Biometrical verification based on infrared heat vein patterns

Elnaz Mazandarani¹, Kaori Yoshida², Mario Köppen³, Ulrike Lucke⁴

¹University of Potsdam, Department of Computer Science, Potsdam, 14482, Germany
²Kyushu Institute of Technology, Department of Computer Science and Electronics, Iizuka, 820-8502, Japan

Abstract

In this paper, we provide the idea of analyzing the infrared heat vein patterns in the palm dorsal (back of the hand) for biometric purposes. This work is motivated by making counterfeit of hand veins more difficult by using heat infrared vein pattern images with the appendant optical image. We present results of past experiments which demonstrate differences between NIR (near infrared) and FIR (far infrared) images and the difficulties of using FIR imaging for biometrical purposes. This paper will show step by step a possibility based on statistical histogram analysis to create a biometrical feature template using FIR imaging with thermographic information as initial images for creating a biometrical template. Furthermore we will present a functioning biometric system with a preliminary version of an achieved EER of 30%.

Keywords: far infrared, hand vein, biometrics, near infrared, equal error rate

1. Introduction

Internet is a solid part of today’s life. The World Wide Web is usable for almost every part of life like work, study, research, leisure, shopping or business known as e-commerce, e-learning, e-government etc. Internet is not only used by adults. 57% of all children in Germany are using the WWW daily for playing online games, learning, listening music or watching videos [1]. Other than activities of the adult’s world most of the online activities of children don’t even assume a user registration. Furthermore many online activities of adults cause automatically electrical contracts for example when booking a flight or buying a book online. That is the reason why personal verification has become an important technique and those activities are based on authentication systems.

In the whole internet no authentication or identification system for children does exist. The reason is actually very logical and simple. Person under full age are not allowed by law to close a contract. That is why a user authentication seems to be needless. But following we will present an example why a user authentication system for person under full age also should exist.

Beside all internet activities mentioned before the social networking is getting more popular among children. The same phenomena can be seen since years in the adult’s world. The social networking used by children are so called child chat. Kidschat.net and YouNow.com, are only two of them. Children are using those chats for social communication but also for presenting themselves. For example YouNow enables the children streaming life videos via internet which can be watched by any user [2]. That means YouNow enables other users to follow any video stream, write comments and ask questions life while another user is streaming a video of herself. Kids are sometimes very open to announce their personal information without having a control who is seeing the information. Child chats often don’t even need a registration before using. Although those chats are made for children users under 13 years old and over 21 years old are also active in child chats. Such child chats open a very new and easy channel for people with worse intentions or stalkers collecting personal information of children. Adults can find ways (for example by pretending being a child too) to win confidence and at the same time the control of the child [3]. This issue of establishing an emotional connection to a child with bad intention is called cyber grooming [3].

Adults can have different intentions to cyber groom. Following are three examples of cyber grooming:
(1) with the aim of child sexual abuse
(2) with the aim to make the child doing illegal things for example streaming copyrighted films or images. In this
case the adult force a child to do something illegal. Since the child is under full age it can’t be judged by law. The adults who are responsible for the child will be judged and forced to pay money as compensation for offending the copyright.

(c) with the aim to convince the child to buy something. For example recommending a ring tone and force the child to klick a link to buy it.

All examples show even if children under full age are not allowed to execute activities based on contracts like shopping it is still important to have an authentication system to safe children in internet or maybe open the way for more activities based on personal identification for younger users.

Many different technologies for user authentication and identification do exist [4]. Those systems are based on three different categories: Knowledge factor (user knows e.g. pincode, password), Ownership factor (user has e.g. ID card, credit card) or Inherence factor (physical or behavioral biometrical characteristics).

There is a difference between verification and identification. Verification or authentication handles the confirmation or denying a person’s claimed identity whereas identification refers to establish a person’s identity [5]. The ownership factor and inherence factor are used for identifying a person whereas the knowledge factor is mostly only used for verifying/authenticating a user like a login systems. Person under full age don’t fulfill the requirements of the ownership factor for an identification system. They are not in possession of items like a credit card on which those item based systems are based on. In case of under full age users only having the inherence factor is thinkable. That means the technique answering to this need is biometrics.

The science referring to metrics related to human physiological and behavioral characteristics for identifying a person is called biometrics [6]. Nowadays many different physiological and behavioral biometrical techniques do exist. Examples of physical biometrics include fingerprints, face, hand geometry, iris, retinal scans and DNA. Examples of behavioral biometrics include voiceprints, signatures and keystroke dynamics [5].

This paper is motivated by the need to create an identity authentication system for users under full age in order to open ways for new online activities but also to safe young users against people with bad intentions. Since the behavior of children is changing during their growth very fast and adults can learn to fake the behavioral of children (for example trying to write like a child) this paper focuses on physiological biometrics for protecting children in internet.

Among physiological biometrical techniques the hand vein pattern is attracting the interest of research community but also in industry. The acceptance for the hand based biometrics system received high attention over recent years because it is based on an internal feature. Most of the hands veins on the back of the hand (palm dorsal) are not visible because they are under the human skin which makes it extremely difficult to damage, modify, fake or counterfeit them. Hand vein biometrics becomes a promising technique for identification but also a method for proving liveness [4]. Another reason for increasing interest is that the hardware like scanners and cameras are getting more users friendly, smaller and cheaper.

This paper proposes the usage of heat infrared and matching optical images of the hand vein pattern in the palm dorsal to make the user verification safe against counterfeit. The thermographic information supports making sure that no other item than a living human hand is used. Fake scenes such as using a picture of a hand or a model of a hand with painted veins will be detected.

Extracting hand veins and creating a template used in biometric systems to enable a matching system for verification is mostly based on near infrared (NIR) imaging. This is nevertheless caused by the fact near infrared cameras have been the cheaper option than far infrared cameras. Further technical reasons will be discussed in later section of this paper. The propose of this paper is based on heat infrared images which makes the usage of far infrared (FIR) imaging necessary.

The paper will present the difference of NIR and FIR imaging and present a novel extraction method based on FIR imaging with thermographic information.

This paper is organized as follows: the following Section 2 will give a short definition of hand vein biometrics and an overview of infrared imaging. Section 3 will introduce the framework of the proposed biometrics system. The experiment and its results will follow in Section 4. The paper ends with a short conclusion section.
2. Related Work and preliminary experiment

The hand vein pattern recognition makes usage of infrared camera and scanners taking infrared images. For that purpose the palm dorsal has to be placed near a scanner or camera in order to take digital picture using infrared light. The result image is used to generate a reference template based on the location and shape of the veins structure. This biometrical feature template is saved in a database and used to compare it within verification with a new template.

2.1 NIR and FIR imaging

Infrared (IR) is electromagnetic spectrum with a longer wavelength and lower frequency than visible light [4]. IR is divided into three spectral regions which differ in the wavelength:

- near infrared (NIR), IR-A, short wave, 0.78-1.4 µm
- medium infrared (MIR), IR-B, medium wave, 3-8 µm
- far infrared (FIR), IR-C, long wave, 15-1.000 µm

NIR and FIR imaging are suitable for taking pictures of a human without danger and harm [4].

Fig. 1 shows sample FIR (left) and NIR (right) images. The hand veins of the NIR image are dark and easily to detect. This is caused by the hemoglobin in the blood. The hemoglobin absorbs the lights (760-1100 nm) of the short wavelength. The reflection effects that the veins appear black and become very clear visible in the picture. That is the reason why NIR images are mostly used to extract hand veins for biometric purposes. NIR images can be rather seen as extended optical information. Fig. 1 also shows a FIR image on the left. This image includes thermographic information but the veins are not as sharply visible as on the NIR image. The image itself is also not as sharp as in the NIR image. The FIR gets affected by the warmth of the superficial skin and also the surroundings. The effect of the surrounding is very clear on Fig. 2 and Fig. 3. Figure 2 shows two FIR images of the hands of one and the same volunteer. Figure 3 shows two FIR images of the palm dorsal of two different volunteers. Although the pictures are made at the same time and at the same place all images are very different. This is caused by the temperature of the environment, the brightness of the environment but also the skin temperature of the person itself.

Fig. 2. FIR images of same volunteer.

Fig. 3. FIR images of two different volunteers.

FIR imaging is less tolerant to changes of the environment and the body conditions than NIR [4]. The figures make clear that using a FIR image as initial images for extracting hand veins for creating a feature template to enable a matching system for verification as processed with NIR images is not possible. However the thermographic information of FIR imaging provides another option of creating a feature template, such as statistical histogram analysis. The steps of the pre-processing as basis of the statistical histogram analysis and its procedure to extract biometric features and the identification of the Equal Error Rate will be shown in the next section.

3. Proposed Framework

The proposed framework for verifying a user based on its hand veins consists of three parts, shown in Fig. 4.

A sensor/camera takes an infrared heat image of the palm dorsal of the human being. The result infrared image has to be improved within a pre-processing process. This pre-processing frames the first part of the system. After the pre-processing the biometrical feature template can be generated. This paper suggests using the statistical histogram analysis for this purpose. The generator uses information of heat image for creating a template. The
system requires thermographic information. Images with missing thermographic information are not permitted for further steps of the system. If heat information is missing, the system will refuse a user verification or even an enrollment of that user. This security feature makes it impossible to try to get verified by using a model or picture of a hand.

After creation of the feature template the third level of matching is enabled. The matching process compares the template with all saved templates in the database. If there is a matching between the current template and a saved and already enrolled user the current user will be verified.

Next, we will present the steps from taking pictures of hand and the pre-processing of the images as basis for feature template creation with statistical histogram analysis.

4. Experiment and Results

4.1 Image Acquisition

In this experiment, a FLIR- E8 device was used to make 256 levelled gray-scale format far infrared JPG images with resolution of 320 x 240 pixels for the contactless image acquisition.

13 volunteers were requested to put both of their hands on a prepared table such that the thumb touches the table. The distance between the hand and the camera was fixed to approximately 15 cm.

4.2 Image Segmentation

The first step of the pre-processing before creating a feature template is the image segmentation, shown in Fig. 5.

The easiest way of image binarization in order to receive a black and white image which represents foreground and background pixels is using threshold for image segmentation [8]. Pixels under or over the defined threshold value are converted in black or white pixels.

4.3 Contour Extraction

Before the extraction of key points of the image of the palm dorsal the segmented image is used as initial image to create a corresponding contour image as second step of the process. The result contour hand image is shown in Fig. 6.

4.4 Extraction of Key Points for the ROI

The third step of the pre-processing is the extraction of reliable key reference points for the region of interest (ROI) of the palm dorsal. For this purpose the pixels of the contour image are scanned from the left to the right. The first appearance of switchover from white to black pixel occurs is the first knuckle point. The first line where two transition of black to white pixel occur is the beginning of the region of interest (marked as x1/y1 and x2/y1 on Fig. 7). Once the points under the knuckles to the left and right are located three values of the ROI (x1, y1 and width) are delivered. The height of the ROI was fixed. The right picture of Fig. 7 shows the result ROI which can be used as bases of the biometrical feature extraction.

4.5 Feature Extraction and Detection of EER

The last step of the biometrical template generation is the extraction of biometrical features. This paper presents

---

**Fig. 4.** Framework of proposed biometrics system.

**Fig. 5.** Step one: Image segmentation using threshold.

**Fig. 6.** Step two: Image contour extraction.
the statistical histogram analysis as method for feature extraction and biometrical template generation for FIR imaging. For the template generation, the histogram of each extracted ROI will be analyzed by the proposed system. A histogram consists of 256 gray scale values. If each gray scale value is handled as a feature this would cause 256 features. But the process of matching between an actual template and a saved template in order to make a decision for acceptance or rejection based on 256 features is too long. So as to reduce the amount of features the 256 histogram features were bundled to 8 features with each consisting of 32 gray scale values.

Once the biometrical features are extracted the process of matching can be started. The 8 new determined features will be compared with 8 saved features of enrolled users. A user will be accepted by the biometrical system if the Euclidean Distance is less than a fixed threshold.

Fig. 8 presents the false acceptance and false rejection rates based on different thresholds for Euclidean Distance of two templates. The figure shows very clear that the error rate of false acceptance and false rejection is equal when the threshold is set to 0.55 (55%). Is the threshold 0.55 the Equal Error Rate is 0.35 (35%).

5. Conclusions

FIR imaging does not deliver images of hands of effectual sharpness and contrast as NIR imaging does. For that reason, this paper presented the statistical histogram analysis as method for feature extraction and biometrical template generation for heat infrared images of palm dorsal in order to verify a person based on hand vein pattern. In a further step we determined the EER of 35%. This EER forms the first biometrical evaluation but it is too high for a biometrical system. Very good biometrics have a EER << 1% (e.g. keystroke: 1%, voice: 6%). This EER has to be improved based on further work and experiments. Next will be a more correct feature extraction for example with Gabor features, and then use feature vectors to train a classifier, and evaluate performance.

Acknowledgment

This work was partly supported by the Japan Society for the Promotion of Science, Grant-in-Aid for Scientific Research (No. PE15705). We would also like to thank the Kyushu Institute of Technology and especially the students to taking part in the experiment.

References

(1) http://www.nwz-inside.de/News/Deine-Welt/Digitale-Welt/Hi-wie-gehts-Zieh-die-Hose-aus,46618 last retrieved on 15/05/11.
(2) http://www.stern.de/digital/online/younow-paedophile-lieben-diese-app-2170891.html last retrieved on 15/05/11.
(6) http://findbiometrics.com/solutions/vein-recognition/ last retrieved on 15/05/11.