International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 18
December 2016

Implementation of Dual Tree Complex Wavelet Transform Approach for Secured Biometric Application

[1] Y.S.S. SRIRAMAM , [2] V. ANURAGH. , [3] M S MADHAN MOHAN, [4]. T. SARAN KUMAR
1. M-Tech,ECE, BVC Engineering college, odalarevu,Amalapuram,AP.
2. Assistant Prof, ECE, BVC Engineering college, odalarevu,Amalapuram,AP.
3. AssistantProf, ,ECE, BVC Engineering college, odalarevu,Amalapuram,AP.
4. Assistant Prof, ECE, BVC Engineering college, odalarevu,Amalapuram,AP.

ABSTRACT: Biometrics-based authentication systems offer obvious usability advantages over traditional password and token-based authentication schemes. However, biometrics raises several privacy concerns. A biometric is permanently associated with a user and cannot be changed. Hence, if a biometric identifier is compromised, it is lost forever and possibly for every application where the biometric is used. Moreover, if the same biometric is used in multiple applications, a user can potentially be tracked from one application to the next by cross-matching biometric databases. In this paper, we demonstrate several methods to generate multiple cancellable identifiers from fingerprint images to overcome these problems. Designing of a novel software-based fake detection method that can be used in multiple biometric systems to detect different types of fraudulent access attempts. We outlined several advances that originated both from the cryptographic and biometric community to address this problem. In particular, we outlined the advantages of cancellable biometrics over other approaches and presented a case study of different techniques. This project can be enhanced by reducing the image using DTCWT. This modification can decrease the image size and execution can be reduced by enhancing the image clarity. This enhancement can be shown using PSNR values.

KEYWORDS: DTCWT, BIOMETRIC,PSNR, RIDGES, Image Quality, Countermeasures, gummy finger, printed iris image or face mask

INTRODUCTION: Biometrics refers to metrics related to human characteristics. Biometrics authentication (or realistic authentication)[note 1] is used in computer science as a form of identification and access control.[1] 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.[2] Biometric identifiers are often categorized as physiological versus behavioral characteristics.[3] Physiological characteristics are related to the shape of the body. Examples include, but are not limited to fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina and odour/scent. Behavioral characteristics are related to the pattern of behavior of a person, including but not limited to typing rhythm, gait, and voice.[4][note 2] Some researchers have coined the term behaviometrics to describe the latter class of biometrics.[5] SECURING information and ensuring the privacy of personal identities is a growing concern in today's society. Traditional authentication schemes primarily utilize tokens or depend on some secret knowledge possessed by the user for verifying his or her identity. While these techniques are very popular, they have several limitations. Both token and knowledge-based approaches cannot differentiate between an authorized user and a person having access to the tokens or passwords. In case of knowledge-based authentication systems, managing multiple passwords (i.e., identities) presents usabilityproblems. Biometrics-based authentication schemes using fingerprints, face recognition, etc., overcome these limitations while offering usability advantages and are therefore rapidly extending traditional authentication schemes. However, despite its obvious advantages, the use of biometrics raises several security and privacy concerns asoutlined below: Biometrics is authentic but not secret: Unlike passwords and cryptographic keys that are known only to the user, biometrics such as voice, face, signature, and even fingerprints can be easily recorded and potentially misused without the user's consent. There have been several instances where artificial fingerprints [14] have been used to circumvent biometric security systems. Face and voice biometrics are similarly vulnerable to being captured without the user's explicit knowledge. In contrast, tokens and knowledge have to be willingly shared by the user to becompromised.

LIVENESS ASSESSMENT IN AUTHENTICATION SYSTEM:

Liveness assessment methods represent a challenging engineering problem as they have to satisfy certain demanding requirements [21]:

(i) non-invasive, the technique should in no case be harmful for the individual or require an excessive contact with the user;

(ii) user friendly, people should not be reluctant to use it;

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 18
December 2016

(i i i) 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;

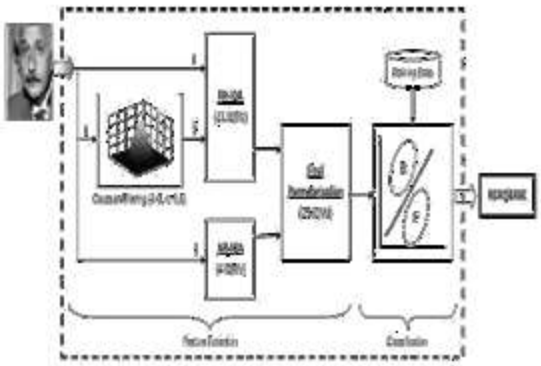
(iv) low cost, a wide use cannot be expected if the cost is excessively high;

(v) 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.

PROPOSED TECHNIQUE:

Software-based techniques,

in this case the fake trait is detected once the sample has been acquired with a standard sensor (i.e., features used to distinguish between real and fake traits are extracted from the biometric sample, and not from the trait itself).



In the present work we propose 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). Moreover, being software-based, it presents the usual advantages of this type of approaches: fast, as it only needs one image (i.e., the same sample acquired for biometric recognition) to detect whether it is real or fake; non-intrusive; user-friendly (transparent to the user); cheap and easy to embed in already functional systems (as no new piece of hardware is required). An added advantage of the proposed technique is its speed and very low complexity, which makes it very well suited to operate on real scenarios (one of the desired characteristics of this type of methods). As it does not deploy any trait-specific property (e.g., minutiae points, iris position or face detection), the computation load needed for image processing purposes is very reduced, using only *general* image quality measures fast to compute, combined with very simple classifiers. It has been tested on publicly available attack databases of iris, fingerprint and 2D face, where it has reached results fully comparable to those obtained on the same databases and following the same experimental protocols by more complex trait-specific top-ranked approaches from the state-of-the-art.

IMAGE QUALITY ASSESSMENT FOR LIVENESS DETECTION:

The use of image quality assessment for liveness detection is motivated by 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.*‖ Expected quality differences between real and fake samples may include: degree of sharpness, color and luminance levels, local artifacts, amount of information found in both type of images (entropy), structural distortions or natural appearance. For example, iris images captured from a printed paper are more likely to be blurred or out of focus due to trembling; face images captured from a mobile device will probablybe over- or under-exposed; and it is not rare that fingerprint images captured from a gummy finger present local acquisition artifacts such as spots and patches. Furthermore, in an eventual attack in which a synthetically produced image is directly injected to the communication channel before the feature extractor, this fake sample will most likely lack some of the properties found in natural images.

Following this —*quality-difference*‖ hypothesis, in the present research work we explore the potential of *general* image quality assessment as a protection method against different biometric attacks (with special attention to spoofing).

FULL-REFERENCE IQ MEASURES:

Full-reference (FR) IQA methods rely on the availability of a clean undistorted reference image to estimate the quality of the test sample. In the problem of fake detection addressed in this work such a reference image is unknown, as the detection systemonly has access to the input sample. In order to circumvent this limitation, the same strategy already successfully used for image manipulation detection in [24] and for steganalysis in [26], is implemented here. the input grey-scale image $\mathbf{I}$ (of size $N \times M$) is filtered with a low-pass Gaussian kernel ($\sigma = 0.5$ and size 3×3) in order to generate a smoothed version $\hat{\mathbf{I}}$ .Then, the quality between both images ($\mathbf{I}$ and $\hat{\mathbf{I}}$) is computed according to the corresponding full-reference IQA metric. This approach assumes that the loss of

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 18
December 2016

quality produced by Gaussian filtering differs between real and fake biometric samples.

GAUSSIAN FILTER:

In electronics and signal processing, a Gaussian filter is a filter whose impulse response is a Gaussian function (or an approximation to it). Gaussian filters have the properties of having no overshoot to a step function input while minimizing the rise and fall time. This behaviour is closely connected to the fact that the Gaussian filter has the minimum possible group delay. It is considered the ideal time domain filter, just as the sinc is the ideal frequency domain filter.[1] These properties are important in areas such as oscilloscopes[2] and digital telecommunication systems.[3] Mathematically, a Gaussian filter modifies the input signal by convolution with a Gaussian function; this transformation is also known as the Weierstrass transform. The Gaussian function is non-zero for x \in (-\infty,\infty) and would theoretically require an infinite window length. However, since it decays rapidly, it is often reasonable to truncate the filter window and implement the filter directly for narrow windows, in effect by using a simple rectangular window function. In other cases, the truncation may introduce significant errors. Better results can be achieved by instead using a different window function; see scale space implementation for details.

DUAL TREE COMPLEX WAVELETS TRANSFORM:

The **complex wavelet transform (CWT)** is a complex-valued extension to the standard discrete wavelet transform (DWT). It is a two-dimensional wavelet transform which provides multiresolution, sparse representation, and useful characterization of the structure of an image. Further, it purveys a high degree of shift-invariance in its magnitude, which was investigated in However, a drawback to this transform is that it is exhibits 2^d (where d is the dimension of the signal being transformed) redundancy compared to a separable (DWT). The use of complex wavelets in image processing was originally set up in 1995 by J.M. Lina and L. Gagnon [1] in the framework of the Daubechies orthogonal filters banks[2]. It was then generalized in 1997 by Prof. Nick Kingsbury. In the area of computer vision, by exploiting the concept of visual contexts, one can quickly focus on candidate regions, where objects of interest may be found, and then compute additional features through the CWT for those regions only. These additional features, while not necessary for global regions, are useful in accurate detection and recognition of smaller objects. Similarly, the CWT may be applied to detect the activated voxels of cortex and additionally the temporal independent component analysis (tICA) may be utilized to extract the underlying independent sources whose number is determined by Bayesian information criterion.

MEASURED PARAMETERS FROM AN IMAGE:

MSE	Mean Squared Error
PSNR	Peak Signal to Noise Ratio
SNR	Signal to Noise Ratio
SC	Structural Content
MD	Maximum Difference
AD	Average Difference
NAE	Normalized Absolute Error
RAMD	R-Averaged MD
LMSE	Laplacian MSE
NKC	Normalized Cross-Correlation
MAS	Mean Angle Similarity
MAMS	Mean Angle Magnitude Similarity
TED	Total Edge Difference
ECD	Edge Cosine Difference
SME	Spectral Magnitude Error
SPE	Spectral Phase Error
GME	Gradient Magnitude Error
GPE	Gradient Phase Error
SSIM	Structural Similarity Index
VIF	Visual Information Fidelity
RRED	Reduced Ref. Entropic Difference
HVS	HVS Quality Index
HLFI	High-Low Frequency Index
BIQI	Blind Image Quality Index
NIQE	Naturalness Image Quality Evaluator

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 18
December 2016

In this context, the present work has made several contributions to the state-of-the-art in the field of biometric security, in particular:

i) it has shown the high potential of image quality assessment for securing biometric systems against a variety of attacks;

i i) proposal and validation of a new biometric protection method;

i i i) reproducible evaluation on multiple biometric traits based on publicly available databases;

iv) comparative results with other previously proposed protection solutions.

The present research also opens new possibilities for future work, including:

i) extension of the considered 25-feature set with new image quality measures;

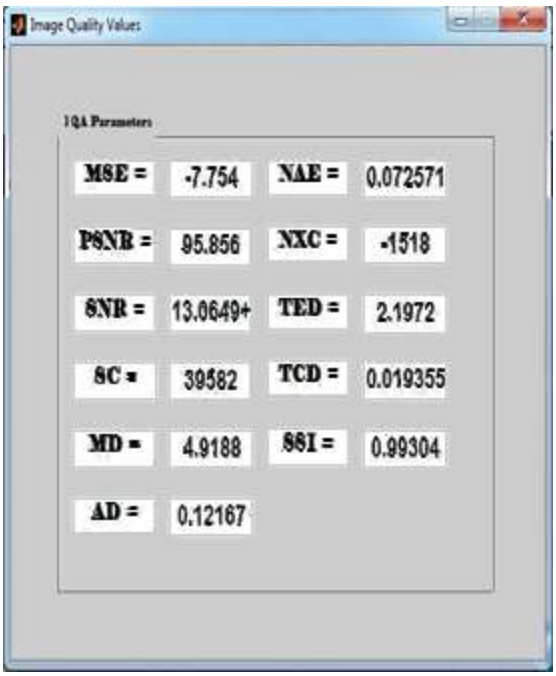
i i) further evaluation on other image-based modalities (e.g., palmprint, hand geometry, vein);

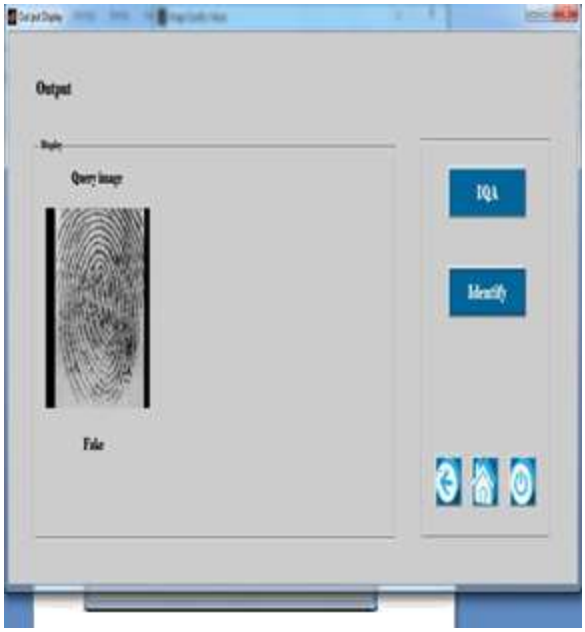
i i i) inclusion of temporal information for those cases in which it is available (e.g., systems working with face videos);

iv) use of video quality measures for video attacks (e.g., illegal access attempts considered in the REPLAY-ATTACK DB);

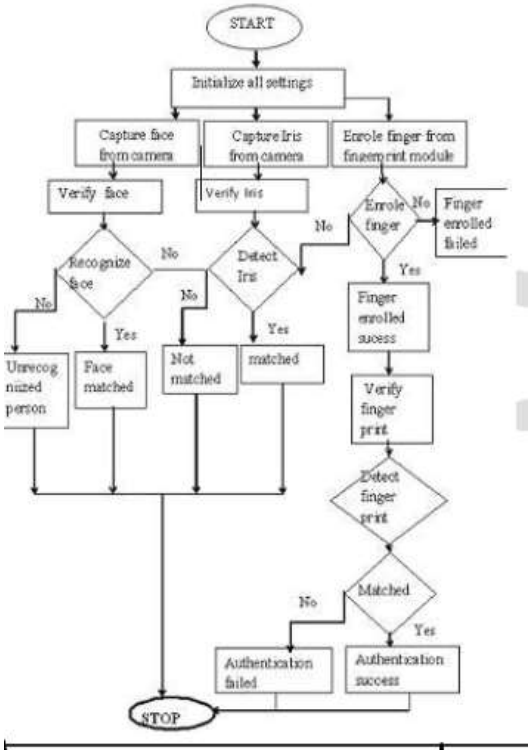
v) analysis of the features individual relevance.

RESULT:





Flow chart



CONCLUSION: Finally, by using DTCWT, IQA techniques, this project is well executed on different sets of images. This is very much efficient in finding of fake or original. This interest has lead to big advances in the field of security-enhancing technologies for biometric-based applications.

However, in spite of this noticeable improvement, the development of efficient protection methods against known threats has proven to be a challenging task. Yet, some disparities between the real and fake images may become evident once the images are translated into a proper feature space. These differences come from the fact that biometric traits, as 3Dobjects, have their own optical qualities.

REFERENCES:

[1] 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.

[2] T. Matsumoto, ―Artificial irises: Importance of vulnerability analysis,‖ in *Proc. AWB*, 2004.

[3] 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.

[4] A. K. Jain, K. Nandakumar, and A. Nagar, ―Biometric template security,‖ *EURASIP J. Adv. Signal Process.*, vol. 2008, pp. 113–129, Jan. 2008.

[5] 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.