ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com

Face Spoofing Detection Using Textural Gradient Features

[1]Parisa Beham M., [2]Mansoor Roomi S.M., [2]Dharmalakshmi D., [1]MadhuramKumar C.

[1]*Department of ECE, Vickram College of Engineering, Madurai Dt -630561, Tamilnadu, India.*
[2]*Department of ECE, Thiagarajar College of Engineering, Madurai Dt -625015, Tamilnadu, India.*

ARTICLE INFO

Article history:
Received 20 January 2015
Accepted 02 April 2015
Published 20 May 2015

Keywords:
Face anti-spoofing, sparse representation, local binary pattern, weighted histogram of gradient orientation, Print attack and CASIA database

ABSTRACT

Face anti-spoofing capability has assumed great importance and attracted intense attention, aiming to assure the reliability of face biometrics. Most of the present day face anti-spoofing techniques focus on data with little variations, which may limit the generalization performance of trained models since potential attacks in real world have become far more complex. Inspired by textural and gradient properties associated with face quality measurement and variations in light reflection, a novel face spoofing detection technique based on deriving weighted gradient features from Local Binary Pattern (LBP) is proposed. The potential of textural features based on LBP, Weighted Histogram of Gradient Orientation (WHGO) and their variations attributable to spoofing attacks like print photographs, cut photographs, warped photographs and video attacks etc has been usefully exploited. The first step of the proposed process is to estimate the LBP of each image followed by extraction of their WHGO features. Finally, a Sparse Representation Classifier (SRC) is trained to discriminate between the genuine and fake faces. The proposed approach is non-intrusive and robust as compared to many existing methods. The proposed anti-spoofing algorithm aims to cover a diverse range of potential attack variations. This is apparent from the extensive training carried out against some of the known spoofing hazards like NUAA imposter, Print attack database and CASIA spoofing attack databases.

To Cite This Article: Parisa Beham M., Mansoor Roomi S.M., Dharmalakshmi D., MadhuramKumar C.., Face Spoofing Detection Using Textural Gradient Features. ***Aust. J. Basic & Appl. Sci.,*** *9(16): 331-337, 2015*

INTRODUCTION

Recent advances of information technology have resulted in the development of person identification based on biometrics. Biometrics has the capability to accurately distinguish between an authorized person and an imposer. Of them due to its potent and successful application, face detection and recognition has received significant attention. In face recognition (FR), the sources of illegal attacks mainly consist of printing photograph, videos and face masks. Among these types of attacks, the most flexible one is printing photographs or screen images captured using tablet PCs and mobile phones. Secure FR systems demand much for the capability of face spoofing detection which can identify whether a face is a real or a fake one. An example of original and fake faces from CASIA spoofing attack database is shown in Fig.1. The state of the art face anti-spoofing approaches can be Mainly multispectral based or micro texture based. The multi-spectral methods utilize the illuminations beyond visual spectrum to tackle the anti-spoofing problem. In (Pavlidis I. and P. Symosek, 2000), it is proved that fake faces exhibit distinguishable properties from the genuine ones under invisible light. By selecting appropriate working spectrum, one can expect that inter-class difference between the genuine and fake faces are to be maximized and the final anti-spoofing decision is made properly (Jianwei Yang Zhen Lei Shengcai Liao Stan Z. Li, 2013). Li *et al*. (2004), analyzed the Fourier spectra to capture the frequency distribution of face images of a live human. Most of the existing techniques mainly concentrate on the measurement of 3D depth information (Shaojie Zhuo,Terence Sim, 2011). The depth information can be used to distinguish whether an input face is from a liveness or a photograph, so as, it is very difficult to deceive the system with the ability of estimating face depth information. In micro texture based analysis Tan *et al*. (2010) proposed a solution based on the Lambertian reflectance properties to distinguish between valid and fake users under the assumption that the surface roughness of both classes is different. The authors use two methods for extracting latent reflectance features: variational and difference-of-gaussian (DoG). Matta *et al*. (2011) also proposed an anti-spoofing solution based on micro texture

Corresponding Author: Parisa Beham M., Department of ECE, Vickram College of Engineering, Enathi, Sivagangai Dt - 630561, Tamilnadu, India.
E-mail: parisa@vickramce.org

analysis. The authors use the LBP texture analysis operator for describing the micro textures and use the feature vectors in a Support Vector Machine classifier to identify fake and original faces. Motivated by texture based methods, Chingovska *et al*. (2012) captured the texture properties of the images with features based on the LBP operator.

Fig. 1: An example of face images from CASIA attack database. 1st, 2nd , 3rd and 4th row represents original face images, warped photographs, cut print photographs and video faces respectively.

The other facial cues include the motion of the facial images such as the blinking of eyes, and the small, involuntary movements of parts of face and head. In (Jee, H.K., 2006) the authors proposed a method for detecting eyes, finding variation of each eye region to determine whether a face is real or not. The basic assumption is that because of blinking and uncontrolled movements of the pupils in human eyes, there should be a big shape variation. In (Pan, G., 2008), an eye blink-based anti-spoofing method is proposed by integrating a structured prediction. Bharadwaj *et al*. (2013) proposed a motion magnification technique that substantially enhances the micro- and macro- facial motion usually exhibited by a subject and proved that the magnified motion improves the performance of spoofing detection techniques, especially texture based approaches. These motion-based methods explore the unnatural movements on the scene in the case of spoofing attacks.

A recent research (Pereira, T.D.F., 2012) used LBP from Three Orthogonal Planes (LBP-TOP) for spoofing detection in the Print Attack database. LBPTOP explicitly utilized the temporal information by computing LBP histograms in XT and YT planes along with spatial information in XY plane. Thus the texture-based methods explore the texture artifacts and the quality deterioration that appear when an image is recaptured.

Existing approaches to spoof detection widely use texture analysis with complex configurations to achieve better performance. However, a spoofing detection technique must not only be robust but also be computationally efficient. To this texture and gradient analysis based approach to face spoofing detection is relatively less explored. In this paper, motivated by the texture based approaches like LBP (Ivana Chingovska Andre, Anjos Sebastien Marce, 2012 ; Maatta, J., 2011) and MLBP (Samarth Bharadwaj, 2013), we concentrate on the methods which rely on a static images to do spoof detection. Such methods can also be directly applied to deal with video spoof attacks for better performance. Face texture and its gradient vary greatly due to changes in ambient illumination, factors attributable to camera and other imaging devices. These stochastic variations make discrimination of fake images against real ones quite difficult.

Contributions of this paper are follows: (1) we introduce a texture and gradient based face spoofing detection using sparse representation classifier. Here we exploit not only the textural property of LBP but also the histogram of gradients derived using WHGO from the LBP texture image. (2) Sparse representation classifier has been trained with the 1D weighted gradient vectors, which makes the system computationally efficient (3) The effectiveness of the proposed algorithm has been proved using publicly available databases viz. NUAA imposter, Print attack, CASIA spoofing attack.

The remainder of this paper is structured as follows. Section 2 describes face anti-spoofing approach using LBP and WHGO. Experiments on NUAA imposter, Print attack, CASIA spoofing attack databases are illustrated in Section 3 and in Section 4, we conclude the paper.

2 Proposed Approach:

The main goal of a biometric security system is the verification of an individual's identity. The primary reason for this is to prevent impostors from accessing protected.

Resources with the help of physical and biological properties of human beings, a biometric system can offer more security for a

security system based on feature recognition. In general, FR algorithms are not complete to discriminate fake face from real face which is a major security issue. It is easy to spoof face recognition systems by facial pictures such as portrait photographs. Therefore, there is an increasing need to detect such attempts of attacks to biometric systems. In the proposed framework as shown in Fig.2, automatically detect the impostors by exploring texture features using LBP and gradient features from the texture of LBP.

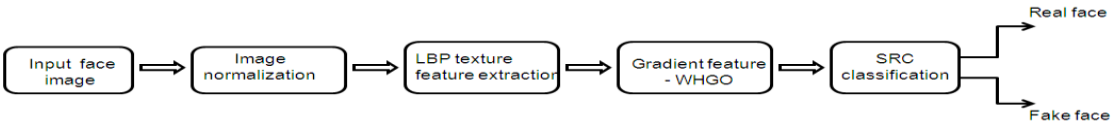

Fig. 2: Illustrating the proposed texture cum gradient based spoofing detection approach with sparse representation classifier.

2.1 Effectiveness of Texture Gradient Features:

Texture based feature extraction is an effective method to derive distinct features from any 2D, 3D still images or videos. From the related works it is inferred that the texture information obtained from the 2-D objects tend to suffer from the loss of texture information compared to the images taken from the 3-D objects. Motivated by this, we exploit weighted gradient features derived from texture image of LBP [12] to find spoofing attack. To derive gradient feature from LBP image we use state of the art WHGO technique [13]. The texture wise discrimination in both LBP image and gradient image is explicitly evident and is shown in Fig. 3 for both real face and fake face which motivates us to use texture gradient feature for spoofing detection. It is observed that, deriving gradient on a texture feature we get more textural information. Finally sparse representation classifier has been trained with the 1D weighted gradient vectors, which consumes less computational time.

2.1.1. Local Binary pattern (LBP):

In literature it has been known that feature level concatenation of LBP features are efficient for spoofing detection. The important reason to use this LBP texture feature is that it's robustness against illumination variation and their less computational complexity. But the original LBP operator is limited to local 3x3 neighborhoods which does not capture global structures that may be the dominant features of some textures. Later to deal with different scale Ojala (1996) extended the LBP by evenly sampling the local neighborhood pixels with radius around the center pixel.

$$LBP_{P,R}(x,y)=\sum_{i=0}^{P-1}s(g_i-g_c)2^i \quad (1)$$

Where $LBP_{P;R}$ *(x; y)* is the decimal value of image location at (x; y), P is the sampling point, R is the patch radius, g_c and g_i are center pixel and neighboring pixels of 3 x 3 window.

$$s(x)=\begin{cases}1, x>0\\ 0, otherwise\end{cases} \quad (2)$$

The final LBP feature descriptor of decimal values is computed and is used as facial feature. We intended to derive weighted gradients feature from this textural image.

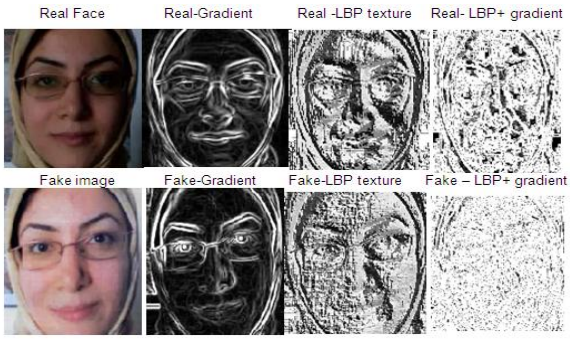

Fig. 3: First row (left to right) real face and its normal gradient face, LBP texture face, and Gradient feature face from LBP. Second row (left to right) imposter face and its normal gradient face, LBP texture face, and Gradient feature face from LBP.

2.1.2. Weighted Histogram of Gradient Orientation (WHGO):

The distribution of the gradient within the region of interest in an image is described by Weighted Histogram of Gradient Orientation (WHGO) descriptors. The WHGO descriptor makes use of information of both gradient magnitude and orientation. WHGO feature is computed by

partitioning the image into 2x2 sub-regions. Gradient magnitudes and orientations are calculated for each sub-region and the gradient orientations are quantized as,

$$O_{ij} = ceil(B \times \frac{\pi + \theta_{ij}}{2\pi}) \quad (3)$$

Where $\theta_{ij} \in \{x \in R \mid -\pi < x <= \pi\}$ is the gradient orientation in pixels (i, j), $O_{ij} \in \{x \in Z \mid 1 <= x <= B\}$ is the orientation bin for pixel (i, j), B is the number of orientation bins and ceil(x) is the function that rounds x to the nearest integer greater than or equal to x. Subsequently, the weight is calculated as,

$$W_{\delta,k} = \frac{\sum_{(i,j)\in\delta} M_{ij} Q_{ij}}{\sum_{(i,j)\in\delta} M_{ij}} \quad (4)$$

$$Q_{i,j}^{k} = \begin{cases} 1, O_{i,j} = k \\ 0, O_{i,j} \neq k \end{cases} \quad (5)$$

where $\delta \in \{x \in Z \mid 1 < x <= 4\}$ is the sub region, $k \in \{x \in Z \mid 1 < x <= B\}$ is the k^{th} dimension of histogram, and $M_{i,j}$ is the gradient magnitude in the pixel (i,j). Finally, WHGO descriptor is computed by ,

$$H_{\delta,k} = W_{\delta,k} \frac{\sum_{(i,j)\in\delta} Q_{ij}^{\ k}}{N_{\delta}} \quad (6)$$

Where N_{δ} is the number of pixels in sub-region. Thus 1D weighted gradient vectors are created and are used to train the SRC. Fig.4 highlights the larger difference of gradient vectors extracted using WHGO for both real and fake face. The overall algorithm of the proposed method is given below.

Algorithm of the proposed approach

Training phase:

1. Select original face and fake face images for training.
2. All the images are gray scaled, normalized and resized to 256 x 256.
3. Extract textural information from each training image using LBP as in eqn. (1).
   - 3.1. Divide the image into 3x3 overlapping blocks (R=1).
   - 3.2. Construct binary pattern of 8 neighboring pixels (P=8) by setting the threshold as central pixel C for a block.
   - 3.3. Find decimal values for each binary pattern computed from the block.
   - 3.4. Replace the Central pixel C by the decimal value found in 2.3.
   - 3.5. Repeat steps 3.2 to 3.4 for all the blocks of the training image.
   - 3.6. Finally, an LBP image with rich textural information is obtained.
4. Derive WHGO from LBP image.
   - 4.1. Partition the LBP image into 2x2 sub-regions.
   - 4.2. Compute gradient magnitude and orientation for a sub-region.
   - 4.3. Quantize gradient orientation into discrete bins using eqn. (3).
   - 4.4. Calculate weight using eqn. (4)
   - 4.5. Compute weighted Histogram of Gradient Orientation by eqn. (5).
   - 4.6. Repeat 4.2 to 4.5 for all the sub-regions.

Testing phase:

5. Acquire the query face image to detect whether it is fake face or not.
6. Derive WHGO from LBP image as mentioned in Step 2 and 3.
7. Discriminate by using sparse representation classifier.

2.2 Spoofing detection using Sparse Representation Classifier:

The conventional nearest neighbor (NN) classifier predicts the label of the image to be tested by only using its nearest neighbor in the training data; therefore it can easily be affected by noise. Nearest Subspace (NS) approximates the test image by using all the images belonging to the same category, and assigns the image to the category which minimizes the reconstruction error (Wright, J., 2006). But NS may not work well for the case where classes are highly correlated to each other.

To overcome these problems, Wright *et al* (2006), proposed a sparse coding based face recognition framework, which can automatically selects the images in the training set to approximate the test image. This method is robust to occlusion, illumination and noise and achieves excellent performance in classification and recognition. Basically, the training samples are not uncorrelated and the distance between the test sample and a training sample should not be independently calculated and should take into account the relationship between different training samples. The sparse method first uses a linear combination of all the training samples to represent the test sample and then exploits modified distance to classify the test sample. The method obtains the coefficients of the

linear combination by solving a linear system. The method then calculates the distance between the test sample and the result of multiplying each training sample by the corresponding coefficient and assumes that the test sample is from the same class as the training sample that has the minimum distance. The method elaborately modifies NNC and considers the relationship between different training samples, so it is able to produce a higher classification Accuracy.

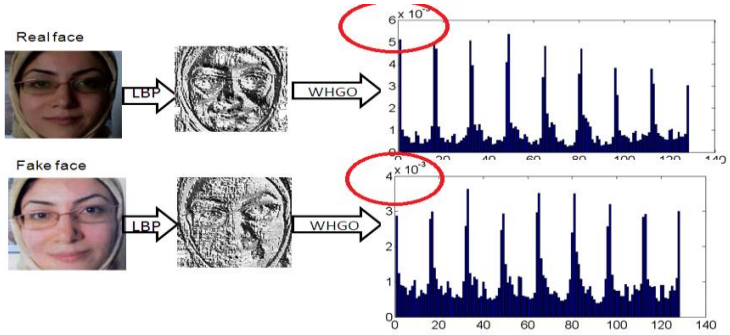

Fig. 4: Figure shows the textural and gradient feature difference between both real and fake face.

3 Experimental Analysis and Results:

To show the efficiency of the proposed framework, the results of texture based feature extraction approaches have been compared with state of the approaches. Face spoofing detection technique must be robust across different types of attacks. Therefore, the experiments are performed on three publicly available databases, namely (1) NUAA imposter database (Xiao yang Tan, 2010), (2) Print Attack database (Anjos, A. and S. Marcel, 2011) and (3) CASIA attack database (Zhang, Z., 2012). All the databases are coupled with a fixed experimental procedure. Assessment of binary classification systems belonging to two classes usually referred to as positive (real face) and negative class (fake face). They are trained to assign scores to the input samples. Then, a threshold is calculated to separate the scores of the positive and the negative class and the samples with scores above the threshold are classified as positives, while the ones with scores below the threshold as negatives.

3.1. Results and Discussion on Spoof attack databases:

3.1.1 Results on NUAA imposter database:

NUAA imposter database uses photos of different sizes as attacks. All the face images are gray scaled, normalized and resized to 64 x 64. Thus from the NUAA database 2383 original face samples and 3912 fake face samples of 15 subjects have been selected respectively. The experimentation has been carried out by varying the number of training images and comparison with various state of the art methods has been done as shown in Fig. 5. In our cross-database experiment, we increase the amount of test samples by combining the two original subsets where the number of real subjects increases significantly. Table 1 lists the detection accuracy of the proposed method on NUAA in comparison with benchmark algorithms. From the table it is observed that the proposed approach managed the cross-database testing and produces higher detection rate of 99.80%

3.1.2 Results on CASIA Attack database:

CASIA is a face anti-spoofing database (Zhang, Z., 2010) with diverse attacks to serve as an evaluation platform in the literature. The database contains 50 genuine subjects, and the fake faces are produced from the high quality records of the genuine faces. Three imaging qualities and three kinds of fake face attacks are: (1) In a warped photo attack, the attacker deliberately warps an intact photo, trying to simulate facial motion. Intact means there is no cut-off region in the photo, in contrast with the cut photo attack. (2) In cut photo attack, to exhibit. Blink behavior, the subject's eye regions are cut off. An attacker hides behind and exhibit blinking through the holes. (3) In video attack, the high resolution genuine videos are displayed using an iPad. For experimentation purpose, we consider 10 persons with 10 sample images per person. To evaluate the effectiveness of the proposed algorithm, all the three attack faces of 10 subjects from CASIA have been taken. Totally 300 fake faces and 100 genuine faces are used for evaluation. Table 2 show the detection rate of face spoofing detection for three attacks and also for combined attacks of CASIA database. Even the CASIA database is so complex, our proposed method shows higher detection rate of 95.50%, which proves the significance of the texture gradient features.

3.1.3 Results on Print Attack database:

The Print-Attack face spoofing database consists of both real-access and attack attempts to 50 different identities. According to the etiquette of PRINT-ATTACK database, we perform three experiments with different fake subsets: i) G+F, "fixed" sub-database; ii) G+H, "hand" sub-database and iii) G+F+H, both of them. For training and testing totally

we have considered 600 and 800 face images respectively. The experimental results are also compared with the DoG (Zhang, Z., 2012) baseline method and MsLBP (Maatta, J., 2011) based method. As shown in table 3, the proposed method outperforms all the others in all three experiments.

.

Since in this work we have used texture gradient vector as a feature domain, our proposed method takes less computational time of 0.375 sec (15 persons) for detection which is half of the computational time of SVM (0.832 sec) method.

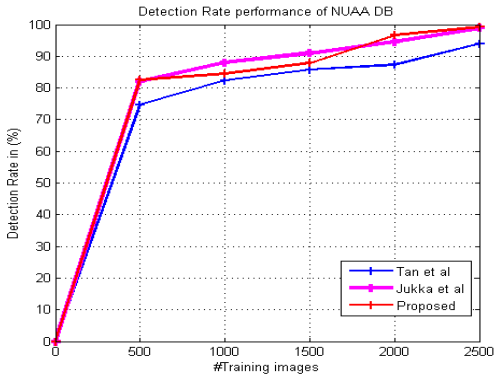

Fig. 5. Spoofing detection rate versus number of training on the NUAA imposter database.

Table 1: Detection rate performance of the proposed method on NUAA database.

Features	Accuracy (%)
WHGO	88.54
LBP	93.75
Concatination of LBP and WHGO	95.32
Proposed approach	99.80

Table 2: Detection rate performance of various attacks of CASIA database.

Attacks	DoG [17]	MsLBP [6]	Proposed approach
Warped photo attack	73.2	78.6	89.65
Cut photo attack	78.0	82.1	95.50
Video attack	68.6	86.1	86.25
Over all dataset	76.0	82.3	83.78

Table 3: : Detection rate performance of Print Attack database.

Scenario	DoG [17]	MsLBP [6]	Proposed approach
G+F	81.9	84.4	89.65
G+H	85.2	88.4	95.50
G+F+H	84.7	90	96.25

4 Conclusions:

One of the common forms of face spoofing attack is impersonation. Many preemptive verification systems are already in vogue to prevent the menace of spoofing. The purpose of this paper is to find an appropriate way to evaluate verification systems which are prone to spoofing attacks. Details of similar works already carried out are discussed in this paper. In the proposed method, the textural gradient features are exploited through LBP and WHGO techniques. We have validated the recognition performance of the proposed system using sparse representation classifier training against three popular spoofing databases.

REFERENCES

Pavlidis I. and P. Symosek, 2000. The imaging issue in an automatic face/disguise detection.In: Computer Vision Beyond the Visible Spectrum. Methods and Applications, page, 15.

Jianwei Yang Zhen Lei Shengcai Liao Stan Z. Li, 2013. Face Liveness Detection with Component Dependent Descriptor, In: IEEE International Conference on Biometrics Compendium, Biometrics (ICB).

Li, J., Y. Wang, T. Tan, A.K. Jain, 2004. Live face detection based on the analysis of fourier spectra. In: SPIE, 296–303.

Shaojie Zhuo,Terence Sim, 2011. Defocus Map Estimation from a Single Image, In: Pattern Recognition, 44(9): 1852-1858.

Tan, X., Y. Li, J. Liu and L. Jiang, 2010. Face Liveness Detection from a Single Image with Sparse Low Rank Bilinear Discriminative Model. In: European Conference on Computer Vision, 504–517.

Maatta, J., A. Hadid and M. Pietikainen, 2011. Face Spoofing Detection from Single Images using

Micro-texture Analysis, In: Intl. Joint Conference on Biometrics, 1–7.

Jee, H. K., S.U. Jung and J.H. Yoo, 2006. Liveness detection for embedded face recognition system, In: International Journal of Biological and Medical Sciences, 1(4): 235-238.

Pan, G., Z. Wu, L. Sun, 2008. Liveness detection for face recognition. In: Recent Advances in Face Recognition, 236–252.

Ivana Chingovska Andre, Anjos Sebastien Marce, 2012. In: On the Effectiveness Of Local Binary Patterns In Face Anti-Spoofing. In: IDIAP research report, 24.

Samarth Bharadwaj, Tejas, I. Dhamecha, Mayank Vatsa and Richa Singh, 2013. Computationally Efficient Face Spoofing Detection with Motion Magnification. In: CVPR.

Pereira, T.D.F., A. Anjos, J.M. De Martino and S. Marcel, 2012. LBP-TOP based countermeasure against facial spoofing attacks. In: ACCV Workshop on Computer Vision with Local Binary Pattern Variants.

Ojala, T., M. Pietikainen and D. Harwood, 1996. A comparative study of texture measure with classification based on feature distribution. In: Pattern recognition, 29: 51-59.

Li Zhou, Zongtan Zhou and DewenHu, 2013. Scene classification using multi-resolution low level feature combination. In: Neuro computing, 122: 284–297.

Wright, J., A.Y. Yang, A. Ganesh, S.S. Sastry, Y. Ma, 2006. Robust face recognition via sparse representation. IEEE Transactions on Pattern Analysis and Machine Intelligence, 31(2): 210-227.

Xiao yang Tan, Yi Li, Jun Liu and Lin Jiang, 2010. " Face Liveness Detection from A Single Image with Sparse Low Rank Bilinear Discriminative Model, ECCV.

Anjos, A. and S. Marcel, 2011. Counter-measures to photo attacks in face recognition: a public database and a baseline. In International Joint Conference on Biometrics.

Zhang, Z., J. Yan, S. Liu, Z. Lei, D. Yi and S.Z. Li, 2012. A face anti spoofing database with diverse attacks. In: 5th IEEE IAPR International Conference on Biometrics Compendium, Biometrics (ICB), Page(s): 26 – 31.