A Practical Design for Face Recognition with Anti-Spoofing Based on Non-Visible Light Cameras

Songnan Xi[1, *], Lingbo Yang[2] and Yao Zhao[2]

[1] School of Information, Beijing Wuzi University, Beijing, China
[2] Tianjin All New Intelligence Ltd, Tianjin, China
[*]Corresponding author e-mail: xisongnan@163.com

ABSTRACT. *As one of the most promising artificial intelligence technologies, face recognition technology has been traditionally associated with security and has recently expanded into other industries such as retail, marketing, health, etc. A challenging issue for face recognition is face spoofing where imposters use a variety of fake faces in an attempt to deceive the face recognition systems. Extensive research has been conducted on face anti-spoofing algorithms and systems. Some researchers tend to design highly advanced and thus complicated algorithms assuming that regular visible light cameras are used so as to reduce peripheral hardware cost. However, implementation of such complicated algorithms may need support of quite advanced processing hardware which costs even much more than what has been saved by the cameras. Furthermore, such designs are not suitable for some practical application scenarios where the space is compact and small distributive devices without super computation strength and with low power consumption have to be used. Complicated algorithms also come with decrease in stability and generalization. An effective solution to reduce algorithms complexity is to capture images using thermal cameras which are inherently convenient for detecting various presentation attacks (PA). Sole rely on thermal cameras would need very high resolution thermal lens and thus bring the problem of much increased hardware cost. Based on extensive study on existing related work and electromagnetic theories and our experience in related practical projects and products, we proposed a practical design for face recognition with anti-spoofing. In our design, a low resolution thermal camera works together with a near infrared camera for face anti-spoofing and recognition. This design is believed to fight PA effectively and recognize faces accurately with relatively low cost and compact devices. These features add to our design's competitive strength in practical applications.*

KEYWORDS: *face recognition, anti spoofing, non-visible light cameras*

1. Introduction

Face recognition, as one of the most promising artificial intelligence (AI) technologies, has been widely used in all sorts of applications, ranging from traditional identity authentication to modern financial payment [1]. Face recognition can also serve as a natural and convenient interface between humans and the internet of things (IOT). With the development of the face-recognition technology, face spoofing also develops where imposters use a variety of fake faces in an attempt to deceive the face recognition systems. Mostly used spoofing methods, also referred to as presentation attacks (PA), are print attack, where attackers use someone's photos printed on paper or displayed on a digital device, replay/video attack, where a footage of face video is replayed on digital devices, and mask attack, where a three dimension (3D) mask is used to resemble the real faces.

Face spoofing detection, also known as face de-spoofing or face anti-spoofing [2, 3, 4], plays a vital role in practical application of face recognition.

A camera is an optical that captures still images or records moving images. It captures light photons, usually from the visible spectrum for human viewing, but in general could also be from other portions of the electromagnetic spectrum. Before moving on to discuss about details of face anti-spoofing algorithms, let us clarify technical terms to refer to different types of cameras and also introduce their specific properties.

Cameras that capture visible spectrum light are what we are mostly familiar with and also are the most common type of cameras. Usually， if one use the word of camera itself alone, he or she is referring to this common type of cameras. Sometimes, in order to emphasize its visible spectrum, the term of visible cameras is used. However, this term may be misunderstood as a camera that is not hidden and can be seen to people, as in contrast with the hidden cameras. Thus, for better clarification, the term of visible light cameras is adopted in this work. And all the other types of cameras that can detect lights from other portions of the electromagnetic spectrum can be referred to as non-visible light cameras. Near infrared (NIR) cameras and thermographic cameras are among non-visible light cameras. A thermographic camera is also known as an infrared camera or thermal imaging camera or infrared thermography. Thermal cameras are also often used for both simplicity and clarification and are what we will use in this work.

The visible light is within the wavelength range of 400-700 nanometers (nm). Near infrared (NIR) cameras detects the light of the spectrum referred to as near-infrared to distinguish it from far-infrared, which is the domain of thermal imaging. Wavelengths used for NIR photography range from about 700 nm to about 900 nm. The thermal cameras operate in wavelength as long as 14,000 nm.

Visible light cameras are not as robust as NIR for face recognition. Unlike visible light, there is almost no NIR radiation in a natural environment. So for NIR photography, certain NIR light source is usually used so that the objects will reflect enough NIR signals for the cameras to detect. This NIR light source is called complementary NIR source. Although this increases hardware cost a little bit, NIR images bring more advantage in the sense that they will not be affected by the ambient situation as much as visible light images and consequently more robust in face recognition or anti-spoofing. To be more concrete, for the same person or the same face, features of the ground-truth visible image may be quite different from that of the to-be-detected true image since these two images are highly likely taken in different environment with different visible light situation. As a result, it is quite likely that the same person would not be detected to be himself or herself. In contrast, due to little inference of near infrared light from the natural environment, NIR images are basically determined by the complementary NIR light source and thus there is no obvious difference between the ground truth image and to-be-detected image no matter what the ambient situation is.

Thermal cameras detect radiation determined by the temperature of the objects, so as with NIR cameras, the ambient light level does not matter. To be even better than NIR, sine human faces emit thermal emission voluntarily, thermal cameras don’t need complementary light source and can work even in total darkness.

From the perspective of face anti-spoofing, another disadvantage with visible-light is that feature difference between fake faces of presentation attack and live faces is much less obvious than features of fake and live face images of NIR cameras and thermal cameras. After all, we can see the same face of a person via visible light, no matter it is a live face or the face or a piece of paper or screens. Difference using thermal cameras is even larger than that of NIR images, since a piece of paper or screens usually don’t have the same temperature as human bodies.

2. Existing Research of Face Recognition with Anti-spoofing Based on Visible Light Cameras

Visible-light cameras are much more familiar to us than non-visible light cameras and consequently are of great interest to early study on face recognition or face anti-spoofing algorithms.

At first, research resorted to handcrafted traditional features that are discriminative enough between real live faces and certain presentation attacks so as for the classifier to make judgement [5, 6].

With the development and successful application of artificial intelligence (AI) technologies, especially since the introduction of AlexNet in 2012 [7], deep learning algorithms have been adopted in face anti-spoofing research [8]. At first, due to the lack of enough training image data in public dataset, deep learning methods were unable to work as well as the handcrafted feature face spoofing detection. Breakthrough was not achieved until the year of 2018 when [2] was published on CVPR. In this paper, authors proposed to fight print and replay attack using the depth map and mask attack by detecting the physiological features such as the heart rate via remote photo-plethysmography (rPPG) signals. The performance was superior to that of handcrafted feature methods for the first time.

One issue with these advanced face anti-spoofing algorithms is their complexity, which is caused by the less robustness and image feature difference using visible-light photography, as presented in the introduction section. Such complicated algorithms need highly powerful processing hardware to support huge loads of computation, which results in large increase in total hardware cost. Besides, high performance processing hardware, such as graphical processing unit (GPU), CPU and high-speed memory, makes it hard to deploy in a compact space and thus are not suitable for certain application scenarios, especially for embedded systems. For example, for an intelligent face recognition lock, it would be impractical to connect the lock with a computer with a powerful GPU to implement the face recognition algorithms.

Furthermore, the more complicated the algorithms are, the worse instability and generalization they can provide. High complexity also means high power consumption, which is another reason for these algorithms less practical.

With the improvement of a variety of non-visible light cameras in quality and decrease in their cost, less complicated algorithms are studied and proposed, as introduced in details in the following section.

3. Existing Research Based on Non-visible Light Cameras

Among all sorts of non-visible light cameras, such as thermal cameras and infrared cameras, thermal cameras who have the inherent advantage in discriminating fake and real faces and thus reduce the algorithms complexity has caught great attention of researchers. The temperature distribution pattern and feature of real faces are not easy to emulate and thus make thermal images an excellent choice for fighting PA.

In [9], thermal images, after some external knowledge being inserted, are fed into convolutional neural networks (CNN) for face liveness detection. The external knowledge is inserted by multiplying temperatures of pixels within reasonable real face temperature range. Consequently, the pixels corresponding to real faces are amplified and those corresponding to background or fake face are suppressed. This is similar to attention mechanism [10]. Simulation results in [9] verify the performance of face anti-spoofing based on thermal images.

Seminal research has been conducted in [11], where visible spectrum images are synthesized from thermal images via their multiple region synthesis algorithm where features are extracted from global and multiple local regions using a fully convolutional neural network (CNN). The obtained synthesized visible images are then used for face recognition. Their method allows for cross-spectrum matching and adjudication, which is of great significance.

Thermal camera based methods introduced above usually solely rely on thermal cameras, and thus high resolution and high quality thermal cameras have to be used to achieve good face recognition and anti-spoofing performance. This brings the issue of quite high hardware cost, which makes the algorithms not quite practical.

In some research, near infrared (NIR) cameras are used and their performance of fighting all types of PA is shown to be satisfactory [12, 13]. However, the issue of complexity still exits and thus limits their application in industrial embedded products.

We have also carried out tests on certain actual face recognition and anti-spoofing products based on NIR images. Although fake faces shown on screens can be perfectly detected, NIR shows not as good performance as in the presentation of fake faces printed on papers. The performance is even worse if the printed face is cut out of the paper.

4. Proposed Practical Design for Face Recognition with Anti-spoofing

As presented before, complication of the face anti-spoofing algorithms using regular visible light cameras is frowned upon, and these algorithms also have the problem of not being able to be applied in dark environments, such as in a bar or during nights. By resorting to high resolution thermal cameras, one can overcome some disadvantages with visible light cameras but still face the problem of high hardware cost. NIR cameras cost less than the thermal cameras and also considered for face anti-spoofing. As presented before, some algorithms using NIR cameras, although can fight against all types of PA, are computation consuming. Other algorithms can achieve excellent performance against certain types of presentation attacks. But NIR cameras alone are not able to fight all of attacks. So, we propose to adopt a low resolution thermal camera for face anti-spoofing. It costs much less than high resolution thermal cameras and still holds the advantages of thermal cameras in face liveness detection.

While NIR cameras may not be as ideal for face anti-spoofing as the low resolution thermal cameras, NIR images have been proved to be good enough for recognizing real faces. Excellent performance, combined with relatively cheap price, makes NIR cameras popular in certain practical face recognition embedded systems. Usually, NIR light source is used together with the NIR camera. Objects to be detected and recognized reflect NIR lights emitted from complementary NIR light source and generate NIR images that are to be captured by the NIR camera. In practice, NIR LED can be used as complementary NIR source.

With performance, cost and actual deployment in commercial products all considered, we propose a cascade face recognition with anti-spoofing design where both a low resolution thermal camera and an NIR camera are adopted. Figure 1 shows the process of the whole system and Figure 2 shows an example of how the thermal and NIR cameras are arranged, together with two NIR LED as the complementary NIR light source.

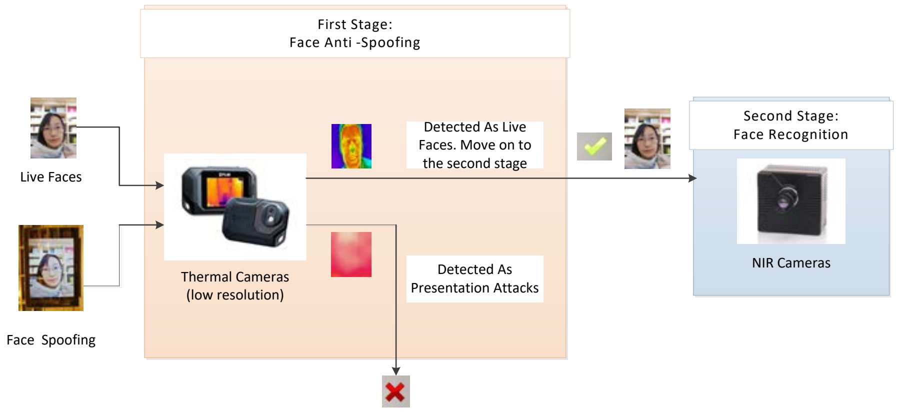

Figure. 1 Diagram of the proposed face recognition with anti-spoofing design for practical application

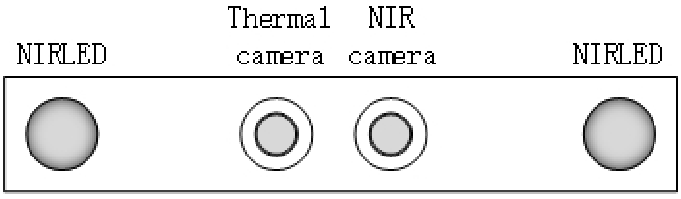

Figure. 2 Layout of thermal and NIR cameras and NIR LED

First, low resolution thermal images, captured by the thermal camera, are used to rule out all mostly used presentation attacks, allowing only real faces to be passed on to the second stage. In the second stage, near infrared images of real faces are used for accurate face recognition. As explained in details in the following, in our design, by working together with near infrared cameras in a cascade style, the resolution of the thermal camera does not need to be high and satisfactory performance can still be achieved using relatively simple algorithms. Thus total cost of both peripheral and processing hardware can be controlled to be within a reasonable range. This also means that the proposed design can be deployed in embedded systems. All these features make our design suitable for practical applications.

The features revealed by thermal images are quite discriminative between real faces and fake faces of print attack. Real human faces emit very strong signals within the detectable range of thermal cameras. In contrast, fake faces of print attack, no matter printed on or cut of paper, show almost no detectable signals on thermal images and thus can be easily detected even with low resolution thermal cameras. For replay attacks and fake faces shown on screens, either no obvious thermal images can be produced if the device is not warm enough to be near normal human face temperature, or when the device is intentionally heated to be as warm as human faces, the patterns of the thermal images would be quite different from that of real faces' thermal images. In either case of the replay attacks, low resolution thermal images are good enough to detect the attacks without involving complicated algorithms.

As for mask attacks, an imposter may wear a 3D mask covered with certain heating wires that are designed so as to ‘look’ like the temperature distribution of a real face. It is also impossible to capture enough features with sufficient accuracy. Since the change in the distribution is very slow, low resolution, such as 40 pixels by 30 pixels, would be good enough.

Due to the inherent advantages of thermal images, we can adopt support vector machine (SVM) or CNN for face anti-spoofing in the first stage of our design. The computation complexity of these algorithms can be sufficiently supported by the processing hardware in an embedded system face anti-spoofing algorithms.

5. Conclusion and Future Work

Researchers tend to start their study with something they are most familiar with and this is also true for the research of face spoofing detection where researchers have conducted a plethora of study on the visible light photography for face recognition, yet not as much study using non visible cameras. However, it happens that the best solution may lie in somewhere that is relatively new or strange to us. For example, while we naturally use decimal number system in our everyday life, binary, rather than decimal, is the ideal number system for computers. Recent research has revealed the advantage of NIR and thermal cameras in face recognition and face anti-spoofing.

As analyzed in details in this work, with NIR or thermal cameras, we can adopt relatively simple face recognition with face anti-spoofing algorithm. This brings multiple advantages. Less complicated algorithms have better stability and generalization capability. We do not have to rely on high performance processing hardware and thus decrease the hardware cost. Furthermore, this enables the implementation of the algorithm on devices as small and light-weight as an embedded system. Less complexity also means less power consumption.

To make the best of the advantages of both NIR and thermal cameras, both types of photography are used in our proposed design. Furthermore, from the perspective of practical industrial products, satisfactory performance needs to be achieved with at as low as possible cost. After careful study and consideration, we have decided to use low resolution thermal cameras to further lower hardware cost. Due to the fact that a great deal of difference exits between thermal images of live faces and fake faces, low resolution thermal cameras will be good enough for detecting face spoofing. NIR cameras, on the other hand, bring no extra cost compared with regular visible light cameras since NIR images can actually be detected by using the same image sensors as for the visible images.

Combining literature survey and analysis of related work and our testing experience and results of an industrial face recognition based intelligent lock product, we have proposed a cascade design where a low resolution thermal camera is used in the first stage for face liveness detection and then in the second stage, NIR images are captured by an NIR camera with the complementary light source from two NIR LEDs at each side are used for face recognition.

We have up till now concentrated more on the qualitative aspects of the proposed design. To make it complete and ready to be deployed in practice, we are going to carry out study to determine the quantitative aspects. To begin with, as for the low resolution thermal cameras, we are going to determine the specific values of the lowest resolution that is acceptable. We have proposed this design based on our analysis of existing literature and experience in real application and we believe the complexity of the algorithms to adopt will be much lower. Nevertheless, we haven't determined the specific architecture and detailed algorithms for face anti-spoofing and recognition. This is on-going in our work.

Acknowledgements

This work is funded by the Beijing Wuzi University Youth Foundation with project number of 2018XJQN02, and funded by intelligent logistics system Beijing Key Laboratory (No. BZ0211) and Beijing Intelligent Logistics System Collaborative Innovative Center.

References

[1] https://emerj.com/ai-sector-overviews/facial-recognition-applications/.

[2] Yaojie Liu, Amin Jourabloo, Xiaoming Liu, Learning Deep Models for Face Anti-Spoofing: Binary or Auxiliary Supervision, CVPR2018

[3] Jiangwei Li, Yunhong Wang, Tieniu Tan, A.K.Jain. Live face detection based on the analysis of fourier spectra. In SPIE (BTHI),volume 5404, pages 296–304, 2004.

[4] Yaojie Liu, Joel Stehouwer, Amin Jourabloo, Xiaoming Liu. Deep Tree Learning for Zero-shot Face Anti-Spoofing, CVPR2019

[5] Zinelabidine Boulkenafet, Jukka Komulainen, Abdenour Hadid. Face Spoofing Detection Using Colour Texture Analysis. IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, 2016.

[6] Zinelabidine Boulkenafet, Jukka Komulainen, Abdenour Hadid. Face Antispoofing Using Speeded-Up Robust Features and Fisher Vector Encoding, IEEE SIGNAL PROCESSING LETTERS, 2016.

[7] Alex Krizhevsky, llya Sutskever, Geoffrey E. Hinton. ImageNet Classification with Deep Convolutional Neural Networks. In Advances in neural information processing systems 25 (2).

[8] Zhenqi Xu. Learning Temporal Features Using LSTM-CNN Architecture for Face Anti-spoofing, 2015 3rd IAPR.

[9] Jongwoo Seo, In-Jeong Chung. Face Liveness Detection Using Thermal Face-CNN with External Knowledge. Symmetry 2019, 11, 360.

[10] S. Woo, J. Park, J.-Y. Lee, and I. S. Kweon, “Cbam: Convolutional block attention module,” in Proc. ECCV, 2018.

[11] Benjamin S. Riggan, Nathaniel J. Short, Shuowen Hu. Thermal to Visible Synthesis of Face Images using Multiple Regions. arXiv: 1803.07599

[12] Javier Hernandez-Ortega, Time Analysis of Pulse-based Face Anti-Spoofing in Visible and NIR, CVPR2018 workshop.

[13] Xudong Sun, Context Based Face Spoofing Detection Using Active Near-Infrared Images, ICPR 2016.