Journal Homepage: - www.journalijar.com
INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)
Article DOI: 10.21474/IJAR01/1418
DOI URL: http://dx.doi.org/10.21474/IJAR01/1418
ISSN NO. 2320-5407

RESEARCH ARTICLE

IMAGE QUALITY ASSESSMENT FOR FAKE BIOMETRIC DETECTION: APPLICATION TO FINGER-VEIN IMAGES.

***Remya Krishnan.**
Student Researcher, Department of Computer Science, Rajagiri School of Engineering.

Manuscript Info

Manuscript History

Received: 12 June 2016
Final Accepted: 19 July 2016
Published: August 2016

Key words:-
Finger-vein, Reduced Reference, Full Reference, No Reference, Image Quality Measures.

Abstract

A biometric authentication system is most widely accepted and used across all fields in real life. Among all the biometric techniques, most of the extrinsic biometric traits (e.g., fingerprint and face) are susceptible to spoof attacks. Finger-vein biometric unlike the others provide a secure mechanism for authentication due to its hidden nature. However the finger-vein biometric system is to some extent vulnerable to spoofing and other indirect attacks. The work presents a software based liveness detection method to address the vulnerability issue. The proposed work focuses on Image Quality Assessment approach where a set of 10 Quality measures are extracted from a single image to recognize the forged samples from the real ones. It is more efficient, less intrusive and fast compared to the other state-of-the art works which makes it feasible for real-time applications. The work uses the publically available database to evaluate the performance of the system which provides better FPR and FNR rates.

Introduction:-

A biometric system is a computer system which is used to identify the person based on the behavioral and physiological characteristic. From the casual user of the home computer, to businesses, medical professionals, and government, there is a wide area of application for biometric security. Most common biometric systems use extrinsic traits like fingerprints, face, iris etc. for authentication. But these biometrics are easily susceptible to attacks. The finger-vein biometric on the other hand utilises the vein patterns under the skin to uniquely authenticate a person. The finger-vein has some advantages over the other biometrics in the areas of security and practicality as shown in Table 1 [1].

Though finger-vein is a better option, the risk for attacks cannot be fully dismissed. The major attacks on the biometrics can be classified as direct and indirect attacks. For an efficient biometric system the performance mainly depends on its capability to handle different kinds of attacks.

The work proposes a new parameterization based on quality measures for a software-based liveness detection as a countermeasure against the attacks. For this a set of 10 image quality features are extracted from a single image provided which is further processed to finally classify the real from the fake finger-vein samples.

Corresponding Author:- Remya Krishnan
Address:- Student Researcher, Department of Computer Science, Rajagiri School of Engineering.

	Security		Practicality				
	Anti-forgery	Acc-uracy	Speed	Enroll-ment	Conven-ience	Cost	Size
Fingerprint	✗	●	●	✗	●	✓	✓
Iris	●	✓	●	●	✗	✗	✗
Face	●	✗	●	●	✓	✗	✗
Voice	●	✗	●	●	✓	●	●
Finger Vein	✓	✓	✓	●	●	●	●

Key: ✗ Poor, ● Average, ✓ Good

Table 1 Qualitative Comparison of Major Biometric Methods

Related Works:-

The Image Quality Assessment (IQA) approach has been a research work for quite some time in the image processing domain. A number of authors have used this technique for analyzing or quantifying the image.

The work on IQA for fake biometric detection has been applied to fingerprints, face and iris in [2]. Here a 25 feature parameterization is carried out which classifies a real from a forged biometric sample. The idea behind the approach being 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 [2]. But the approach was designed to work only for extrinsic biometric traits.

The vulnerability of finger-vein to attacks has been researched and worked on. The work in [3] discusses the extent of finger-vein technology. The spoofing attacks were conducted on the finger-vein biometric system using printed images. The experimental results claim the Spoofing False Accept Rate as high as 86%. This shows a high degree of susceptibility of finger-vein system to attacks.

Another work on vulnerability of finger-vein system focuses on the direct attacks and the countermeasure by texture analysis using steerable pyramids [4].

Finger-vein biometric system mostly utilizes the trait specific property of the finger-vein to classify the images. The different phases include Image Acquisition, Pre-processing, Feature extraction and finally Classification/ Verification. There are different approaches for Feature extraction which includes Repeated Line Tracking [5], Gabor filters [6] and Maximum Curvature [7]. But these approaches might not be effective as a countermeasure for attacks on the system.

Liveness detection denotes the methods capable in discriminating real human from synthetic human traits. The schemes of liveness detection in biometric system depend upon the type of biometric trait.

Some other works on liveness detection approach also have been rendered. It has been applied to fingerprints and iris biometrics. The work proposed by Javier et.al in [8] is an image quality approach where a parameterization of 22 features is performed. The work was applied to iris biometric samples.

Another similar work on fingerprint biometrics based on liveness detection proposes a 10 IQA feature parameterization as in [9]. The final feature vector is used for classification of the fingerprint samples.

Biometric Attacks and Countermeasures:-

Every Biometric system is vulnerable to attacks to some extent. The attacks can be of different types that aim various stages of authentication. As shown in Figure 1, eight possible attacks on the biometric were identified by Ratha in [10]. All these attacks can be broadly classified into two groups: Direct attacks and Indirect attacks.

The Type1 attack aims at the sensor level where the biometric sample is presented to the system. The attack is carried out by creating a synthetic or fake biometric that mimics an authorized individual. This attack comes under the Direct attack or so called spoofing attacks.

The remaining seven attacks comes under the category of Indirect attacks. The Type3 attack compromises the feature extraction module by manipulating the template creation. Type5 attack manipulates the matching module to output a forged matching score. The Type6 attack compromises the stored template in the database by a Trojan horse. The template can be altered, added or deleted. The attacks 2, 4, 7 and 8 aim the communication channel in the system. This compromises the value transmitted through the channels.

To prevent these attacks or at least inhibit the aforementioned attacks, certain countermeasures can be enacted. The Multimodal or Multifactor biometrics employs more than one physiological or behavioural characteristic to authenticate resulting in a more secure and accurate classification. But the additional cost for accommodating an extra biometric comes into play.

Another approach for preventing attacks is Challenge-Response, where the identification of a person is based on voluntary or involuntary responses. In a voluntary response, the end user will consciously react to something that the system presents. In an involuntary response, the user's body automatically responds to a stimulus.

The widely accepted among the countermeasures is an approach based on Liveness detection. Here it uses the physical traits or properties of a biometric to distinguish real (live) or synthetic samples. Liveness assessment methods have to satisfy certain demanding requirements [11]:

1. Non-invasive, the technique should in no case be harmful for the individual or require an excessive contact with the user.
2. User friendly, people should not be reluctant to use it
3. Fast
4. Low cost
5. Good performance.

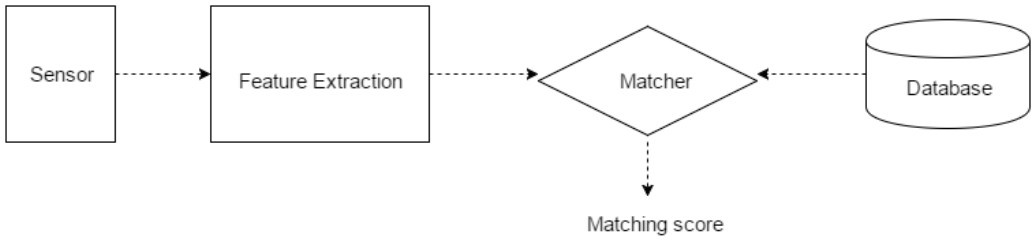

Figure 1:- Eight different attack points in a biometric authentication system (adapted from [10]).

Image Quality Assessment Approach:-

The problem addressed in the work is to classify a finger-vein sample efficiently and accurately from the fraudulent samples. For this the image quality is assessed for liveness detection of the sample. This works on 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" taken from [2]. Using this assumption the proposed work use the "quality difference" to protect against different types of attacks.

The image quality assessment can be broadly classified into Subjective and Objective quality assessment.

The subjective quality assessment approach include human involvement for assessing or perceiving the quality of image by performing voting or questionnaire. The subjective image quality varies from person to person based on factors like experience, mood changes etc. Other factors like cost and time makes the approach impractical for real-world applications.

The other approach is Objective quality assessment where the quality of the image is estimated or predicted automatically. The quality assessed using the objective approach must correlate with the human predictions.

The objective IQA method can be classified into three categories based on the availability of a reference image (distortion-free) image.

1. Full Reference (FR) model: Most common approach where a perfect, distortion-free image is available for quality predictions. There are in general two classes for this quality assessment approach: simple statistical error metrics and human visual system feature based metrics.
2. No Reference (NR) model: In some real-world applications where a reference image is not available for quality assessment, this "blind" quality assessment approach is used.
3. Reduced Reference (RR) model: In this approach only a partial of the reference image is available. A set of features are extracted which are used as a side information for assessing the quality of an image.

Security Protection Approach:-
The work proposed address a biometric protection system that employs image quality assessment approach to efficiently classify a finger-vein image as real or fake. The work focuses on selecting a set of discriminant features that can uniquely represent a finger-vein image and classify as genuine. The system takes as input a single finger-vein image which is used to be classified as real or fake. The image quality vector is calculated from this single input image. The major steps include: Image Acquisition, Image Preprocessing, IQA Feature extraction and Verification/Classification as shown in Figure 2.

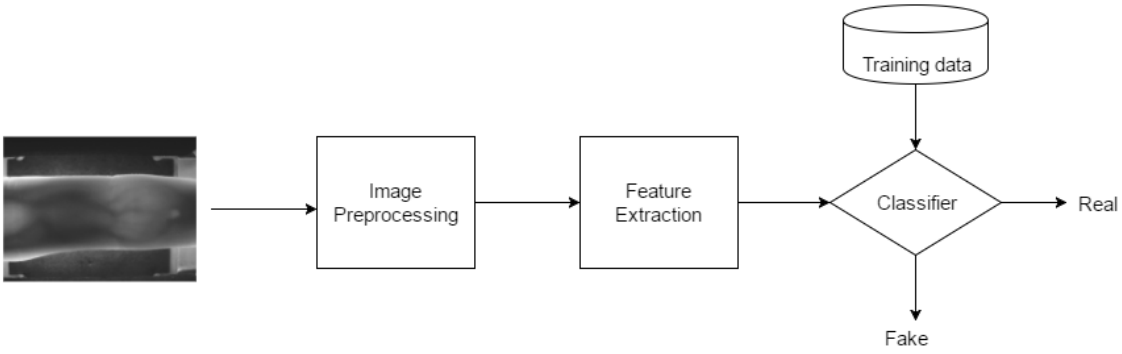

Figure 2:- Biometric protection method based on IQA for finger-vein.

Dataset Acquisition for finger vein image:-
The finger-vein images are captured by the principle of light transmission. There are typically two methods used for this: light reflection and light transmission method. The dataset used in the work is SDUMLA-HMT Database which is publically available. Every image is stored in "bmp" format with 320×240 pixels in size. For experiments the database is equally divided into two subsets: train set and test set.

The available database only contains genuine finger-vein images. For experiments we have created a database for fake finger-vein images. The fake sample set is created by performing some manipulations like jpeg compression, blurring etc. on the original sample set. This dataset is also divided up into two sets: train set and test set.

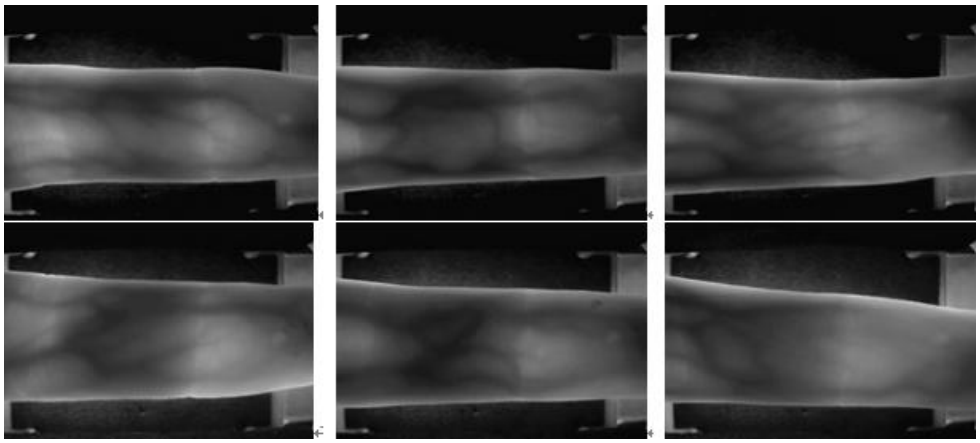

Figure 3:- Preview of the finger-vein images from SDUMLA-HMT Database.

Preprocessing:-

Biometric system has to perform some preprocessing steps on the input sample before authentication. These steps aim to output an image with better quality by removing noise, sharpening, adjusting contrast, brightness etc. The quality of image will influence the accuracy rate of the biometric system.

The preprocessing steps mainly involve image segmentation, Noise removal and image normalization. In image segmentation, the region of interest areas of the image are identified and localized. Noise removal and smoothening is performed on the input image by passing it through a low pass Gaussian filter (size 3*3 and σ=0.5) in a MATLB R2013a platform. After image segmentation, the image enhancement is carried out by first resizing the image.

Feature Extraction:-

Feature extraction module involves dimensionality reduction. Features extracted from an image provide more information about the image. The proposed work focuses on extracting IQA features rather than trait specific features for image representation. The extracted IQA features fall into 3 major categories: full reference, no reference and reduced reference. The classification is shown in Figure 4.

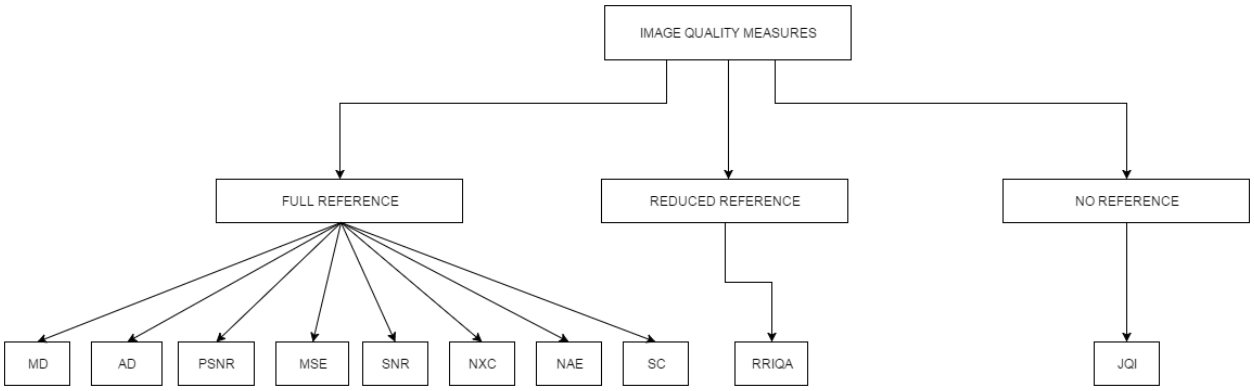

Figure 4:- Classification of the 10 IQA features

Full Reference IQA features include those features that require a distortion free reference image to estimate the quality of the image. The features extracted are based on signal differences and correlation measure between the original and distorted images. The error sensitivity measures are estimated here which simulates the human visual perception of error features. It is easier to compute and thus cost complexity is reduced [12]. The detailed computation is shown in Table 2.

Table 2:- List of the 10 IQA features

No	Type	Acronym	Name	Ref.	Calculation
1	FR	MD	Maximum Difference	[13]	$\text{MD} = max\lvert I_{i,j} - I'_{i,j} \rvert$
2	FR	AD	Average Difference	[13]	$\text{AD} = \frac{1}{MN}\sum_{i=1}^{N}\sum_{j=1}^{M}(I_{i,j} - I'_{i,j})$
3	FR	PSNR	Peak Signal to Noise Ratio	[14]	$\text{PSNR} = 10\log\left(\frac{(max(I^2))}{MSE}\right)$
4	FR	MSE	Mean Squared Error	[15]	$\text{MSE} = \frac{1}{MN}\sum_{i=1}^{N}\sum_{j=1}^{M}(I_{i,j} - I'_{i,j})^2$
5	FR	SNR	Signal to Noise Ratio	[16]	$SNR = 10\ \log\left(\frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(I_{i,j})^2}{N\ .M\ .MSE}\right)$
6	FR	NXC	Normalized Cross-Correlation	[13]	$NXC = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(I_{i,j}\ .\ I'_{i,j})}{\sum_{i=1}^{N}\sum_{j=1}^{M}(I_{i,j})^2}$
7	FR	NAE	Normalized Absolute Error	[13]	$\text{NAE} = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert I_{i,j} - I'_{i,j}\rvert}{\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert I_{i,j}\rvert}$
8	FR	SC	Structural Content	[13]	$\text{SC} = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(I_{i,j})^2}{\sum_{i=1}^{N}\sum_{j=1}^{M}(I'_{i,j})^2}$
9	RR	RRIQA	Reduced Reference IQA	[17]	Detailed implementation in [19]
10	NR	JQI	JPEG Quality Index	[18]	Detailed implementation in [20]

Experiments and Results:-

The experimental work is performed using the SDUMLA-HMT Database of finger-vein images. The image is stored in "bmp" format with 320×240 pixels in size. The database available contains genuine finger-vein samples. A fake finger-vein image set is created for experimental evaluation. For the work, the database is equally divided into two subsets: train set consisting of real and fake images and test set containing the remaining real and fake images.

The performance of the system is evaluated for comparison with the existing protection system. The objective of the work is to classify the real from the fake samples. For the performance evaluation, the best feature set selection is done. This is done by selecting a subset of the features and finding the best optimal subset with better performance. With the experiments performed, the 10 feature set performs the best with minimum Mean Squared Error (MSE) as shown in Figure 5.

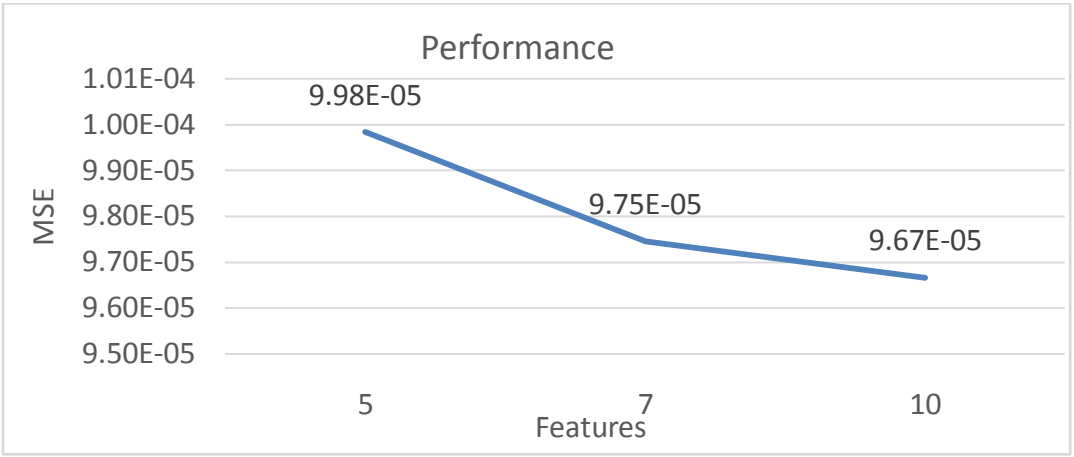

Figure 5:- Best feature set selection comparison.

The performance of the system is best with the 10 selected features. The classifier gives a performance of 82.9% with a standard classifier. The different performance measures are shown in Table3. The results show that the proposed approach gives a good performance while classifying. Low values of False Positive Rate (FPR) and False Negative Rate (FNR) makes the system less vulnerable to attacks.

Table 3:- Performance measures for 10 feature IQA.

Measures	Value
Sensitivity	71 %
Specificity	65 %
False Positive Rate	35 %
False Negative Rate	29 %

Conclusion:-

Biometric systems undergo various attacks that affect the performance of the authentication system. Different approaches for the protection of biometric system has been discussed. The proposed work focuses on the protection of the finger-vein biometric system. The objective discussed aims to classify the real from fake finger-vein images by not considering the trait specific features. It implements the image quality assessment approach to predict the quality thereby efficiently classifying the samples. A parameterization based on 10 image quality measures is proposed in the work. The classifier provide 82.9% performance with the available database. Best feature selection set approach gives the best discriminant set of features among them. The set of 10 quality measures provides the performance with the least MSE. The work provides a best solution for finger-vein authentication systems to protect against attacks with less values of FPR and FNR. Biometric security can be enhanced by implementing such approach.

References:-

1. Ben Edgington. “Introducing Hitachi’s Finger Vein Technology A White Paper”. Version 1.0,May 2007
2. J. Galbally, Sbastien Marcel, J. Fierrez. "Image Quality Assessment for Fake Biometric Detection". in IEEE Transactions on Image Processing, Vol. 23, No. 2, Feb 2014
3. P Tome, M Vanoni, S Marcel. ”On the vulnerability of finger vein recognition to spoofing “. Biometrics Special Interest Group (BIOSIG)
4. Miura, N., Nagasaka, A." Feature extraction of finger-vein pattern based on repeated line tracking and its application to personal identification", Machine Vision and Applications, 2004
5. Kumar, A., Zhou, Y.B. "Human identification using finger images". IEEE Transactions on Image Process, 2012.
6. Miura, N., Nagasaka, A., Miyatake, T." Extraction of finger-vein patterns using maximum curvature points in image profiles". IEICE Transactions on Information and Systems, 2007.
7. J. Galbally, J. Ortiz-Lopez, J. Fierrez, and J. Ortega-Garcia, "Iris liveness detection based on quality related features", in Proc. 5th IAPR ICB, Mar./Apr.2012
8. 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., 2012.
9. Ratha, N., Connell, J., &Bolle, R. (2001). “An analysis of minutiae matching strength”. In LNCS: Vol. 2091. Proc. AVBPA Berlin: Springer.
10. D. Maltoni, D. Maio, A. Jain, and S. Prabhakar, “Handbook of Fingerprint Recognition”. New York, NY, USA: Springer-Verlag, 2009.
11. A. M. Pons, J. Malo, J. M. Artigas, and P. Capilla, “Image quality metric based on multidimensional contrast perception models,” Displays J., vol. 20, no. 2, pp. 93–110, 1999.
12. A. M. Eskicioglu and P. S. Fisher, “Image quality measures and their performance,” IEEE Trans. Commun., vol. 43, no. 12, pp. 2959–2965,Dec. 1995.
13. Q. Huynh-Thu and M. Ghanbari, “Scope of validity of PSNR in image/video quality assessment,” Electron. Lett., vol. 44, no. 13,pp. 800–801, 2008.
14. I. Avcibas, B. Sankur, and K. Sayood, “Statistical evaluation of image quality measures,” J. Electron. Imag., vol. 11, no. 2, pp. 206–223, 2002.
15. S. Yao, W. Lin, E. Ong, and Z. Lu, “Contrast signal-to-noise ratio for image quality assessment,” in Proc. IEEE ICIP, Sep. 2005, pp. 397–400.
16. Z Wang and E P Simoncelli, “Reduced-reference image quality assessment using a wavelet-domain natural image statistic model”, Published in Proc. SPIE, Conf. on Human Vision and Electronic Imaging, X, vol.5666 ,Jan 2005.
17. 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.
18. LIVE. http://live.ece.utexas.edu/research/Quality/index.htm., 2012
19. Z. Wang,E. P. Simoncelli. “Reduced-Reference Image Quality Assessment”. Internet: www.cns.nyu.edu/~lcv/rriqa/., Dec. 20, 2004