A Method of Personal Authentication by Shape Recognition of the Lips and Front Teeth

Masanori NAKAKUNI*, Hiroshi DOZONO**, Eisuke ITO[+], Yoshiaki KASAHARA[+] and Hideaki NAKAKUNI[++]

* Information Technology Center
Fukuoka University
8-19-1, Nanakuma, Jonan-ku, Fukuoka 814-0180
JAPAN

** Faculty of Science and Engineering
Saga University
1-Honjyo, Saga 840-8502
JAPAN

[+] Research Institute for Information Technology
Kyushu University
6-10-1 Hakozaki, Higashi-ku, Fukuoka 812-8581
JAPAN

[++] Department of Medical Informatics
Shimane University School of Medicine
89-1 Enya-Cho, Izumo-Shi, Shimane 693-8501
JAPAN

nak@fukuoka-u.ac.jp, hiro@dna.ec.saga-u.ac.jp, itou@cc.kyushu-u.ac.jp, kasahara@nc.kyushu-u.ac.jp, nakakuni@med.shimane-u.ac.jp

Abstract: - In this paper we propose a method for carrying out personal authentication by recording a photo of a computer user's face, recognizing the shape of their lips and front teeth, and performing image matching. Using this method, personal authentication is carried out by comparing the previous and current shape of a user's lips and front teeth when they log on to a computer. This method has a number of merits. As teeth are normally hidden behind the user's lips, user authentication is not carried out automatically as is the case with facial recognition. This means that it is possible for the user to decide for themselves whether or not to carry out user authentication. As it is not possible for a user to be recognized simply by their face being recorded on camera, their privacy is protected. Additionally, as the shape of lips and front teeth vary between individuals, there is a high probability that a user can be correctly identified. Furthermore, there is a low probability of significant changes to the shape of adult teeth over a period of months or years unless major dental work is carried out, so this method is potentially suited to personal authentication. Another merit of this method is the fact that it is possible to perform user authentication using an inexpensive webcam. In this paper, we will detail experiments using this method to perform personal authentication as well as the subsequent results.

Key-Words: - Biometrics, Authentication method, Lips, Front teeth

1 Introduction

In recent years, there have been frequent cases of computers being compromised by malware over the Internet [1]. Malware is short for "malicious software," and indicates software designed to compromise and cause damage to a computer that is executed without the permission of that computer's owner. Various different types of malware exist. Some types of malware steal information stored on a computer. For example, there are cases in which IDs and passwords for logging in to a Web service are stolen using malware. The unauthorized use of stolen IDs and passwords is a serious problem. This is because it is difficult to ascertain whether or not access using a stolen ID and password is with criminal intent. For example, there are Intrusion Detection System (IDS) [2] mechanisms that can detect and block unauthorized access such as a DoS attack that exploits a security hole. An IDS can detect malicious behavior in traffic data traveling over a network, so they make it easy to defend against unauthorized access. However, as identity fraud using stolen IDs is carried out using legitimate user authentication procedures, it is extremely difficult to determine whether or not access is being made by a person other than the registered user. In particular, for user authentication employing a password, anyone who knows that password can pose as its owner. Similarly, user authentication methods

using ID cards also make identity fraud easy. This makes it difficult to detect when a compromise has taken place and determine the scope of the compromise accurately.

Meanwhile, the number of IDs that each user possesses is currently increasing, and the management of these IDs is becoming more difficult. Some users set different passwords for each ID for security reasons, but this means a larger number of passwords must be remembered, and there are repeated incidents of users not being able to log in to a system because they have forgotten their password. In order to resolve these issues, the use of biometrics authentication (fingerprint authentication, vein authentication, iris authentication, etc.) [3] that can identify users without them having to remember a password is beginning to gain broader acceptance. Today, biometrics authentication is being used in a number of everyday situations. For example, these authentication methods are sometimes used when money is withdrawn from an ATM.

2 Biometrics authentication

2.1 Existing methods and their issues

As mentioned previously, there are a number of methods for performing biometrics authentication. For example, fingerprint authentication has been implemented in biometrics authentication, and its use in everyday life is becoming more frequent. However, there are still many issues with fingerprint authentication. For example, issues regarding the protection of privacy have not yet been resolved. Fingerprints are used for criminal investigations, so many people are reluctant to have their fingerprints registered in an authentication system for fingerprint authentication. Another example of biometrics authentication is the invention of authentication methods using facial image data. This method uses face matching to carry out authentication. As with fingerprints, face matching technology is also used in criminal investigations. At present a large number of cameras have been installed throughout urban areas for monitoring the activities of criminals. The faces of passers-by are automatically recorded by the cameras, and these faces are then automatically analyzed. This demonstrates that issues still remain with this method regarding the protection of privacy.

2.2 Issues regarding the protection of privacy

There are a variety of issues with biometrics authentication, but issues regarding the protection of privacy are particularly noteworthy. As mentioned previously, personal authentication is sometimes carried out automatically when using biometrics authentication, even when the user does not intend for this to happen. To resolve issues such as this, there is a need to pursue personal authentication methods that cannot be executed unless the user performs a deliberate action. To achieve this, we have devised a method for carrying out personal authentication by recognizing the shape of a user's lips and front teeth. Normally the user's mouth is closed, so as long as they do not open their mouth and show their teeth, personal authentication using this method is not possible. This means there is a high possibility that this method can protect privacy.

3 Personal authentication using the shape of lips and front teeth for recognition

3.1 Personal authentication process

The process for carrying out authentication is shown in Figure 1. First, a user name is entered. Next, the user's lips and front teeth are recorded. Finally, authentication is carried out by matching the recorded image against template images. The system we proposed was given the name "SAS," taking the first letter of each word in "Smile Authentication System." This is due to the fact that the user smiles to record their lips and front teeth when carrying out authentication.

3.2 Equipment and software for authentication experiments

Here we will explain the SAS experiment equipment and software for carrying out personal authentication. The SAS development environment and operating environment is shown in Table 1. HSP is a software development environment developed by a Mr. Onitama from Japan, and is provided free of charge. In recent years development has progressed towards an open source conversion. HSP features a diverse variety of plug-ins for extending the commands used in a program, and most of these are provided free of charge. A syntax similar to BASIC is used for programming. As HSP uses a simple syntax, an increasing number of elementary school and junior

high school students are using it in Japan. One of HSP's most notable merits is the fact that it enables the creation of software with a high level of functionality using simple, concise code.

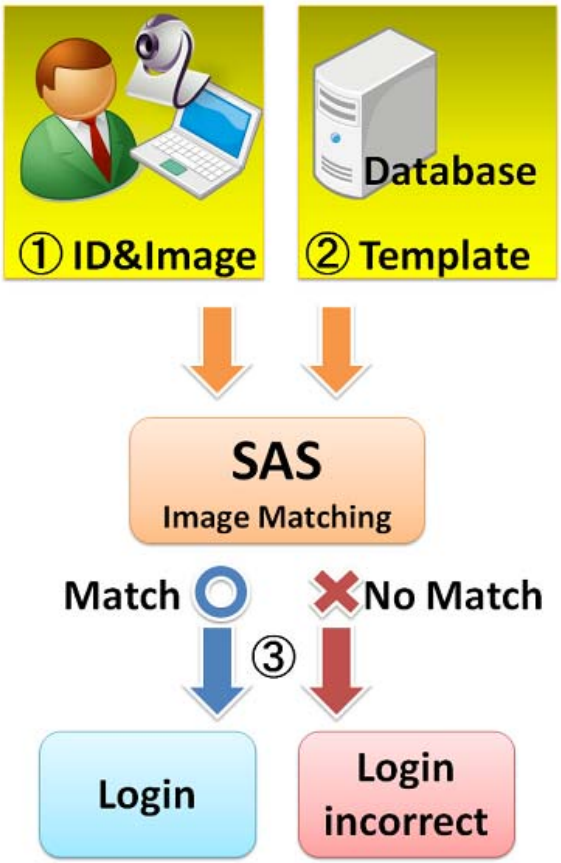

Figure 1: Process for user authentication

Table 1: System architecture of the experimental device

Hardware	
CPU	Intel Core2 Duo U7600 1.2GHz
Memory	2GByte
HDD	60GByte
Camera	Logicool Qcam Pro 4000
Software	
OS	Windows Vista Business
Development Language	HSP (Hot Soup Processor)

3.3 Preparations for authentication experiments

For authentication it is necessary to match the images recorded during authentication against images of a user's lips and front teeth that have been registered as a template in advance. This means that templates for authentication must first be prepared. For template creation the lips and front teeth of the user to be authenticated are recorded using a camera, as shown in Table 2. Figure 2 shows an example of this template. The OpenCV image matching function is used for image matching. OpenCV has a function for carrying out template matching using a number of methods. Additionally, it is easy to call OpenCV functions using HSP.

Figure 2: Example of template

4 Results of personal authentication experiments using SAS

We carried out personal authentication experiments using SAS. There were 2 experimental subjects. 5 templates were prepared for each experimental subject. 10 personal authentication experiments were carried out for each experimental subject. The results of these experiments are shown in Table 2.

FRR indicates the False Rejection Rate, meaning the proportion of experiments in which a legitimate

user could not be authorized properly. FAR indicates the False Acceptance Rate, meaning the proportion of experiments in which an unauthorized user was mistakenly recognized as a legitimate user. In other words, this shows the success rate of attempts to pose as a legitimate user. Ideally, both the FRR and FAR rates should be as close to 0 as possible. We believe that the results shown in Table 2 are comparatively good.

Table 2: Results of authentication experiments

User No.	FRR	FAR
User 01	0.20	0.00
User 02	0.30	0.00
Average	0.25	0.00

5 Conclusion

In this paper we proposed a method for carrying out personal authentication using images of a user's lips and front teeth. Furthermore, by carrying out personal authentication experiments using this method and presenting the results, we were able to show the potential for using this method as a method for personal authentication. This method can be implemented using a computer and an inexpensive USB camera. Furthermore, this method can potentially be applied to a variety of systems. Recently, more and more laptop computers feature a built-in camera, so an environment for making the use of this method extremely easy is developing steadily. However, there are a number of issues that remain unresolved using this method. For example, it may be extremely difficult to differentiate between twins. Another issue is preventing identity fraud in which the authentication process is falsified using a photo taken of the lips and front teeth of a legitimate user. There is a need to include a mechanism in SAS for differentiating between a three-dimensional face and a two-dimensional photo to prevent this kind of falsification. Additionally, as the experiments that were carried out involved only a small number of experimental subjects, we are exploring the possibility of carrying out authentication experiments with a larger number of users in the future, and including falsification countermeasures in these experiments.

References:

[1] IPA/ISEC in JAPAN, 2007. Computer Virus / Unauthorized Computer Access Incident Report, http://www.ipa.go.jp/security/english/virus/press/200712/E_PR200712.html.

[2] About.com, 2003. Introduction to Intrusion Detection Systems (IDS), http://netsecurity.about.com/cs/hackertools/a/aa030504.htm.

[3] Security Focus, 2001. An Introduction to IDS, http://www.securityfocus.com/infocus/1520.

[4] Kolesnikov, O., D. Dagon, and W. Lee, 2006. Advanced Polymorphic Worms: Evading IDS by Blending in with Normal Traffic. In USENIX Security Symposium 2006.

[5] COMPUTERWORLD, 2007. QuickStudy - Biometric authentication, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=100772.

[6] Fernando L. Podio and Jeffrey S. Dunn, 2000. Biometric Authentication Technology: From the Movies to Your Desktop , http://www.itl.nist.gov/div893/biometrics/Biometricsfromthemovies.pdf.

[7] Tao Qian, Veldhuis Raymond N. J., 2006. Biometric Authentication for a Mobile Personal Device, Mobile and Ubiquitous Systems, 2006 3rd Annual International Conference on Mobile and Ubiquitous Systems (MOBIQUITOUS 2006), pp.1-3.

[8] Kyunghee Lee and Hyeran Byun, 2003. A New Face Authentication System for Memory-Constrained Devices, IEEE Transactions on Consumer Electronics, Vol. 49, No. 4, pp.1214-1222.

[9] E. Acosta, L. Torres, and A. Albiol, 2002. An automatic face detection and recognition system for video indexing applications, 2002 IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP).

[10] Masanori Nakakuni, Hiroshi Dozono et.al, 2007. Application of Self Organizing Maps for the Integrated Authentication using Keystroke Timings and Handwritten Symbols, WSEAS TRANSACTIONS on INFORMATION SCIENCE & APPLICATIONS, Issue.2 Volume.4, pp. 413-420.

[11] Hiroshi Dozono, Masanori Nakakuni, Hisao Tokushima and Yoshio Noguchi, 2006. Application of Self Organizing Maps to User Authentication Using Combination of Key Stroke Timings and Pen Calligraphy, Proceedings of the

5th WSEAS Int. Conf. on COMPUTATIONAL INTELLIGENCE, MAN-MACHINE SYSTEMS AND CYBERNETICS.

[12] Hiroshi Dozono, Masaori Nakakuni et.al, 2006. The Analysis of Key Stroke Timings using Self Organizing Maps and its Application to Authentication, Proceedings of the International Conference on Security and Management 2006, pp.100-105.

[13] Hiroshi Dozono, S. Ito, Hisao Tokushima and Masanori Nakakuni, 2007. The Analysis of Key Typing Sounds using Self Organizing Maps, The 2007 International Conference on Security and Management, pp. 337-341.

[14] Hiroshi Dozono, Daishi Takata, Masanori Nakakuni and Yoshio Noguchi, 2005. The Analysis of Pen Pressures of Handwritten Symbols on PDA Touch Panel Using Self Organizing Maps, The 2005 International Conference on Biometric Authentication (BIOAU'05), pp. 440-445.

[15] ONION software: Hot Soup Processor Official Homepage (in Japanese), http://www.onionsoft.net/hsp/.