inTUIt – Simple Identification on Tangible User Interfaces

Alexander Wiethoff, Robert Kowalski, Andreas Butz
LMU University of Munich
Amalienstr. 17, 80333 Munich, Germany
{firstname.lastname}@ifi.lmu.de, kowalski@cip.ifi.lmu.de

ABSTRACT
In this paper we present *inTUIt*, an experience prototyping approach to investigate different simple identification techniques for tangible user interfaces (TUI) on digital surfaces. We have developed four different experience prototypes, proposing alternative approaches to the establishment of temporary ownership of digital content and TUIs in public environments.

Author Keywords
Identification, TUI, Prototyping.

ACM Classification Keywords
H5.2. Information interfaces and presentation (e.g., HCI): User Interfaces – Haptic I/O, Input devices and strategies

General Terms
Design, Experimentation.

INTRODUCTION

Tangible user interfaces (TUI), in combination with digital surfaces, have gained more awareness in the field of interaction design. They offer physical affordances connected to digital actions. Under the umbrella term “graspable interface”, interesting projects have been developed in recent years [3,6]. However, as these deployed digital surfaces are intended to be used within collaborative scenarios by multiple users, a critical challenge is the establishment of user identity within the TUI context, which is a prerequisite to establish ownership between the personal digital content and the user. An example of such a collaborative use case was *Photohelix* [6], which controlled a photo-browsing application with a TUI object on a digital surface. A comparative study revealed that content in a large collection was accessed faster using a graspable interface. However, accessing personal content in the implemented prototype was only possible after a login process, in which the username was entered through a virtual keyboard. This was a time-consuming task and broke the tangible paradigm. The original vision behind *Photohelix* was that every user would carry his or her own TUI object, which would grant him or her access to the application and his or her personal content. Especially when dealing with content on digital surfaces that has already been declared as public by its producers (e.g., one’s music listening history on the *last.fm* music service, or one’s photo-stream from the picture sharing platform *flickr.com*), heavyweight identification mechanisms, such as entering passwords and usernames, can prove overprotective and too time-consuming to users. Another reason to improve the memorability of an identification mechanism is that users might forget their dedicated username because remembering passwords and usernames already overwhelms them when accessing their web applications and services, as discussed by Adams et al. [1]. We wanted to investigate alternative and more lightweight identification mechanisms that might be acceptable to users when accessing these types of data on a digital surface with a TUI. We selected a collaborative deejaying music application mockup as the contextual framework for our research. The application is designed for public access via a digital surface and is controlled using two TUIs simultaneously. In our envisioned scenario, multiple users continuously create and shuffle new playlists together based on their existing *last.fm* listening histories, as could happen, for example, at a party. To judge which identification method might be favored by the users for accessing their content, we have implemented four experience prototypes, equipped with different identification techniques such as gesture, rhythm, handwriting, and fingerprint scanning. These prototypes were compared against each other in a qualitative/quantitative user study and evaluated against one conventional authentication mechanism on a digital surface: A login field in combination with a virtual keyboard.

RELATED WORK

Many recently deployed TUI projects use digital surfaces and a graspable interface for interaction with audio content or processing [4,7,14]. Most of these projects, however, do not address identification mechanisms for accessing personal content. Stajano et al. [15] described security policy as an authentication method, which could be also applicable to a TUI, but might prove overprotective for accessing public data, as in our approach. Balfanz et al. [2] exemplified identification in ad-hoc wireless networks using a combination of mechanisms such as physical contact, infrared and speech recognition. Since our user

TEI’11, January 22–26, 2011, Funchal, Portugal.

research emphasized embodied interactions, we interpreted the idea of physical contact more literally, with physical actions. Claycomb et al. [5] proposed an approach where identification was established via image recognition on visual tags, which is more suitable for establishing a connection between two devices. Toye et al. [17] explored using smart phones as an identification mechanism. In contrast to their work, we decided not to require any additional infrastructure from the user, because not everyone possesses such a device and compatibility problems would aggravate real life deployment. Furthermore, a smart-phone as a tangible user interface does not offer the appropriate physical affordances to perform the digital actions we envisioned. Additional approaches include analysis of tapping patterns [11], Radio Frequency Identification (RFID) and its successor Near Field Communication (NFC) [12] and gestures such as pointing [16]. These served as an inspiration to select different techniques that we first presented in the user study and later implemented in our prototypes. Kumar et al. [8] described a study of individual pairing mechanisms and methods. While some of these methods are promising, they are also highly technological; our approach is more oriented towards embodied interactions, potentially providing a higher memorability as concluded by Wobbrock et al. [18]. In addition, Orr et al. demonstrated with their *Smart Floor* [10] that a physical, embodied approach can mitigate confounding issues, such as noise and varying light conditions, that plague other authentication mechanisms.

PROCESS AND PROTOTYPE

Following a user-centered design process [9] in the initial user research phase we interviewed eight different people, aged 23-28 years old, from various backgrounds. When presented with the possibility of identifying themselves using a TUI as an input method, the participants favored the ideas of using tapped signals or direct handwriting recognition, as compared to other suggested approaches.

Concepts of the Experience Prototypes

The prototypes we built offered five different identification techniques to the users. After a successful identification through the TUI, a digital surface would bring up their dedicated personal content, in our case a representation of their music collection categorized in different genres, arranged around the TUI. The implementations allowed the following identification forms. **Fingerprint scanning**: Identification was established when users swiped their finger over a scanner. To recognize their biometrics, a button had to be activated, which saved their fingerprint in the database (see Figure 1a). **Handwriting recognition**: Users identified themselves by metaphorically signing the TUI. To do this, users wrote their initials with their finger on an embedded touchscreen (see Figure 1b). **Spatial gestures**: Users defined a three-dimensional (6 DOF) gesture with the TUI and retrieved their personal content by repeating it (see Figure 1c). **Tapping signals**: Identification was established through a dedicated knocking pattern, e.g. a rhythm from a song. (see Figure 1d). **Virtual keyboard**: A virtual keyboard on the digital surface, in combination with a username login-field, served as a standard mechanism for identifying users.

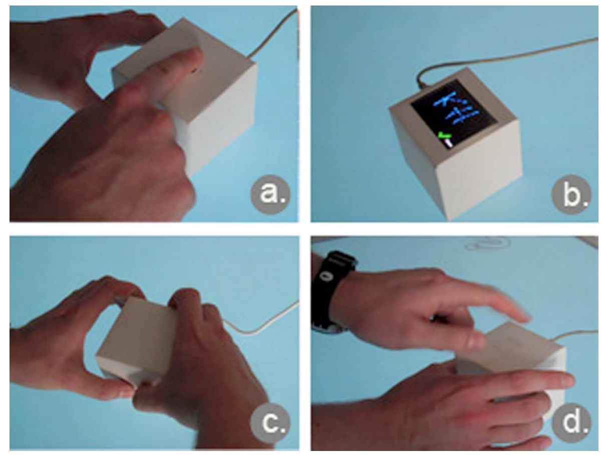

Figure 1. Different identification mechanisms embedded in TUIs : a.) Fingerprint scanning b.) Handwriting recognition c.) Spatial gestures and d.) Tapping signals

USER STUDY

As we intended only to measure the user's satisfaction in the different identification mechanisms, we explicitly left out design factors of the TUIs in order to avoid bias in our study. Thus, four simple geometrical forms of the same shape and size were created out of white cardboard and served as representations of the TUI (see Figure 1). The user study took part over two days with 13 participants, between 25-35 years, from various backgrounds. Each session lasted about 40 minutes and was recorded on video. Qualitative and quantitative data was collected using a questionnaire. The questionnaire focused on the evaluation of the different identification mechanisms via five-point Likert Scales ranging from "strongly agree" to "strongly disagree", as well as qualitative questions about willingness of use, identification alternatives and whether these techniques are perceived as an improvement in comparison with traditional mechanisms.

Results

Figure 2 shows the results for each individual identification method. **Fingerprint scanning:** Concerning the pleasantness of use, participants repeatedly stated that the fingerprint scanner requires a finger to slide in the direction opposite to the common one used on laptop computers. Regarding quickness of use, the extent of necessary learning on how to program the TUI, programming the TUI, identification via the TUI and the memorability of the method, the majorities "strongly agreed" that these tasks are easy. However, all participants indicated that they have strong privacy concerns because they do not know where the fingerprint is stored or who has access to it. **Handwriting recognition:** Here, the majority of the participants “strongly agreed” on the ease and quickness of use measures. However, the usage pleasure received a lower score, which, according to the feedback, was due to the small display size. As seen in Figure 2, the characteristics of “easy to learn”, “easy to program” and “easy to ID”, were “strongly agreed” with by most participants. In contrast, due to the limited number of permutations with two initials, users repeatedly mentioned security concerns with this kind of identification, even though they were reminded of the harmlessness of the content. **Spatial gestures:** The participants voted this TUI as the least popular one. This is reflected by the lowest scores for ease and pleasantness of use, “easy to learn”, “easy to program” and “easy to ID”. Remembering the identification patterns proved hugely problematic for the participants. Nevertheless, one participant mentioned that this problem would be reduced over time as soon as users performed the patterns a few times and their muscular memory automated the process. **Tapping signals:** In contrast to spatial gestures, rhythm tapping was the most popular identification method. This is facilitated by its high scores throughout all questions, apart from memorability, privacy and security. Considering the memorability, participants mentioned that it might be too difficult for unmusical persons to remember the pattern. Furthermore, the users had the impression that the knock pattern could easily be replicated by other persons, resulting in the low security score. **Virtual keyboard:** As expected, the virtual keyboard achieved high scores for ease of use, “easy to learn”, “easy to program” and “easy to ID”. From the qualitative feedback, this is due to the fact that all participants were already familiar with this kind of identification. However, the issue of keeping an additional password in mind was mentioned repeatedly and affects the score of “easy to remember”.

For the evaluation of the user rankings we used the Copeland's method [13]. Regarding the popularity, tapping signals was the Condorcet winner. This was followed by fingerprint scanning, handwriting recognition and the virtual keyboard in second place with 2 wins and 2 losses each. The Condorcet loser is the spatial gestures technique. Concerning the ease of use, the resulting ranking is as follows: Fingerprint scanning, virtual keyboard, tapping signals, handwriting recognition and spatial gestures. For pleasure of use, the Condorcet winner and loser are the same as with the popularity ranking. In between, fingerprint scanning, handwriting recognition, and the virtual keyboard achieved positions two to four. The last comparative question dealt with perception, which method the participants perceived as the quickest to use. An interesting observation with this question is that the measured identification times do not coincide with the perceived usage speed. While the ranking identifies the fingerprint identification as the Condorcet winner, the time measurements for the user identification revealed the rhythm recognition as being over six seconds faster than the fingerprint on average. This seems to be due to the fact that the fingerprint reading trial often required two identification attempts because the finger had been scanned in the wrong direction at first. Also faster than the fingerprint was the handwriting recognition, with a three second advantage. Considering the slowest kinds of identification methods, the virtual login and the gesture recognition have been ranked forth and fifth and measured in reverse order with a two-second gap.

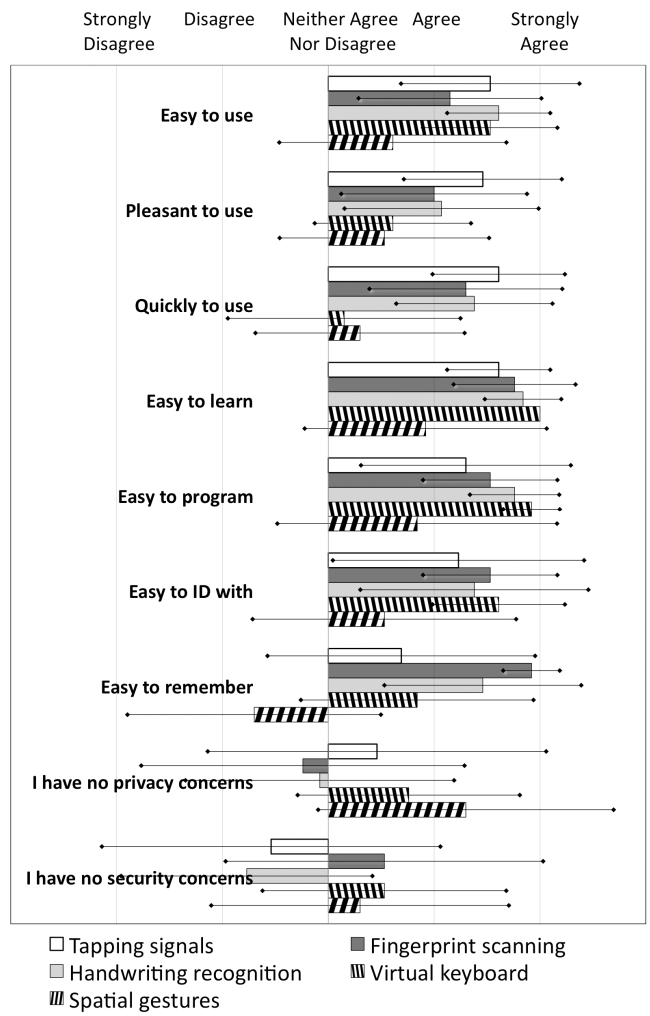

Figure 2. Overview of the ratings from the different experience prototypes

When asked about their willingness to use the TUIs, nine participants chose the fingerprint identification (four votes) as well as the rhythm recognition (five votes) over the other techniques, whereas three could not imagine using any of the presented methods. In considering further identification alternatives, voice- and facial recognition, as well as iris scans, and the drawing of line patterns, similar to the *HTC Sense®* UI, were mentioned. The final general question dealt with what the user's impression if these identification TUIs made the identification process less abstract. While five participants denied that it would have any impact, four stated that it does and might be especially true for persons with less technical aptitude.

DISCUSSION

Due to minor identification time measuring errors, the results for the measured usage speed were not 100% accurate, and therefore not extensively discussed. Initial trends are already visible from the evaluated data, which support our hypothesis that alternative techniques are generally preferred over traditional ones. However, this might be only the case if they are comparatively more fun to use and quicker to learn. Furthermore, the degree of memorability, together with security and privacy aspects, plays an important role. The performed user study did not cover long-term memorability. This is especially important with regards to gesture identification: with repeated physical actions, the identification process might be automated by the user and accelerated over time. Considering the security and privacy aspects, it should be noted from the users' feedback that the underlying public data scenario reduced the concerns of the participants. For private data, these concerns are likely to be much more serious.

CONCLUSION AND FUTURE WORK

In this paper we presented four different identification mechanisms embedded in TUIs and one conventional mechanism on a digital surface. These also included more conventional authentication mechanisms that had not been explored in conjunction with TUIs before, thereby proposing alternative approaches to the establishment of temporary ownership of digital content and TUIs in public environments. Therefore we propose simple identification mechanisms, as exemplified in this work, when dealing with non-sensitive data in combination with digital surfaces and TUIs, thus saving users' time in identifying themselves or accessing URLs. The results of our study show that the participants favor these rather opportunistic identification approaches in comparison with traditional techniques used in TUIs. Further investigation might improve the users' experience. In particular, privacy concerns have to be considered extensively with public content, as this was one aspect consistently mentioned by users in the study. Finally, since our implementations were mainly based on explicit interaction forms, it would be interesting to look at implicit identification techniques (e.g. grasp-sensing) as well, which might incorporate a higher degree of privacy.

REFERENCES

1. Adams, A., Sasse, M. Users Are Not the Enemy. In *Communications of the ACM*. 1999.
2. Balfanz, D., Smetters, D.K., Stewart, P., Wong, H.C. Talking To Strangers: Authentication in Ad-Hoc Wireless Networks. *Citeseer* 2003.
3. Baudisch, P., Becker, T., Rudeck, F. Lumino: tangible blocks for tabletop computers based on glass fiber bundles. In *Proc. CHI 2010*
4. Bischof, M., Conradi, B., Lachenmaier, P., Linde, K., Meier, M., Pötzl, P., Andre, E. XENAKIS - Combining tangible interaction with probability-based musical composition. In *Proc. TEI´08*.
5. Claycomb, W.R., Shin, D. Secure Real World Interaction Using Mobile Devices. In *Proc. PERMID* 2006.
6. Hilliges, O., Baur, D., Butz, A. Photohelix: Browsing, Sorting and Sharing Digital Photo Collections. In *Proc. Tabletop 2007*
7. Jordà, S., Fabra, P., Geiger, G., Alonso, M., Kaltenbrunner, M. The reacTable: Exploring the synergy between live music performance and tabletop tangible interfaces In *Proc. TEI´07*
8. Kumar, A., Saxena, N., Tsudik, G., Uzun, E. A comparative study of secure device pairing methods. In *Pervasive and Mobile Computing*. 2009.
9. Mao, B.J., Vredenburg, K., Smith, P.W., Carey, T. User-centered design practice. In *Communications of the ACM*. 48.
10. Orr, R.J., Abowd, G.D. The smart floor. In *Proc. EA. CHI '00*
11. Rekimoto, J., Ayatsuka, Y., Kohno, M. SyncTap: An Interaction Technique. In *Proc. Mobile HCI´03*,
12. Rukzio, E., Wetzstein, S., Schmidt, A. A Framework for Mobile Interactions with the Physical World. In *Proc. WPMC'05*
13. Saari, D., Merlin, V. The Copeland method. *Springer* 1996.
14. Schiettecatte, B., Vanderdonckt. J. AudioCubes: a distributed cube tangible interface based on interaction range for sound design. In *Proc. TEI '08*.
15. Stajano, F. The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks. *CiteSeerX* 2000.
16. Swindells, C., Inkpen, K.M., Dill, J.C., Tory, M. That one there! Pointing to establish device identity. In *Proc. UIST '02*.
17. Toye, E., Sharp, R., Madhavapeddy, A., Scott, D. Using Smart Phones to Access Site-Specific Services. In *IEEE Pervasive Computing* 2005.
18. Wobbrock, J.O. TapSongs: tapping rhythm-based passwords on a single binary sensor. In *Proc.UIST '09*