Security evaluation of a finger vein authentication algorithm against wolf attack

Akira Otsuka*, Tetsushi Ohki*, Ryogo Morita†, Manabu Inuma‡, Hideki Imai†
*AIST, e-mail: otsuka@ni.aist.go.jp, tetsushi.ohki@aist.go.jp
†Chuo University, ‡Josai University, e-mail: inuma@josai.ac.jp

***Abstract*—Presentation attack against biometric authentication systems is getting attention by many researchers since the seminal paper[4]. In this paper, we consider a new kind of presentation attack called wolf attack. Wolf attack does not require biometric feature from a victim which the other presentation attacks does but synthesizes biometric feature from scratch by analyzing vulnerability in biometric matching algorithms. The concept of wolf attack was first introduced in [2]. In the same paper, it was theoretically shown that in a finger vein authentication algorithm[3], there exists a wolf biometric feature which perfectly impersonates any individuals. In order to show the real impact of the attack, in this paper, we demonstrate the first experimental wolf attack to the finger vein authentication algorithm[3], by conducting a presentation attack using the artificially synthesized wolf artifact to an experimental finger vein authentication system. As a result, the impersonation success probability (or WAP defined later) is observed more than 50[%] at a threshold which gives the equal error rate of 1.6[%].**

I. Wolf and Wolf Attack Probability

Une, Otsuka and Imai [2] defined the wolf attack as follows. Let S_A be a set consisting of all possible input values including ones generated from non-biometric objects such as artefacts or synthetic objects. Let T_h be a set consisting of templates generated from all human samples. Let COMP be a comparison algorithm employed in the comparison and decision subsystem, which takes input values $s \in S_A$ and a template $t \in T_h$ and outputs $match$ if s and t are decided to be close by a predetermined threshold, and returns $nonmatch$ otherwise.

Definition 1.1 (p-wolf): An input value s_w is called *p-wolf* if the probability that the comparison result of s_w with a human template is $match$ is equal to p, namely

$$\mathop{\mathrm{E}}_{t \in T_h} \Pr[\,\mathrm{COMP}(s_w, t) = match\,] = p.$$

In the following, we focus biometric verification (one-to-one authentication) systems.

Definition 1.2 (Wolf attack): Assume that the attacker satisfies the following two conditions.

(i) The attacker has no information of a biometric feature of a genuine user to be impersonated. Namely we assume that, in the verification phase, the attacker claims an identity chosen uniformly at random.

(ii) The attacker has complete information of the algorithms employed in the enrollment phase and the verification phase.

Wolf attack is defined as an attacker's attempt to impersonate a user by presenting a wolf to the sensor of the system.

Definition 1.3: Wolf attack probability, WAP, is defined as the maximum of the expected success probability of impersonation over all possible wolf objects.

$$\mathrm{WAP} = \max_{s_w \in S_A} \mathop{\mathrm{E}}_{t \in T_h} \Pr[\,\mathrm{COMP}(s_w, t) = match\,] \quad (1)$$

II. Finger vein authentication algorithm

The algorithm proposed by Miura et al.[3] consists of the following steps.

1) Capture images by near-infrared camera
2) Extract finger vein patterns from the captured images
3) Compare a pair of vein patterns
4) Make decision on the matching score

The essential part of the algorithm is that the near-infrared image is reduced to one third of its original size. In this process, pixels of 3×3 are compressed to one value. According to the number of pixels decided as vein pixels (black pixels) out of 9 pixels, the value for the i-th value x_i is determined as follows. The algorithm employs the resultant compressed image, which we call a finger vein pattern, as a biometric feature for comparison.

$$x_i = \begin{cases} 0 & \text{if 0-2 pixels are decided vein} \\ null & \text{if 3-6 pixels are decided vein} \\ 1 & \text{if 7-9 pixels are decided vein} \end{cases} \quad (2)$$

The dissimilarity score is defined over two vein patterns defined in (2) as follows:

$$R(x, x') = \frac{HD(x, x')}{\#\{i \,|\, x_i = 0\} + \#\{i \,|\, x'_i = 0\}} \quad (3)$$

where $x, x' \in \{0, 1, null\}^n$ represents the vein patterns of length n, and $HD(x, x') = \#\{i \mid |x_i - x'_i| = 1\}$ denotes the Hamming distance between x and x'. Note that

$$|null - 0| \;=\; |null - 1| \;= 0.$$

Then the comparison algorithm declares the input and enrolled vein patterns to match if the dissimilarity score is less than the predetermined threshold, and otherwise declares not to match.

III. Wolf attack experiment

A. finger vein capture

The finger vein capture equipment in Fig.1 is designed as described in [3]. The near-infrared LED array emits the NIR light transmits the finger and the image is captured by NIR camera device through band-pass filter with center wavelength of 800nm. The size of finger vein images is 198×78.

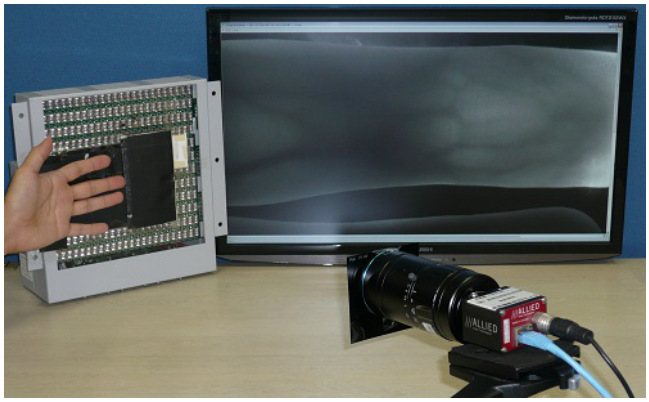

Fig 1. Camera and near-infrared illumination

B. Artificial wolf finger

The artificial wolf finger (Fig.2) consists of orange-colored rubber plates, white thin plastic plate and OHP sheet. White thin plastic plate is affixed on piles of orange-colored rubber plates, and OHP sheet is affixed on white thin plastic plate. In order to imitate the intensity of infra-red transmittance similar to the human fingers, we adjusted the thickness of orange-colored rubber plates. OHP sheet and white thin plastic plate are used is to reduce the noisy random pattern from the orange-colored plate. The wolf pattern is printed on a OHP sheet by a laser printer. The estimated resolution of camera on the wolf object is 130 dpi.

Fig.3 (a), (b) are the captured wolf feature and its extracted vein pattern. If we could input the original wolf feature in [2] to the sensor, extracted vein pattern will be totally filled with $null$ (ambiguous/gray) pixels, hence zero dissimilarity score against any vein pattern in equation (3). In the real experiment, it is not easy to make such an ideal wolf sample. As we see in Fig.3, some pixels are recognized as 0 (background) or 1 (vein) pixels by the feature extraction algorithm because of various noise and non-uniform light intensity.

Fig 2. Artificial finger

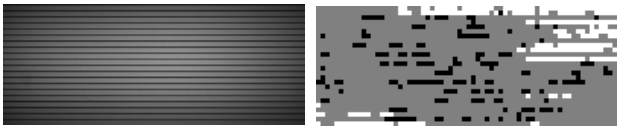

Fig 3. (a) wolf feature (b) Extracted vein pattern

C. Experimental Results

We performed the wolf attack experiment using the artificial wolf object against implemented finger vein authentication MNM algorithm.

Samples that we use the experiment are as follows.

- near-infrared images of 70 human fingers (4 images per each finger, 280 images in total)
- near-infrared image of the wolf artificial object (one image)

Fig.4 shows the score distribution of the experiment. Setting the decision threshold to 37, the genuine samples and imposter samples are separated with equal error rate of 1.6%. This is considered a moderate performance as an experimental biometric authentication system. The score distribution of the wolf image resides in the middle of genuine and imposter score distribution. The wolf image performs with significantly lower dissimilarity score than imposter images and with closer dissimilarity score to genuine images. With the same threshold of 37, the wolf image is accepted with probability 51.6% against 280 human finger images. Thus, 0.516-wolf was found.

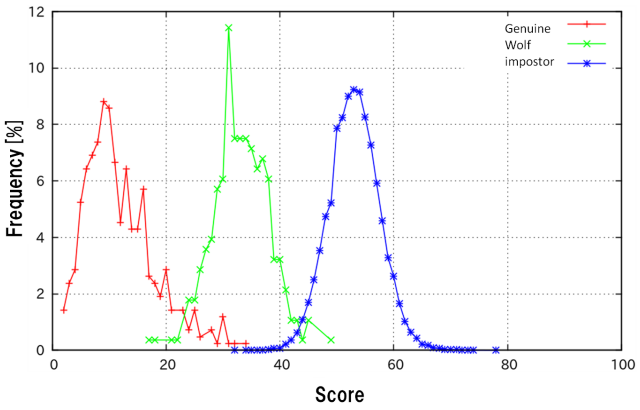

Fig 4. Score distribution

IV. Conclusion

In this study, we demonstrated wolf attack analysis to a finger vein authentication algorithm, by implementing an experimental finger vein authentication equipment and by presenting artificial wolf objects to the equipment. As a result, the impersonation success probability is observed 51.6% against the experimental system with equal error rate of 1.6%.

References

[1] Masaki Watanabe, Toshio Endoh, Morito Shiohara, Shigeru Sasaki, “Palm vein authentication technology and its applications,” Proceedings of The Biometric Consortium Conference September 19th-21st, 2005, Hyatt Regency Crystal City, Arlington, VA, USA

[2] M. Une, A. Otsuka, H. Imai, “Wolf Attack Probability: A New Security Measure in Biometric Authentication Systems,” In: Lee, S.-W., Li, S.Z. (eds.) International Conference of Biometrics 2007, LNCS, vol. 4642, Springer-Verlag Berlin Heidelberg, pp. 396-406, 2007

[3] Naoto Miura, Akio Nagasaka, Takafumi Miyatake, “extraction of finger-vein patterns using maximum curvature points in image profiles,” MVA2005 IAPR Conference on Machine Vision Applications, May 16-18, 2005 Tsukuba Science City,Japan

[4] T. Matsumoto, et al., “Impact of Artificial ’Gummy’ Fingers on Fingerprint Systems,” Proceedings of the Conference Optical Security and Counterfeit Deterrende Techniques IV, Part of IS sT/SPIE’s ElectronicImaginf 2002, pp.275-289.

[5] Inuma, Manabu, Akira Otsuka, and Hideki Imai. ”Theoretical framework for constructing matching algorithms in biometric authentication systems.” Advances in Biometrics. Springer Berlin Heidelberg, 2009. 806-815.