MagiSign: User Identification/Authentication

Based on 3D Around Device Magnetic Signatures

Hamed Ketabdar
Quality and Usability Lab, TU Berlin
Deutsche Telekom Laboratories
Ernst-Reuter-Platz 7,
10587 Berlin
hamed.ketabdar@telekom.de

Kamer Ali Yüksel
TU Berlin
Ernst-Reuter-Platz 7
10587 Berlin
kamer.yuksel@telekom.de

Amirhossein Jahnbekam, Mehran Roshandel, Daria Skripko
Deutsche Telekom Laboratories
Ernst-Reuter-Platz 7
10587 Berlin
{amirhossein.jahanbekam, mehran.roshandel, daria.skripko}
@telekom.de

Abstract—**In this paper, we present "MagiSign", a new user identification/authentication technique based on 3D magnetic signatures created in the space around a (mobile) device. The main idea is to influence magnetic (compass) sensor embedded in some mobile devices (e.g., iPhone 3GS, G1/2 Android) using a properly shaped magnet. The user draws 3D signatures in the 3D space around the device using a magnet (e.g., pen, rod, ring shaped). This is what we call as "3D Magnetic Signature". The temporal pattern of change in the magnetic field around the device is sensed and registered by the internally embedded magnetic sensor. For authentication/identification, new magnetic signature samples are compared with models created based on registered signatures. As the magnetic signature can be flexibly created in 3D space, it provides a wider choice for authentication. Unlike regular signatures, a hardcopy can not be easily generated resulting in higher security. "MagiSign" technique does not require expensive or complex hardware/algorithm, and does not impose major change in hardware or physical specifications of the device. It can be especially suitable for small mobile devices.**

Keywords-User Identification/Authentication, 3D Magnetic Signature, Around Device Interaction, Magnet, Embedded Magnetic (Compass) Sensor.

I. INTRODUCTION

Portable personal devices such as PDAs or mobile phones are being widely used during daily life. These devices can be used to store or access sensitive information. They are frequently used in insecure locations with little or no physical protection, and are therefore susceptible to theft and unauthorized access. User authentication/identification therefore seems to be essential for granting access to certain information or services. The authentication is conventionally performed using secret codes and personal identification numbers (PINs) [1]. However, they can be easily compromised, shared, observed, stolen or forgotten. Other techniques such as Fingerprint [2], a face profile [3], voice based verification [4], or combination has been also investigated.

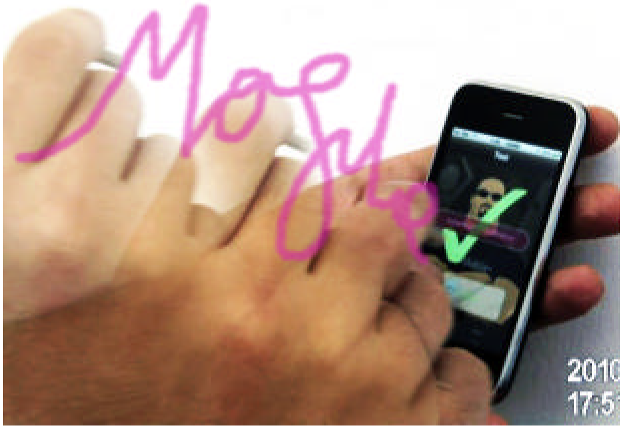

Figure 1: 3D Magnetic Signature

In this work, we propose a new authentication/identification technique, mainly for small mobile devices, based on interaction with embedded magnetic (compass) sensor. This sensor is already embedded in some mobile devices (e.g., Apple iPhone and Google Android) for navigation purposes. We call the new method "MagiSign" or "3D Magnetic Signature". The user simply makes a 3D signature in the space around the device using a properly shaped magnet (rod, ring, pen) (Figure 1). Movement of the magnet changes temporal pattern of magnetic filed sensed by the magnetic sensor integrated in the mobile device. For signature identification/authentication, a new signature sample is matched against models created for signatures of users. The idea is partly inspired by Around Device Interaction (ADI) framework [5][6][7], which propose using space around the device for interaction with the device.

As the magnetic signature can be created in 3D space, it provides a very large flexibility for the choice of signature. Unlike regular signatures, it is not easy to make hardcopies of such a signature. The proposed technique relies only on a magnetic sensor (already embedded in some devices mainly for navigation purposes), and a magnet as external accessory. Compared to camera and fingerprint sensor, a magnetic sensor can be much simpler, smaller and cheaper, and can be internally embedded. It does not impose major change in hardware or physical specifications of devices, which can be especially important for small mobile devices. Extracting useful biometric information from magnetic sensor data can be algorithmically simpler than computer vision or audio processing techniques and the method is not subject to different sources of illumination, occlusion, and audio noise. Such an approach opens up a new, simple and effective way for user identification/authentication based on 3D Magnetic Signatures. Although we mainly talk about mobile devices, the presented approach can be also used for other platforms in a similar way.

The paper is organized as follows: Section 2 describes the idea behind our approach for user identification/verification in more details. Section 3 explains feature extraction and signature/user classification. Section 4 presents experiments and results. An implementation of the proposed approach as a demonstrator on Apple iPhone is introduced in Section 5, and Section 6 provides conclusions and future work tracks

II. MAGENTIC SIGNATURE : THE IDEA

As already mentioned, the basic idea behind our approach is to provide a new user identification/authentication technique based on the so called “3D Magnetic Signature” or “MagiSign”. The user creates his own arbitrary 3D signature using a properly shaped magnet in the 3D space around the device (Figure 1). Movement of the magnet changes the magnetic field sensed (registered) by the built in compass (magnetic) sensor. For identification/verification, temporal pattern of a new signature is compared against a model already created based on pre-registered magnetic signature samples of users. Some mobile devices such as Apple iPhone 3GS, and Google Android are already equipped with compass (magnetic field) sensor. The magnet which should be used for creating signatures is a regular non-powered magnet in a proper shape such as rod, ring or pen. The idea is partly inspired from Around Device Interaction framework which proposes to use space around the device for touch less interaction with the device based on analyzing different sensory information [5][6][7].

The 3D magnetic signature provides a wider choice for authentication as it can be flexibly drawn in 3D space around the device, and can be consequently very difficult to replicate. Additionally, unlike regular signature, no hardcopy of the magnetic signature can be easily produced, resulting in higher security.

Although it is potentially possible to capture gesture based signatures by e.g., camera [10], getting useful information from magnetic sensor is algorithmically and technically much simpler than implementing computer vision techniques. In contrast to accelerometer based gesture recognition techniques [9], our hand gesture recognition approach requires a peripheral magnet. Nonetheless, using a tiny magnet in our case helps the user not to loose the direct sight to the mobile device screen. In addition, for installed Authentication/Identification devices in gates, shaking the entire device is not possible while a tiny magnet can be easily used to draw a signature. Our method does not impose major change in hardware or physical specifications of mobile devices. It does not require installing complex, expensive, and space occupying sensors which can be critical in small mobile devices. It is only based on a magnetic sensor which is internally embedded in some new mobile devices. For mobile devices such as iPhone and G1/2 Android, it is only necessary to have a properly shaped magnet as an extra accessory. Unlike face and audio based authentication techniques, our approach does not suffer from illumination variation, occlusion and audio sources of noise. Since the interaction in our method is based on magnetic field (which can pass through hand, body, clothes and many other different objects), even the space at the back of device can be efficiently used for signing, yet providing more flexibility for authentication. Additionally, the user can interact with the mobile device, even if the device is not in the line of sight, or covered (e.g., mobile device in a pocket or bag). For instance, the user can activate a service or unlock the device without taking it out of his pocket/bag.

We have built a demonstrator called “MagiSign” (presented in Section 5) based on the magnetic signature concept. The demonstrator is built as an application for Apple iPhone 3GS. The application allows recording signature templates, and verifying the user identity based on new signature samples. A confidence score indicating the match between new signature samples and the templates is also provided on the screen.

III. PROCESSING MAGNETIC SIGNATURES

Magnetic signatures are created based on arbitrary moving a magnet (a rod or ring) by hand in the space around the device along different 3D trajectories (Figure 1). The signature can be a simple 3D motion, or the regular signature of the user drawn on the air! or any other combination of even higher complexity which actively uses all 3D space around the device. The rod shaped magnet can be installed in a pen. We have used iPhone 3GS as mobile device for our studies.

The embedded compass (magnetic) sensor provides a measure of magnetic field strength along x, y, and z directions. The values change over a range of -128 to 128.

In our current setup, the user should press a button during performing the magnetic signature, in order to indicate the beginning and end of recording magnetic signals. An alternative would be automatically detecting begin and end of the signature by comparing Euclidean norm of magnetic field strength against a pre-defined threshold.

The embedded magnetic sensor captures temporal pattern of change in magnetic field due to the movement of the magnet.

Some features are then extracted from signals captured by the magnetic sensor. The extracted features are then used to train reference statistical models for different users/signatures. During the test of the system, new signature samples are matched against the reference statistical models. An output score indicating the match between the new signature sample and existing models is then used as a basis for identification/verification.

IV. FEATURE EXTRACTION

Feature extraction allows for preserving information which can be discriminative between signatures/users and removes redundant information. All the features are extracted over samples in an interval marked by the beginning and end of the signature. This interval is divided into two equal length windows, and a feature vector is extracted for each window. The two feature vectors are then concatenated to form a new feature vector to be used for signature classification. Dividing the signature interval to multiple windows allows for capturing temporal pattern of the signature in a more detailed way. Features we have used are mainly based on average or variance of magnetic field strength in different directions, as well as piecewise correlation between field strength in different directions. Features used in this study are listed in the following:

- Average field strength along x, y, and z directions (3 features)
- Variance of field strength along x, y, and z directions (3 features)
- Average of Euclidean norm of filed strength along x, y, z (1 feature)
- Variance of Euclidean norm of field strength along x, y, and z (1 feature)
- Piecewise correlation between field strength along x-y, x-z, and y- z (3 features)

These features form an 11 elements feature vector for each window. The two window feature vectors are then concatenated to form a new 22 elements feature vector for each signature.

Alternatively, all above features can be extracted from a time derivative of magnetic signals, instead of raw magnetic signals. Applying a derivative operator before feature extraction can cancel the effect of magnetic source noises (e.g., earth magnetic field).

V. IDENTIFICATION/AUTHENTICATION

The extracted feature vector is used as input to machine learning algorithms for signature identification/verification. We have studied Multi-Layer Perceptron (MLP) [8] as the classifier.

Multi-Layer Perceptron (MLP) is an Artificial Neural Network which can realize an arbitrary set of decision regions in the input feature space. The feature vectors are used to train the MLP. During testing the system, a feature vector is presented at MLP input. The MLP estimates posterior probability of different signature classes at output (each MLP output is associated with one signature/user class). The signature/user class with highest posterior probability is selected as identification/authentication output.

VI. EXPERIMENTS AND RESULTS

We have set up signature identification/verification experiments in order to evaluate our method. We have invited 15 test users for the experiments. Each user is asked to make a magnetic signature 15 times using a rod shaped magnet. We recorded the signals captured by the embedded magnetic sensor using an application developed for Apple iPhone 3GS.

Features are extracted from magnetic signals as described in Section 3.1. As already mentioned, the input to feature extraction can be raw magnetic signals, or their time derivatives. Both cases are studied in the experiments. The extracted features are used for signature/user classification using MLP. We have used a 10 fold cross-validation scheme for managing training and test data.

Table I shows signature/user identification results using MLP as classifier for features extracted from raw, as well as derivative magnetic signals. As can be seen in the table, the best performance reaches good accuracy of 95.2% for user identification. Using raw magnetic signals slightly outperforms the use of derivatives, however we think if the identification process is performed in a situation that orientation or tilt angle of the mobile device can not be well stabilized, derivatives could be more informative.

Table II shows authentication related measures for the experiment, averaged over different users (raw signals are used for feature extraction). These measures are area under ROC curve, True Positive (TP) rate, and False Positive (FP) rate. The authentication results show a good trade-off between true and false alarms.

We have further investigated the issue of user identification/authentication using simple and identical (among users) 3D gestures instead of personalized signatures. For the experiment, we invited 6 users which are asked to all draw similar and simple gestures shown in Figure 2. These gestures are then used for user identification in the same process as explained for personalized signatures.

Table III shows user identification results for different gestures. As it can be seen in the table, even using very simple identical gestures, users can be identified with relatively high accuracy. This means that the whole process extracts biometric information allowing user identification, using even identical simple gestures.

TABLE I. Signature/user identification results. The first column shows the results when raw magnetic signals are used as input to feature extraction. The second column shows results when derivative of magnetic signals is used for feature extraction.

Source	Raw signals	Derivative signals
Accuracy	95.2%	94.4%

TABLE II. User authentication measures, averaged over users.

Measure	ROC Area	TP rate	FP rate
Value	0.991	0.952	0.003

TABLE III: User identification accuracy for simple identical gestures. Gestures are identical among users.

Gesture ID	1	2	3
Accuracy	90.0%	92.2%	91.2%

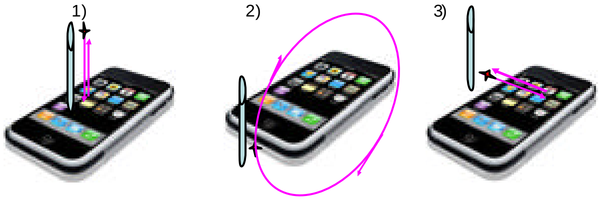

Figure 2: Simple gestures used for user identification.

VII. DEMONSTATOR

Based on the idea presented in this paper, we have implemented a user verification/identification demo for Apple iPhone 3GS. In our demo program, users are allowed to register a few templates of their 3D Magnetic Signature (at least two) around the device. Afterwards in user identity phase, new signature samples can then be recognized/verified against previously recorded patterns. The demo application can also provide a confidence score indicating the level of match between a new signature sample and registered templates. The demo application uses dynamic time warping (DTW), a template matching approach to match between signature samples and registered templates. The accuracy of the signature recognition application using 2 registered templates of users' signature is up to 92%. The application also allows the user to adjust sensitivity of the algorithm for verifying signatures by filtering the magnetic signals.

VIII. CONCLUSIONS AND FUTURE WORK

In this paper, we have studied a new simple yet effective technique for identification/authentication based on what we call as "3D Magnetic Signature" or "MagiSign". The user can use 3D space around the device to flexibly create 3D signatures using a properly shaped magnet. The 3D magnetic signature provides a wider choice for authentication as it can be flexibly drawn in 3D space around the device. Unlike regular signature, no hardcopy of the magnetic signature can be easily produced, resulting in higher security. "MagiSign" is a touch-less way of authentication. It and does not impose major changes in hardware or physical specifications of mobile devices. It is only based on a simple, very small and internally embedded sensor.

There are plenty of possibilities for further improving the current system. For instance, users can create 3D Magnetic Signatures using their own personalized magnet. This personalized magnet can be considered as a physical key. Shape, polarity, angle of usage (during signing), and intensity of the magnet can affect magnetic signature pattern. Therefore, the security level of such a signature can be reinforced using personalized magnets e.g., with custom shape, polarity, intensity, etc. We are also interested to run a survey to analysis attacking possibilities by asking the users to imitate the signature of other people.

REFERENCES

[1] "HP iPAQ Pocket PC h5500 User Guide," Hewlett-packard Company, http://bizsupport.austin.hp.com/bc/docs/support/SupportManual/lpia8006/lpia8006.pdf, July 2010.

[2] P. Gupta, S. Ravi, A. Raghunathan, and NK. Jha, "Efficient Fingerprint-Based User Authentication for Embedded Systems," Design Automation Conf., pp. 244-247, June 2005.

[3] N. Aaraj, S. Ravi, A. Raghunathan, and N.K. Jha, "Architectures for Efficient Face Authentication in Embedded Systems" Proc. Design, Automation & Test in Europe, March, pp. 1-6, 2006.

[4] C.C. Leung, Y.S. Moon, and H Meng, "A Pruning Approach for GMM-Based Speaker Verification in Mobile Embedded Systems," Lecture Notes in Computer Science, vol. 3072/2004, pp. 607-613, 2004.

[5] T. Starner, J. Auxier, D. Ashbrook, and M. Gandy, "The gesture pendant: A self-illuminating, wearable, infrared computer vision system for home automation control and medical monitoring," International Symposium on Wearable Computing, 2000, pp. 87-94.

[6] S. Kratz, and M. Rohs, "HoverFlow: expanding the design space of around-device interaction," In Proc. of the 11th International Conference on Human Interaction with Mobile Devices and Services, Bonn, Germany, pp. 1-8, 2009.

[7] L.S. Theremin, "The Design of a Musical Instrument Based on Cathode Relays," Reprinted in Leonardo Music J., No. 6, pp. 49-50, 1996.

[8] M.L. Minsky and S. Papert, "Perceptrons," Cambridge, MA: MIT Press, 1969.

[9] P. Keir, J. Payne, J. Elgoyhen, M. Horner, M. Naef, and P. Anderson, "Gesture-recognition with Non-referenced Tracking," 3D User Interfaces 3D User Interfaces (3DUI'06), pp.151-158, 2006.

[10] Y. Wu, and T.S. Huang, "Vision-Based Gesture Recognition: A Review," Proceedings of the International Gesture Workshop on Gesture-Based Communication in Human-Computer Interaction, pp. 103-115, 1999.