SVM BASED PERFORMANCE OF IRIS DETECTION, SEGMENTATION, NORMALIZATION, CLASSIFICATION AND AUTHENTICATION USING HISTOGRAM MORPHOLOGICAL TECHNIQUES

Dr. T. Arumuga Maria Devi
Assistant Professor
Centre for Information Technology and Engineering,
Manonmaniam Sundarnar University,
Tirunelveli, Tamilnadu, India

S. Mariammal
Research Scholar,
Centre for Information Technology and Engineering
Manonmaniam Sundarnar University,
Tirunelveli, Tamilnadu, India

ABSTRACT

An Efficient Authentication for Iris Authentication Using Iris Pattern, the proposed System detects the Presentation Attack. A novel presentation attack detection (PAD) scheme based on one-of-the-art schemes. The proposed M-BSIF that can accurately capture both micro-texture (with multiscale binarized statistical image features and linear support vector machines. Extensive experiments are carried out on four different publicly available iris artifact databases that have revealed the outstanding performance of the proposed PAD scheme when benchmarked with various well-established state small scale size) as well as coarse texture (using large scale size) information from both per ocular and iris region.

Key words: Image Segmentation, Image Normalization, Morphological Operation, IRIS Recognition, Anti-Spoofing, Presentation Attacks, Artifact.

Cite this Article: Dr. T. Arumuga Maria Devi and S. Mariammal, SVM Based Performance of IRIS Detection, Segmentation, Normalization, Classification and Authentication Using Histogram Morphological Techniques, International Journal of Computer Engineering and Technology, 7(4), 2016, pp. 1–11.

http://www.iaeme.com/ijcet/issues.asp?JType=IJCET&VType=7&IType=4
INTRODUCTION
Biometric systems have been widely used for many applications. Biometric recognition or, simply, biometrics refers to the automatic recognition of individuals based on physiological or behavioural characteristics. Biometrics including face, iris, fingerprints, voice, palms, hand geometry, retina, handwriting, gait etc. have been used for the security applications and have many advantages compared to the traditional security systems such as identification tokens, password, personal identification numbers (PINs) etc. Iris recognition is one of the most promising methods because the iris has the great mathematical advantage that its pattern variability among different persons is enormous. In addition, as an internal (yet externally visible) organ of the eye, the iris is well protected from the environment and stays unchanged as long as one lives. However, biometric recognition systems are vulnerable to be spoofed by fake copies, for instance, fake finger tips made of commonly available materials such as clay and gelatine.

RELATED WORKS
To propose the new method of detecting fake iris attack based on the Purkinje image by using collimated IR-LED (Infra-Red Light Emitting Diode). Especially, we calculated the theoretical positions and distances between the Purkinje images based on the human eye model and the performance of fake detection algorithm could be much enhanced by such information. We determine the input image as the live iris and accept the user. If not, we reject the input image as the fake iris. To enhance the performance of our algorithm, we should have more field tests and consider more countermeasures against various situations and counterfeit samples in future. We propose the new method of detecting fake iris attack based on the Purkinje image. Experimental results show that the FRR and FAR are 0.33%, respectively.

To develop a new iris image segmentation methodology with a more robust behavior. This new methodology could contribute to the aim of non-cooperative biometric iris recognition, where the ability to process this type of image is required. Accuracy degradation on the first and second images was just about 0.14%. We have described the problems associated with the segmentation of iris images with poor quality. We presented some of the most cited methodologies in the iris segmentation literature and used the UBIRIS database. In this method we ignore fragile bits. And finally we use SVM (Support Vector Machine) classifier for approximating the amount of people identification in our proposed system. Reduces Processing time and increase the Classification Accuracy. This paper provide a less feature vector length with an insignificant reduction of the percentage of correct classification. It is proposed an effective algorithm for iris feature extraction using contourlet transform. We propose an efficient method to tackle this problem. Firstly, the normalized iris image is divided into sub-regions according to the properties of iris textures. To evaluate the usefulness of the proposed method. Extensive experiments indicate that the proposed method can be well adapted for iris spoof detection. We propose a texture analysis based method for efficient iris spoof detection (especially for contact lens detection). The basic idea is the textural differences between counterfeit iris images and the live iris images. We propose a new fake iris detection method based on wavelet packet transform. Paper printed iris can be well detected. It can help to further increase the robust of the iris recognition system. The fake iris database and conduct experiments on a large number of iris databases in various environments to evaluate the stability and reliability of the proposed method. We have presented an efficient fake iris detection method based on wavelet packet transform together with SVM. This method
is completely robust for fake iris detection because it exploits the pupil dynamics for iris localization. The proposed method not only showed the very high accuracy rate of iris segmentation at comparable timing cost but also very accurate segmentation of iris with minimal loss of features. More Time Take. The strength of the method is that it is not based on the above stated assumptions which are seldom true but that it uses a very practical approach which is based on the comparison of two iris images at different light intensities to detect the change in the size of pupil.

**PROPOSED SYSTEM**

A novel presentation attack detection (PAD) scheme based on multiscale binarized statistical image features and linear support vector machines. Extensive experiments are carried out on four different publicly available iris artifact databases that have revealed the outstanding performance of the proposed PAD scheme when benchmarked with various well-established state-of-the-art schemes.
IMPLEMENTATION

ILLUMINANCE IMAGE

Illumination is an important concept in visual arts. The illumination of the subject of a drawing or painting is a key element in creating an artistic piece, and the interplay of light and shadow is a valuable method in the artist's toolbox. The placement of the light sources can make a considerable difference in the type of message that is being presented. Multiple light sources can wash out any wrinkles in a person's face, for instance, and give a more youthful appearance. In contrast, a single light source, such as harsh daylight, can serve to highlight any texture or interesting features.

EyeBall Detection

Eye detection and tracking is integral for attentive user interfaces properties of eyes, their appearance and dynamics to detect and track eyes reliably.

Boundary Detection
Boundary is traced for all points with binary value as 1 in all direction starting from selected point that is the first point that has value as 0 coming from top to bottom in any one quarter of image. Thus, complete boundary is traced for a complete iris without any intersection.

SEGMENTATION AND NORMALIZATION

IRIS Code Generation

Step 1:
C image size is of 64X512. We Divide normalized iris image into basic cell regions for generation of iris code. One cell region has 64 (row) ×32 (col) pixels size. A Standard deviation of pixels value is used as a representative value of a basic cell region for calculation.

Step 2:
Now we got 16 bit values we have to convert this into 16 bit binary value by considering the threshold as mean from each block.

Step 3:
If the pixel values of is greater than threshold make it 1.
**Step 4:**
Else make it 0
By following above step we can obtain 16 bit binary Iris Code for Verification.

**Iris Pattern Generation**

![Iris Pattern Generation](image)

**Gabor Filters**
A set of Gabor filters which have different frequencies and correspond to different orientations can be used in extracting useful information or features from an image. The 28 frequency and orientation representation offered by Gabor filters are similar to those in the human visual system, and hence they have been found to be particularly useful in texture representation and discrimination

**TRAINIMAGE**

**Select Train Image**

![Train Image](image)

Photographic Experts Group is a lossy compression technique for color images. Although it can reduce files sizes to about 5% of their normal size, some detail is lost in the compression.

**Boundary Detection**

![Boundary Detection](image)
Boundary is traced for all points with binary value as 1 in all direction starting from selected point that is the first point that has value as 0 coming from top to bottom in any one quarter of image. Thus, complete boundary is traced for to complete iris without any intersection.

**IRIS Pattern Generation**

*Gabor Filters*

A set of Gabor filters which have different frequencies and correspond to different orientations can be used in extracting useful information or features from an image. The 28 frequency and orientation representation offered by Gabor filters are similar to those in the human visual system, and hence they have been found to be particularly useful in texture representation and discrimination.

**AUTHENTICATION**

*MultiScale BSIF*
M-BSIF will allow one to combine various filter responses that in turn extract not only a rich set of information but also allows one to generalize the BSIF for presentation attack detection of iris on both visible and NIR spectrum. In this work, we choose three different filters of size $17 \times 17$ with a length of 12 bits, $7 \times 7$ with a length of 10 bits and $5 \times 5$ with a length of 8 bits.

**Classification**

![Classification Image](image)

**Authentification**

**Performance**

![Performance Image](image)

**Analysis**

![Analysis Image](image)
SVM Based Performance of IRIS Detection, Segmentation, Normalization, Classification and Authentication Using Histogram Morphological Techniques

RESULT AND DISCUSSION
In this paper iris detection algorithm have been developed using MATLAB 9.0. It is tested on 2.4 GHz CPU with 1 GB ram. And used database CASIA Iris, which is available in the public domain have been selected for experiments. The database consists of photographic of 30 images (320*280) and also each image consists of 3 different positioned images. And using MATLAB 9.0 GUI is developed and which show stepwise result by matching hamming code and finally person is recognize.

CONCLUSION
In this paper, we have presented an efficient fake iris detection method based on wavelet packet transform together with SVM. Experimental results have illustrated the encouraging performance of the current method both in accuracy and speed. Using this method, paper printed iris can be well detected. It can help to further increase the robust of the iris recognition system.

- Highly accurate but easy
- Fast
- Needs some developments
- Experiments are going on
- Will become day to day technology very soon

REFERENCES


SVM Based Performance of IRIS Detection, Segmentation, Normalization, Classification and Authentication Using Histogram Morphological Techniques

AUTHORS

Assistant Professor Dr. T. ARUMUGA MARIA DEVi Received B.E. Degree in Electronics & Communication Engineering from Manonmaniam Sundaranar University, Tirunelveli India in 2003, M. Tech degree in Computer & Information Technology from Manonmaniam Sundaranar University, Tirunelveli, India in 2005 and Worked as Lecturer in department of Electronics & Communication Engineering in Sardar Raja College of Engineering and also received Ph.D Degree in Information Technology – Computer Science and Engineering from Manonmaniam Sundaranar University, Tirunelveli, India in 2012 and also the Assistant Professor of Centre for Information Technology and Engineering of Manonmaniam Sundaranar University since November 2005 onwards. Her research interests include Signal and Image Processing, Multimedia and Remote Communication.

Research Scholar, S. MARIAMMAL Received M.Sc degree in Information Technology from Manonmaniam Sundaranar University in 2004, Currently M.Phil in Information Technology. Her research interests include image processing, computer communication and networking.