of artifacts distortion specific IQA. The most common being the blocking artifact, which is usually the result of block based compression algorithms running at low bit rates. NR QA for blocking distortion as well as pioneering research into NR measurement of distortion introduced by Wavelet based compression algorithms based on Natural Scene Statistics modeling.

4. FEED FORWARD NEURAL NETWORK

Artificial neural networks (ANNs) are networks of simple processing elements (called neurons) operating on their local data and communicating with other elements. The design of ANNs was motivated by the structure of a real brain, but the processing elements and the architectures used in ANN have gone far from their biological inspiration. There exist many types of neural networks, but the basic principles are very similar. Each neuron in the network is able to receive input signals, to process them and to send an output signal. Each neuron is connected at least with one neuron, and each connection is evaluated by a real number, called the weight coefficient, that reflects the degree of importance of the given connection in the neural network.

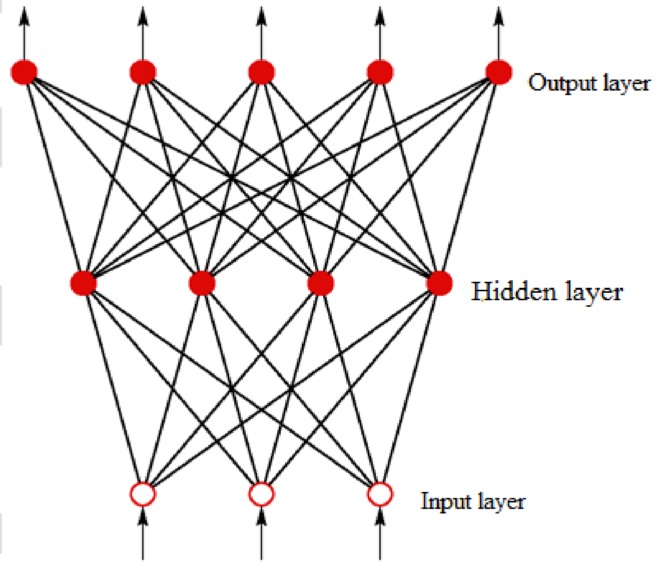


Fig. 2: An example of a 2-layered network

In principle, neural network has the power of a universal approximator, i.e. it can realize an arbitrary mapping of one vector space onto another vector space. The main advantage of neural networks is the fact, that they are able to use some a priori unknown information hidden in data (but they are not able to extract it). Process of capturing the unknown information is called learning of neural network or training of neural network. In mathematical formalism to learn means to adjust the weight coefficients in such a way that some conditions are fulfilled. There exist two main types of training process: supervised and unsupervised training. Supervised training (e.g. multi-layer feed-forward (MLF) neural network) means, that neural network knows the desired output and adjusting of weight coefficients is done in such way, that the calculated and desired outputs are as close as possible. Unsupervised training means, that the desired output is not known, the system is provided with a group of facts (patterns) and then left to itself to settle down (or not) to a stable state in some number of iterations.

A feed forward neural network is a biologically inspired classification algorithm. It consists of a (possibly large) number of simple neuron like processing units, organized in layers. Every unit in a layer is connected with all the units in the previous layer. These connections are not all equal; each connection may have a different strength or weight. The weights on these connections encode the knowledge of a network. Often the units in a neural network are also called nodes. Data enters at the inputs and passes through the network, layer by layer, until it arrives at the outputs. During normal operation, that is when it acts as a classifier, there is no feedback between layers. This is why they are called feed forward neural networks. In the following Figure 4.3 is an example of a 2-layered network with, from top to bottom: an output layer with 5 units, a hidden layer with 4 units, respectively. The network has 3 input units.

RESULTS

Different biometric traits are the input image of this system. Input image is passed through a Gaussian filter and obtain a smoothed version of input image. Image quality assessment is used to extract features from input image and Gaussian filtered image. These image quality features are used to classify the input image as real or fake with the help of feed forward neural network. Simulation is performed using the MATLAB R2014a. The simulation results are as follows:

INPUT IMAGES

Input images were collected from various sites that found with the help of Google. Three biometric traits, face, finger print and iris, are used in this system. Input face image is collected from https://www.idiap.ch/dataset/replayattack . The input fingerprint image is collected from http://prag.diee.unica.it/LivDet09 /. The input iris image is collected from http://www.citer.wvu.edu/.

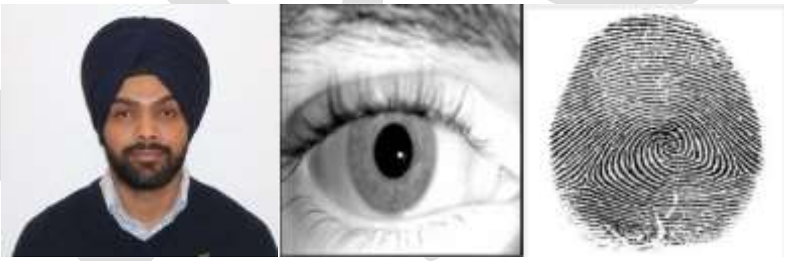
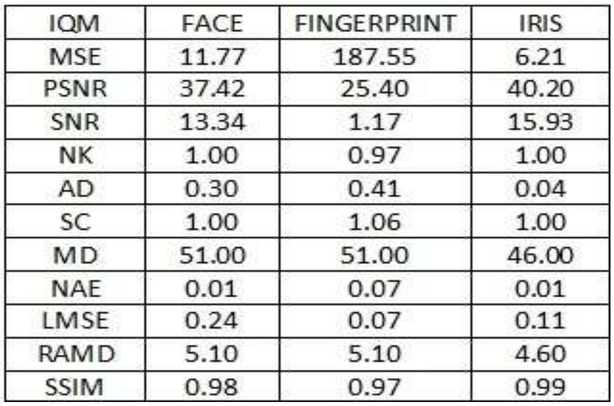


Fig. 3: Input images Face, Fingerprint, Iris

IMAGE QUALITY MEASURES

Table 1: Image Quality Measures of Face, Fingerprint, Iris



IQM	FACE	FINGERPRINT	IRIS
MSE	11.77	187.55	6.21
PSNR	37.42	25.40	40.20
SNR	13.34	1.17	15.93
NK	1.00	0.97	1.00
AD	0.30	0.41	0.04
SC	1.00	1.06	1.00
MD	51.00	51.00	46.00
NAE	0.01	0.07	0.01
LMSE	0.24	0.07	0.11
RAMD	5.10	5.10	4.60
SSIM	0.98	0.97	0.99

An image quality subsystem computes quality scores for images that represent a measure of visual quality of the images. Initial quality scores and can be computed for the images based on image feature values for the images and a transformation factor that represents a measure of importance of image quality for computing relevance scores for images. Image Quality Measures of three input image are shown Table.1. General 11 image quality features extracted from one image to distinguish between legitimate and imposter samples. Smoothed version of input image and input image is compared using image quality assessment to extract image features.

CLASSIFICATION

The feature vector is generated and the image sample is classified as real or fake, using simple classifiers. The feed forward neural network is used to classify the input image is real or fake. The operation of this network can be divided into two phases: learning phase and classification phase. In the classification phase the weights of the network are fixed. A pattern, presented at the inputs, will be transformed from layer to layer until it reaches the output layer. Now classification can occur by selecting the category associated with the output unit that has the largest output value. Feed forward neural network based iris image classification is shown in Figure 4, Figure 5 and Figure 6. Feed forward networks consist of a series of layers. The first layer has a connection from the network input. Each subsequent layer has a connection from the previous layer. The final layer produces the network's output. Feed forward networks can be used for any kind of input to output mapping. A feed forward network with one hidden layer and enough neurons in the hidden layers, can fit any finite input-output mapping problem.

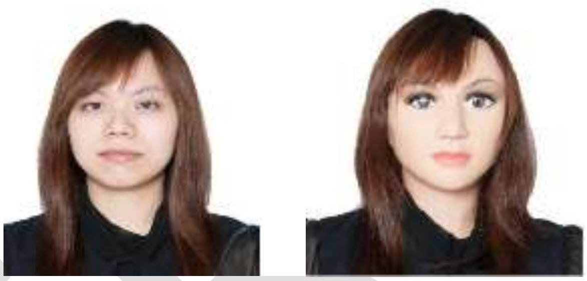


Fig. 4: Classified input face image

CONCLUSION

In real world, biometric systems face various forms of attacks. In these attacks, the intruder uses some type of synthetically produced artifacts, or tries to mimic the behavior of the genuine user, to fraudulently access the biometric system. This project uses Quality Difference Hypothesis, which uses the assumption that image quality properties of real access and fraudulent attacks are different. So image quality assessment is used as a protection tool against different biometric attacks. By the use of IQA this method is able to consistently perform at a high level for different biometric traits. This system uses three biometric traits as the input image, such as face, fingerprint and iris. From the input, image quality measures are extracted and feed forward neural network is used to classifies the input image is real or fake.

REFERENCES:

[1] Javier Galbally, Sbastien Marcel, and Julian Fierrez. "Image quality assessment for fake biometric detection: application to iris, fingerprint and face recognition", IEEE Trans on Image Processing, vol. 23, no. 2, pp. 710-724, Feb. 2014.

[2] 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.

[3] Anil K. Jain and Arun Ross., "Multibiometric systems", Communications Of the ACM, Vol. 47, No. 1, January 2004.

[4] P. S. Sanjekar and J. B. Patil. "An overview of multimodal biometrics", SIPIJ Signal and Image Processing, vol. 4, no. 1, pp. 1-21, February 2013.

[5] J. Galbally, C. McCool, J. Fierrez, S. Marcel, and J. Ortega-Garcia, "On the vulnerability of face verification systems to hill-climbing attacks",Pattern Recognit., vol. 43, no. 3, pp. 1027-1038, 2010.

[6] Jaime Ortiz-Lopez, Javier Galbally, Julian Fierrez and Javier Ortega-Garcia. "Predicting iris vulnerability to direct attacks based on quality related features", in Proc. AWB, 2004

[7] Anil Jain, Lin Hong, Yatin Kulkarni. "A multimodal biometric system using fingerprint, face, and speech", IEEE Trans. on Image Processing, vol. 21, no. 3, pp. 919-933, March 2008.

[8] Anil K. Jain, Karthik Nandakumar, and Abhishek Nagar. “Biometric template security”, EURASIP Journal on Advances in Signal Processing, December 2007.

[9] Jieying Zhu and Nengchao Wang ., “Image quality assessment by visual gradient similarity” IEEE Trans. on Image Processing, vol. 21, no. 3, pp. 919-933, March 2012.

[10] Javier Galbally, Fernando Alonso-Fernandez, Julian Fierrez, and Javier Ortega- Garcia. “Fingerprint liveness detection based on quality measures”,IEEE Trans. On Image Processing , vol. 1, no. 2, Apr. 2006.

[11] M. G. Martini, C. T. Hewage, and B. Villarini, “Image quality assessment based on edge preservation,” *Signal Process., Image Commun.*, vol. 27, no. 8, pp. 875–882, 2012.

[12] N. B. Nill and B. Bouzas, “Objective image quality measure derived from digital image power spectra,” *Opt. Eng.*, vol. 31, no. 4, pp. 813–825, 1992.

[13] 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.

[14] 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.

[15] B. Girod, “What’s wrong with mean-squared error?” in Digital Images and Human Vision. Cambridge, MA, USA: MIT Press, 1993, pp. 207–220