IRIS Liveness Detection Using Mobilenetv2

Sneha Pradeep[1], Safrin S[2]
[1, 2] Dept of Computer Science
[1, 2] Noorul Islam Centre For Higher Education Kumaracoil, Thuckalay.

Abstract- *A new iris liveness detection technique for iris based on quality related measures is presented. The novel anti-spoofing technique is tested on a database comprising over 1,600 real and fake (high quality printed images) iris samples proving to have a very high potential as an effective protection scheme against direct attacks.The focus of this paper is on presentation attack detection for the iris biometrics, which measures the pattern within the colored concentric circle of the subjects' eyes, to authenticate an individual to a generic user verification system. Unlike previous deep learning methods that use single convolutional neural network architectures, this paper develops a framework built upon triplet convolutional networks that takes as input two real iris patches and a fake patch or two fake patches and a genuine patch. The aim is to increase the number of training samples and to generate a representation that separates the real from the fake iris patches. The smaller architecture provides a way to do early stopping based on the liveness of single patches rather than the whole image. The matching is performed by computing the distance with respect to a reference set of real and fake examples. The proposed approach allows for realtime processing using a smaller network and provides equal or better than state-of-the-art performance on three benchmark datasets of photo-based and contact lens presentation attacks.*

Keywords- Convolutional Neural Network, Fake Iris Patch, Realtime Processing, Iris Liveness Detection Technique, Presentation Attacks.

I. INTRODUCTION

Authentication is an important step for giving access to resources to authorized individuals. The conventional authentication systems like a pin, card, a password cannot distinguish between real users and imposters who have unethically got access to the system.(The device that allows the automatic identification of an individual is known as a biometric system. Liveness detection is a preventive approach for containing sensor level attacks in biometrics authentication systems, where a malignant user builds a fake replica of a legitimate biometrics, applies it directly to the sensor and declares its corresponding identity. This task is formulated as a binary classification problem to establish if the claimed identity is genuine or it does not correspond to the subject in front of the sensor.Iris liveness detection approaches can broadly be divided into: i)software-based techniques, in which the fake irises are detected once the sample has been acquired with a standard sensor (i.e., features used to distinguish between real and fake eyes are extracted from the iris image, and not from the eye itself), and ii) hardware-based techniques, in which some specific device is added to the sensor in order to detect particular properties of a living iris such as the eye hippus (which is the permanent oscillation that the eye pupil presents even under uniform lighting conditions) or the pupil response to a sudden lighting event (e.g., switching on a diode).

Currently, Presentation Attack Detection (PAD) techniques are increasingly becoming critical for biometrics systems since a large number of people use these technologies to access their personal data and for safety purposes such as passing the security checks at airports. Unfortunately, this massive usage of biometrics comes with various security and privacy issues. Different attacks can be directed to the authentication system to grant access to some exclusive area or to steal confidential data. For instance, the software and the network configuration can have security holes or bugs, and the matching algorithms can be fooled if the attacker knows the software implementation details. Moreover, whereas a physical key or badge can be replaced, the biometrics are permanent and their pattern, if visible, can be easily captured and reproduced. Among all the weak points of an authentication system, the biometrics scanner is probably the most vulnerable part since it is in direct contact with the potential malignant user that has to be captured. Liveness detection is a technique to prevent these so called presentation attacks by formulating a binary classification problem to establish whether the biometrics under examination comes from a legitimate user or it is an illegitimate authentication attempt. In this paper we focus on the iris biometrics, where the pattern in the eyes can be easily obtained from a high-resolution photograph and then showed to a sensing device, fooling the authentication system by declaring the identity of the real biometrics owner (e.g., using a printed photo, a video on a tablet or printed contact lens). In the present work, we analyze the potential of quality assessment (already considered in the literature for multimodal fusion, or score rejection) to identify real and fake iris samples acquired from a high quality printed image. It is not the first time quality assessment has been explored as a way to detect spoofing attacks. A similar strategy to the one proposed in the present paper based on quality related features has already been used for spoofing detection in fingerprint based recognition systems, achieving remarkable good results in the first International Fingerprint Liveness Detection Competition. Furthermore, some quality based features have also been used individually for liveness detection in traits.We propose a new parameterization based on quality related measures which is used in a global software-based solution for iris liveness detection. This novel strategy has the clear advantage over other previously proposed methods of needing just one iris image (i.e., the same iris image used for access) to extract the necessary features in order to determine if the eye presented to the sensor is real or fake. This fact shortens the acquisition process and reduces the inconvenience for the final user. The presented method is tested on an iris database which comprises 1,600 real and fake (high quality printed images) samples where it has proven its high potential as a countermeasure to prevent spoofing attacks. Different conclusions are also extracted regarding the most convenient types of quality features to be considered in liveness detection

II. LITERATURE SURVEY

2.1 An Optimised Defensive Technique to Recognize Adversarial Iris Images Using Curvelet Transform

Author :J. K. Meenakshi, G. Maragatham
Year of Publishing : 6 June 2022
Paper Type : An optimised defensive technique to recognize adversarial iris images using curvelet transform," Intelligent Automation & Soft Computing, vol. 35, no.1.

Adversarial inputs are introduced to purposefully confuse a neural network, restricting its use in sensitive application areas such as biometrics applications. In this paper, an optimized defending approach is proposed to recognize the adversarial iris examples efficiently. The Curvelet Transform Denoising method is used in this defense strategy, which examines every sub-band of the adversarial images and reproduces the image that has been changed by the attacker. The salient iris features are retrieved from the reconstructed iris image by using a pre-trained Convolutional Neural Network model (VGG 16) followed by Multiclass classification. The classification is performed by using Support Vector Machine (SVM) which uses Particle Swarm Optimization method (PSO-SVM). The proposed system is tested when classifying the adversarial iris images affected by various adversarial attacks such as FGSM, iGSM, and Deepfool methods. An experimental result on benchmark iris dataset, namely IITD, produces excellent outcomes with the highest accuracy of 95.8% on average.

2.1.1 Advantages

- Better accuracy
- Improves performance

2.1.2 Disadvantage

- Relevant it must be related to the intended class

2.2 Deep Residual Learning for Image Recognition

Author : Kaiming He, Xiangyu Zhang, Shaoqing Ren, Jian Sun
Year of Publishing : 2016
Paper Type : IEEE Conf. on Computer Vision and Pattern Recognition, Las Vegas, NV, USA, pp. 770–778

Deeper neural networks are more difficult to train. We present a residual learning framework to ease the training of networks that are substantially deeper than those used previously. We explicitly reformulate the layers as learning residual functions with reference to the layer inputs, instead of learning unreferenced functions. We provide comprehensive empirical evidence showing that these residual networks are easier to optimize, and can gain accuracy from considerably increased depth. On the ImageNet dataset we evaluate residual nets with a depth of up to 152 layers—8× deeper than VGG nets [40] but still having lower complexity. An ensemble of these residual nets achieves 3.57% error on the ImageNet test set. This result won the 1st place on the ILSVRC 2015 classification task. We also present analysis on CIFAR-10 with 100 and 1000 layers. The depth of representations is of central importance for many visual recognition tasks. Solely due to our extremely deep representations, we obtain a 28% relative improvement on the COCO object detection dataset. Deep residual nets are foundations of our submissions to ILSVRC & COCO 2015 competitions1 , where we also won the 1st places on the tasks of ImageNet detection, ImageNet localization, COCO detection, and COCO segmentation.

2.2.1 Advantages

- Use the spatial and temporal characteristics of video.
- High precision

2.2.2 Disadvantages

- Unusable in situations with a single facial image.
- Slow

2.3 Hybrid Feature Extractions and CNN for Enhanced Periocular Identification During Covid 19

Author: Raniyah Wazirali, Rami Ahmed.
Year of Publishing : 08 October 2021
Paper Type: Healthcare Intelligence using Deep Learning and Computer Vision Workshops.

The global pandemic of novel coronavirus that started in 2019 has seriously affected daily lives and placed everyone in a panic condition. Widespread coronavirus led to the adoption of social distancing and people avoiding unnecessary physical contact with each other. The present situation advocates the requirement of a contactless biometric system that could be used in future authentication systems which makes fingerprint-based person identification ineffective. Periocular biometric is the solution because it does not require physical contact and is able to identify people wearing face masks. However, the periocular biometric region is a small area, and extraction of the required feature is the point of concern. This paper has proposed adopted multiple features and emphasis on the periocular region. In the proposed approach, combination of local binary pattern (LBP), color histogram and features in frequency domain have been used with deep learning algorithms for classification. Hence, we extract three types of features for the classification of periocular regions for biometric. The LBP represents the textual features of the iris while the color histogram represents the frequencies of pixel values in the RGB channel. In order to extract the frequency domain features, the wavelet transformation is obtained. By learning from these features, a convolutional neural network (CNN) becomes able to discriminate the features and can provide better recognition results. The proposed approach achieved the highest accuracy rates with the lowest false person identification.

2.3.1 Advantage

- Excellent defence against photo assaults

2.3.2 Disadvantage

- Accuracy declines when attacked

2.4 Iris Recognition; From Classic to Modern Approaches

Author: Vahid Nazmdeh; Shaghayegh Mortazavi; Daniel Tajeddin; Hossein Nazmdeh; Morteza Modarresi Asem
Year of Publishing : 14 March 2019
Paper Type: 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)

Biometrics is considered as the use of physiological and behavior characteristics to decide an individual. Numerous biometric attributes have been enhanced and used to confirm the person's character. These days, acknowledgment of individuals by the iris picture is inexactly used once secure ID of an individual is required. The iris detection framework has been mostly used and demonstrated to be useful and compelling in identifying an individual with high accuracy and nearly perfectly matching. Among authentication methods, iris detection systems have attracted so much attention, because rich iris tissue offers robust biometric criteria for determining people. In this paper, improvements in research methodologies used by various scholars and researchers for iris localization, iris segmentation, feature extraction, classification, and encryption of the Iris images are discussed. Additionally, authors discussed the drawbacks of previous algorithms and their findings of the results and surveyed the function of previous practices, and investigate the disadvantages and benefits of this identification by iris. It could be the first step towards starting a wider study.

2.4.1 Advantages

- Usable with single image and video
- Fast

2.4.2 Disadvantage

- Based only on spatial information from the image.

2.5 Iris liveness detection competition (LivDet-Iris)

Author:PriyankaDas, JosephMcGrath, ZhaoyuanFang, AidanBoyd, , SébastienMarcel, MateuszTokielewicz, PiotrMaciejewicz, KevinBowyer, Adam Czajka, Stephanie Schuckers, Juan Tapia, Sebastian Gonzalez, Meiling Fang, NaserDamer, Boutros, ArjanKuijper, Renu Sharma, Cunjian Chen, Arun Ross
Year of Publishing : September2020
Paper Type : IEEE International Joint Conference on Biometrics.

An international competition series called LivDet-Iris was established in 2013 with the goal of evaluating and disclosing advancements in iris Presentation Attack Detection. It is open to academics and industry (PAD). Results from the LivDet-Iris 2020 competition, the fourth in the series, are presented in this publication. The competition this year incorporated numerous novel components: (a) added new attack kinds (screen samples, cadaver eyes, and prosthetic eyes); (b) started LivDet-Iris as an ongoing endeavour; and (c) made the testing process for LivDet-Iris available to everyone via the Biometrics Evaluation and Testing website (BEAT) * an open-source platform that enable the continuous benchmarking of new algorithms, and (c) performance evaluation of the submitted entries against three baseline techniques (provided by the Universities of Notre Dame and Michigan State) and three open-source iris PAD techniques that are freely available. The competition's top performer recorded a weighted average APCER and BPCER of 59.10% and 0.46%, respectively, for each of the five assault types. The most recent assessment of iris PAD across a broad range of presentation attack tools is provided in this study.

2.5.1 Advantage

- Totally transparent to the user

2.5.2 Disadvantage

- Expensive

2.6 Iris Recognition Using Artificial Neural Network

Author: Nada A. Alhamdi, Mohamed B. Aldebri;,Moad H. Alkout
Year of Publishing: 27 July 2022
Paper Type2022: IEEE 2nd International Maghreb Meeting of the Conference on Sciences and
Techniques of Automatic Control and Computer Engineering(MI-STA).

Today, iris recognition becomes one of the most popular and useful techniques used for person verification, which takes advantage of the fact that the eye has some unique characteristics represented by the iris or more precisely in the pupil. Iris scanning biometric systems measure the unique patterns in the iris of human’s eye to verify and authenticate their identity. Fast, contactless and renowned for its accuracy, biometric iris recognition can work at long distance with some solutions that leverage the modality requiring only a glance from a user. This paper presents a study on the performance of iris recognition system using PYTHON for implementation and CASIA-V I iris databases as training and testing images where seven hundreds of iris images were used. The measurements demonstrated our model provides higher identification accuracy than the VGG16 model. This paper presents a simple methodology for pre-processing iris images and the design and training of a feedforward artificial neural network for iris recognition. Three different iris image data partitioning techniques and two data codings are proposed and explored. BrainMaker simulations reveal that recognition accuracies as high as 93.33% can be reached despite our testing of similar irises of the same color. We also experiment with various number of hidden layers, number of neurons in each hidden layer, input format (binary vs. analog), percent of data used for training vs testing, and with the addition of noise. Our recognition system achieves high accuracy despite using simple data pre-processing and a simple neural network.

2.6.1 Advantages

- Higher performance
- Perfect recognition accuracy

2.6.2 Disadvantage

- Mostly slower

2.7 Iris Recognition Development Techniques.

Author: Jasem Rahman Malgheet,Noridayu Bt Manshor,and Lilly Suriani Affendey
Year of Publishing: 23 Aug 2021
Paper Type:24th International Conference on Iris Pattern Recognition.

Recently, iris recognition techniques have achieved great performance in identification. Among authentication techniques, iris recognition systems have received attention very much due to their rich iris texture which gives robust standards for identifying individuals. Notwithstanding this, there are several challenges in unrestricted recognition environments. In this article, the researchers present the techniques used in different phases of the recognition system of the iris image. The researchers also reviewed the methods associated with each phase. The recognition system is divided into seven phases, namely, the acquisition phase in which the iris images are acquired, the preprocessing phase in which the quality of the iris image is improved, the segmentation phase in which the iris region is separated from the background of the image, the normalization phase in which the segmented iris region is shaped into a rectangle, the feature extraction phase in which the features of the iris region are extracted, the feature selection phase in which the unique features of the iris are selected using feature selection techniques, and finally the classification phase in which the iris images are classified. This article also explains the two approaches of iris recognition which are the traditional approach and the deep learning approach. In addition, the researchers discuss the advantages and disadvantages of previous techniques as well as the limitations and benefits of both the traditional and deep learning approaches of iris recognition. This study can be considered as an initial step towards a large-scale study about iris recognition.

2.7.1 Advantage

- Improving classification accuracy

2.7.2 Disadvantage

- Not usable in single face image scenarios.

2.8 Iris liveness detection using regional features

Author:Y. Hu, K. Sirlantzis, and G. Howells,
Year of Publishing:2016.
Paper Type:IEEE Transaction Circuits System Video Technology

In this study, we use regional features to detect iris liveness. The relationship between the features in neighbouring regions is used to design regional features. They essentially capture the distribution of features amongst nearby regions. Through the use of two models—the spatial pyramid and the relational measure—which look for feature distributions in regions of variable size and form, respectively, we generate the regional features. The spatial pyramid model models a local to global feature distribution and extracts features from coarse to fine grid regions. The global distribution contains the information that is more resistant to translational transform, whereas the local distribution captures the local feature fluctuations. The feature-level convolution technique presented in this study serves as the foundation for the relational measure. We can get the feature distribution in regions with various shapes by changing the convolution kernel's shape. They fuse the outcomes based on the two models at the score level to merge the feature distribution data in areas of different size and shape. Experimental findings on benchmark datasets show that the suggested strategy outperforms state-of-the-art features in terms of performance.

2.8.1 Advantage

- Very high accuracy

2.8.2 Disadvantage

- Higher level of cooperation

2.9 Design and Analysis of Deep-Learning Based Iris Recognition Technologies by Combination of U-Net and EfficientNet

Author: Cheng-Shun Hsiao; Chih-Peng Fan; Yin-Tsung Hwang

Year of Publishing: 12 May 2021

Paper Type: 2021 9th International Conference on Information and Education Technology (ICIET)

In this paper, the effective deep-learning based methodology is developed for iris biometric authentication. Firstly, based on the U-Net model, the proposed system uses the semantic segmentation technology to localize and extract the region of interest (ROI) of iris. After the ROI of iris in the eye image is revealed, the inputted eye image will be cropped to the small-size eye image with the just-fitted ROI of iris. Then, the iris features of the cropped eye image are strengthened optionally by adaptive histogram equalization or Gabor filtering process. Finally, the cropped iris image is classified by the EfficientNet model. By the Chinese Academy of Sciences Institute of Automation (CASIA) v1 database, the proposed deep-learning based iris recognition scheme reaches the recognition accuracies up to 98%. Compared with the previous works, the proposed technology can provide the effective iris recognition accuracy for the biometrics applications with iris information. The application of biometrics technology in all areas of people's lives in today's intelligent era. With the advantages of high accuracy and contactless, iris recognition is an important and challenging research area. In this work, an application of the combined network model based on EfficinetNet-b0 is presented in iris recognition, which integrates iris segmentation, normalization, iris feature extraction and matching into a unified network. The network model has high parameter efficiency and speed. Compared with previous deep iris recognition network, the network architecture has three characteristics: (1) Compared with most existing training and phase adjustment algorithms, it is end-to-end trainable. (2) Grad-cam has class recognition and high resolution. It provides a good visual interpretation. (3) An effective and smaller baseline model is proposed that balances the depth, width and resolution of the network based on the scaling model and achieves better results. The hybrid iris databases, composed of CASIA Thousand and Mmu2, proves that the accuracy and efficiency of the composite network framework are better than those of the previous network framework. The visualization of data sets is validated, which proves that the combined model is robust to iris image localization.

2.9.1 Advantage

- Computational simplicity as the operator can be realized

2.9.2 Disadvantage

- High false non match

2.10 Local phase quantization for blur-insensitive image analysis

Author:E. Rahtu, J. Heikkilä, V. Ojansivu, and T. Ahonen

Year of Publishing:2012

Paper Type:International Workshop on Local and non-local approximation in image processing.

Blur is one of the main reasons for deteriorating image quality. This frequent occurrence is typically brought on by faulty optics or camera motion, and it is very challenging to reverse. In addition to degrading visual quality, blurring interferes with computer vision algorithms. In this study, we provide a straightforward but effective picture descriptor that is resistant to the most typical image blurs. The suggested technique can be utilised to describe the underlying image texture because it is based on quantizing the phase data of the local Fourier transform. We demonstrate how to create several iterations of our descriptor by adjusting the method for local phase estimation and making use of the suggested data decorrelation methodology. In experiments on face and texture recognition, the descriptors are evaluated. We demonstrate how to create several iterations of our descriptor by adjusting the method for local phase estimation and making use of the suggested data decorrelation methodology. The descriptors are evaluated in studies on face and texture recognition, and the outcomes are compared with other cutting-edge techniques. In the case of hazy photos, the divergence from the baseline is significant, but our method also performs quite well with sharp images.

2.10.1 Advantage

- Long term stability

2.10.2 Disadvantage

- The weaker insensitivity to blur.

2.11 An End to End Deep Neural Network for Iris Recognition

Author: Qingqiao Hua , Siyang Yina , Huiyang Ni a , Yisiyuan Huanga

Year of Publishing:2019.

Paper Type: 2019 International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI2019)

Whenever people pay for mobile phones, use ATM, log on to websites, pass security checks, or enter the security domain, they cannot operate without authentication. Biometric features (fingerprints, iris, face) are widely used in identity authentication because of their uniqueness, lifelong invariance and security. Common biometrics technologies include face recognition[3], iris recognition, speech recognition, object recognition and so on. Nevertheless, iris recognition is more reliable than face and fingerprint recognition, and has non-invasive and stability . It was first proposed by Burchan ophthalmologist, and various iris recognition techniques have merged since then. Now the main flow of iris recognition]is: (1) iris image acquisition. Iris image acquisition is that ordinary cameras can not capture clear iris texture, because people's iris physical size is relatively small, and need some near infrared light cooperation. (2) Iris image processing. It needs to be effectively segmented and normalized. (3) Iris image feature comparison. Traditional iris recognition methods require users to cooperate actively and recognize according to the instructions. Therefore the user experience is very poor. Compared with traditional feature recognition algorithms, the biggest advantage of in-depth learning is to improve the robustness and generalization ability of the model to image noise on the premise of improving the accuracy The reference of deep learning makes the requirement of iris recognition system for image quality less strict than that of traditional algorithms. Deep learning is a data-driven recognition process and adds the collected image samples of eye deflection, occlusion and attitude change. The training model can recognize iris features very high accuracy. Our main work is to propose a end-to-end deep neural network for iris recognition, which is superior to traditional iris recognition algorithms in accuracy and efficiency, such as wavelet transform , SVM, Resent, SeNet, and so on. It has good robustness to the experimental databases.

2.11.1 Advantage

- Fast processing

2.11.2 Disadvantage

- Not exactly easy to use.

2.12 CNN hyperparameter tuning applied to iris liveness detection

Author: G. Y. Kimura, D. R. Lucio, A. S. Britto, Jr., and D. Menotti.

Year of Publishing:2020.

Paper Type:15th International Conference on Computer Vision Theory and Applications.

Due to its high level of stability and distinctiveness, the iris pattern has substantially enhanced the field of biometric detection. Such a physical characteristic has been crucial in security and other relevant fields. But using artefacts like printed images, fake eyes, and textured contact lenses, presentation attacks, also known as spoofing techniques, can be utilised to get around the biometric system. Numerous liveness detection techniques have been suggested to increase the security of these systems, and the first International Iris Liveness Detection Competition was held in 2013 to assess their efficacy. In this article, we suggest adjusting the CASIA algorithm's hyper parameters. The Chinese Academy of Sciences submitted the CASIA algorithm to the third Iris Liveness Detection competition in 2017. With 8.48% Attack Presentation Classification Error Rate (APCER) and 0.18% Bonafide Presentation Classification Error Rate (BPCER) for the evaluation of the combined datasets, the improvements suggested led to an overall improvement. On the assessed datasets, other threshold values were evaluated in an effort to lessen the trade-off between the APCER and the BPCER, and they were successful.

2.12.1 Advantages

- Highly susceptible to presentation attacks
- Less expensive and less intrusive to the user

2.12.2 Disadvantage

- Rate high cost

2.13 Deep learning-based feature extraction in iris recognition: Use existing models

Author:A. Boyd, A. Czajka, and K. Bowyer
Year of Publishing: 2020
Paper Type:15th International Conference on Computer Vision Theory and Applications

For the problem of iris recognition, modern deep learning approaches can be used to produce efficient feature extractors. The question then arises: should we train such structures from scratch on a huge dataset of iris images, or is it preferable to tweak the current models to make them more suitable for a different domain? In this work, we investigate whether iris-specific feature extractors outperform models trained for non-iris tasks using five distinct sets of weights for the well-known ResNet-50 architecture. An independent dataset from the samples used to train the ResNet-50 model is utilised to test the classification accuracy attained by a Support Vector Machine. Features are retrieved from each convolutional layer. We demonstrate that the best training method is to adjust a pre-made set of weights to the iris recognition domain. In comparison to a model trained from scratch with pre-made weights, this method produces better accuracy. Comparing the winning, fine-tuned strategy to earlier work, in which only generic (not fine-tuned) models were utilised for iris feature extraction, also reveals an improvement in performance. Along with this work, we make the top-performing ResNet-50 model, which has been improved using more than 360,000 iris photos, available to the public.

2.13.1 Advantage

- Complexity and improving the efficiency

2.13.2 Disadvantage

- Lower accuracy

2.14 Fusion of handcrafted and deep learning features for large-scale multiple iris presentation attack detection.

Author:D. Yadav, N. Kohli, A. Agarwal, M. Vatsa, R. Singh, and A. Noore
Year of Publishing:International Conference on Computer Vision and Pattern Recognition - Workshop on Biometrics.

Presentation attacks like textured contact lenses, print attacks, and artificial iris pictures may make iris identification systems susceptible. The need for effective presentation attack detection algorithms has increased as iris recognition applications expand. In this research, we offer a unique approach that combines manually created and deep learning-based features to detect iris presentation attacks. To encapsulate the textural differences between actual and assaulted iris images, the proposed technique combines local and global Haralick texture features in a multi-level Redundant Discrete Wavelet Transform domain with VGG features. A huge iris dataset with more than 270,000 real and compromised iris photos is used to thoroughly test the proposed technique, which results in a total error of 1.01%. The experimental evaluation shows that the suggested approach outperforms state-of-the-art techniques in terms of presentation attack detection performance.

2.14.1 Advantage

- Reliability

2.14.2 Disadvantage

- Low performance

2.15 Presentation attack detection for iris recognition system using NIR camera sensor

Author:D. Nguyen, N. Baek, T. Pham, and K. Park
Year of Publishing:24 April 2018.
Paper Type:International Journal of Computer Science and Network Security, VOL.21 No.12.

The iris recognition system has shown to be efficient for reaching a high recognition accuracy and security level when compared to other biometric recognition systems like fingerprint, finger-vein, or face. However, a number of recent investigations have shown that contact lenses with printed iris patterns or presentation attack pictures that are retrieved using high-quality printed images can mislead iris recognition systems. As a result, this potential danger has the potential to make iris recognition systems less secure. In this article, a new presenting attack detection (PAD) method using an image captured by a near-infrared light (NIR) camera is proposed for an iris recognition system (iPAD). We first used circular edge detection to localise the iris region of the input iris image in order to detect presentation attack images (CED). We used both handmade and deep learning-based methods to extract the image features depending on the outcome of the iris localisation. Using support vector machines, the input iris images were then divided into groups for actual and presentation attacks (SVM). We demonstrate the effectiveness of our suggested strategy in solving the iris recognition presentation attack detection problem and provide detection accuracy that is superior to earlier studies through extensive testing using two publicly available datasets.

2.15.1 Advantage

- High security

2.15.2 Disadvantage

- Computer vision problems

III. SYSTEM REQUIREMENTS

3.1 HARDWARE REQUIREMENTS

Processor	:	Intel i3
Clock Speed	:	3.0 GHz
RAM	:	2 GB
Hard Disk	:	500 GB
Keyboard	:	Standard Keyboard
Mouse	:	Standard Mouse
Monitor	:	18.5 Inch color Monitor

3.2 SOFTWARE REQUIREMENTS

Operating System	:	Windows XP
Front End	:	Python
Back End	:	My SQL

IV. SYSTEM ANALYSIS

4.1 EXISTING SYSTEM

Due to its low stability and uniqueness, liveness detection is Iris pattern recognition has substantially enhanced the biometric authentication field in the current system. The significance of access to vast and diverse training datasets, including a large number of PAI species, is shown by the significant disparities in accuracy among baseline systems that were trained with significantly different data. utilising algorithms to efficiently collect all th checking and accurately identify genuine presentations. By inverting the algorithm adds inverted notion given by networks like ResNet, MobileNetV2 adds inverted residual connections between the bottlenecks. In comparison to its predecessor, MobileNetV2 features help to accelerate feature learning, increase network accuracy, and decrease the number of network parameters. In this study, a customised version of MobileNetV2 was employed to identify genuine and malicious presentation images.

4.1.1 Disadvantages

- Hacking with the iris unlock system can be possible
- Unreliable and low accuracy
- Iris recognition system may have to handle multiple kinds of presentation attacks, including unseen species.

4.2 PROPOSED SYSTEM

Due to its great stability and uniqueness, the proposed Iris pattern recognition has significantly enhanced the biometric authentication field in liveness detection. The significance of access to vast and diverse training datasets, including a large number of PAI species, is shown by the significant disparities in accuracy among baseline systems that were trained with significantly different data. utilising PAD algorithms to accurately recognise genuine presentations. The new features included in MobileNetV2 are intended to speed up feature learning, increase network accuracy over its predecessor, and decrease the number of network parameters. To collect as many attacks as possible and to detect genuine and attack presentation images, a modified version of MobileNetV2 was employed in this study. As a result, finding the best composite of these traits remains a crucial task. a score-level combination of numerous binarized statistical image feature (BSIF) and DenseNet-based features, two different domain-specific features. Six major iris traits are statistically tested after being examined randomly in order to choose the best feature set to combine. The presentation using textured lenses targets the many types of contact lenses found in the iris samples. First, the MobileNetv2a network processes the iris image to determine whether it is a real or fraudulent image. If authentic, the input iris class is trained against several classes, such as live, printed, contact lenses, etc., to determine whether it is a real presentation or an attack presentation. This method focuses more on finding the genuine class than it does on enhancing the identification of presentation attack tools.

4.2.1 Advantages

- The largest iris presentation attack database was created by integrating multiple other databases, it is more trustworthy and robust.
- Improved detection of presentation attack instruments
- This system better adapts to the new anti-spoofing problem

V. SYSTEM DESIGN

5.1 ARCHITECTURE OF THE PROPOSED SYSTEM

System design is the process through which the requirements are translated into representation of the system. The system architecture is shown in figure 5.1

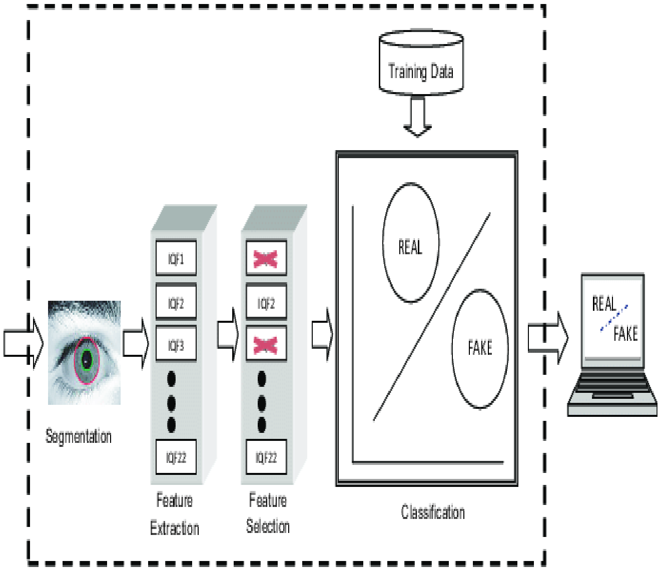

Figure 5.1 Architecture Diagram

The system architecture is shown in figure 5.1 First Segmentation is done on the given input. Then the segmented output obtained is fed for Feature Extraction. The resultant from Feature Extraction is given for Feature Selection. The output from that phase is given for Classification. Then the Fake or real one will be identified.

5.2 FLOW DIAGRAM

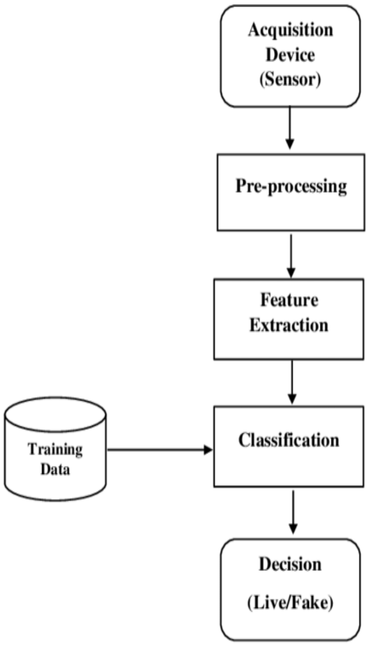

Figure 5.2 Flow Diagram

Initially, the iris image must be uploaded to the system. The uploaded image is then subjected to Segmentation procedure. The Segmented image obtained as output will be loaded for Normalization procedure. The normalized iris image is then given as input for Feature Extraction that is the Selection procedure. The extracted feature will be in turn subjected to Classification. The Real and the Fake can be identified by this classification process. Finally the whole process is terminated.

VI. RESULT AND DISCUSSION

The results show that approach presented in this work takes into account the variability of the attack presentation images, and the number of images per class. These images present a problem for the classifier because the PAI species are not equally represented for instance only five images of cadaver eyes were available for LivDet-Iris 2020. Considering this imbalance, our strategy is primarily focused on classifying bona fide images with high precision first, and attack presentation images second. Therefore, our first approach was training a network with only two classes. Then, a second network was trained from scratch with three and four classes, increasing the number of filters and weighting each class according to the numbers of images per species. To study these limitations and improve performance for these aforementioned scenarios, five experiments were developed in order to analyze the best hyper parameter configuration of MobileNetV2. A combination of serial and parallel DNNs was used, trained from scratch. A grid search was used to determine the learning rate, number of epochs, global pooling operation, alpha value, and input size of images. All the experiments employ the CLAHE algorithm and the class weight balancing operation. All the networks were trained with a limit of 200 epochs, using an early stopping method in case the measured performance would stop improving. In this section we compare our framework against the SID descriptor the convolutional neural network method , the dense SIFT Descriptor, the DAISY descriptor and the LCPD descriptor. Here we list the performance in terms of average classification error on the Iris dataset and the cosmetic lens datasets. With respect to the current best performing methods we obtained a 0% error for the Iris-2013-Warsaw dataset, in line with the SID descriptor of For the Cogent and Vista datasets we get the lowest average classification error, especially, for Vista with an improvement of 72% with respect to the state-of-the-art .

VII. CONCLUSION

In this project based on the assumption that the system encounters a specific iris presentation attack. Here we introduced a framework for iris liveness detection which embeds the recent advancements in deep metric learning. We validated the effectiveness of our approach in scenarios where the iris acquisition system has been violated by photo-based and contact lens attacks. The approach is able to work in real-time and has a better accuracy over the state-of-the-art on two test benchmark datasets. In conclusion, we point out that the employment of software based liveness detection systems should never give a sense of false security to their users. As in other areas such as cyber security, the attackers become more resourceful every day and new ways to fool a biometric system will be discovered. Therefore, such systems should be constantly updated and monitored, especially in critical application such as airport controls. Future work will involve considering different kind of attacks, such as eyes extracted from cadavers. Experiments will be performed on larger datasets considering subjects of different age, sex and ethnicity that are acquired under different time periods, environments and using a variety of sensors with a multitude of spoofing attacks simulations.

REFERENCES

[1] J. K. Meenakshi, G. Maragatham, "An Optimised Defensive Technique to Recognize Adversarial Iris Images Using Curvelet Transform," An optimised defensive technique to recognize adversarial iris images using curvelet transform," Intelligent Automation & Soft Computing, vol. 35, no.1.

[2] Kaiming He, Xiangyu Zhang, Shaoqing Ren, Jian Sun," 2 Deep Residual Learning for Image Recognition," IEEE Conf. on Computer Vision and Pattern Recognition, Las Vegas, NV, USA, pp. 770–778, 2016.

[3] Raniyah Wazirali, Rami Ahmed," Hybrid Feature Extractions and CNN for Enhanced Periocular Identification Dur.ing Covid 19," Healthcare Intelligence using Deep Learning and Computer Vision Workshops, 2021

[4] Vahid Nazmdeh; Shaghayegh Mortazavi; Daniel Tajeddin; Hossein Nazmdeh; Morteza Modarresi Asem ," Iris Recognition; From Classic to Modern Approaches," 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), 2019.

[5] Joseph McGrath, Zhaoyuan Fang, Aidan Boyd, Sébastien Marcel, Mateusz Trokielewicz, Piotr Maciejiz, Kevin Bowyer, Adam Czajka, Stephanie Schuckers, Juan Tapia, Sebastian Gonzalez, Meiling Fang, NaserDamer, Boutros, ArjanKuijper, Renu Sharma, Cunjian Chen, Arun Ross," Iris liveness detection competition (LivDet-Iris)",IEEE International Joint Conference on Biometrics, 2020.

[6] Nada A. Alhamdi, Mohamed B. Aldebri;,Moad H. Alkout," Iris Recognition Using Artificial Neural Network,"IEEE 2nd International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA),2022.

[7] Jasem Rahman Malgheet,Noridayu Bt Manshor,and Lilly Suriani Affendey," Iris Recognition Development Techniques," 24th International Conference on Iris Pattern Recognition,2021.

[8] Y. Hu, K. Sirlantzis, and G. Howells," Iris liveness detection using regional features," IEEE Transaction Circuits System VideoTechnology,2016.

[9] Cheng-Shun Hsiao; Chih-Peng Fan; Yin-Tsung Hwang," Design and Analysis of Deep-Learning Based Iris Recognition Technologies by Combination of U-Net and EfficientNet", 2021 9th International Conference on Information and Education Technology (ICIET),2021.

[10] E. Rahtu, J. Heikkilä, V. Ojansivu, and T. Ahonen," Local phase quantization for blur-insensitive image analysis,"International Workshop on Local and non-local approximation in image processing,2012.

[11] Qingqiao Hua , Siyang Yina , Huiyang Ni a , Yisiyuan Huanga," An End to End Deep Neural Network for Iris Recognition,"International Conference on Identification, Information and Knowledge in the Internet of Things,2019.

[12] G. Y. Kimura, D. R. Lucio, A. S. Britto, Jr., and D. Menotti," CNN hyperparameter tuning applied to iris liveness detection," 15th International Conference on Computer Vision Theory and Applications,2020.

[13] A. Boyd, A. Czajka, and K. Bowyer," Deep learning-based feature extraction in iris recognition: Use existing models," 15th International Conference on Computer Vision Theory and Applications,2020.

[14] D. Yadav, N. Kohli, A. Agarwal, M. Vatsa, R. Singh, and A. Noore." Fusion of handcrafted and deep learning features for large-scale multiple iris presentation attack detection," International Conference on Computer Vision and Pattern Recognition - Workshop on Biometrics,2018.

[15] D. Nguyen, N. Baek, T. Pham, and K. Park," Presentation attack detection for iris recognition system using NIR camera sensor,"International Journal of Computer Science and Network Security, VOL.21 No.12,2018.