Spatial Authentication on Large Interactive Multi-Touch Surfaces

Johannes Schöning
Institute for Geoinformatics
University of Münster
Robert-Koch-Str. 26-28
48149 Münster, Germany

Michael Rohs
Deutsche Telekom Laboratories
TU Berlin
Ernst-Reuter-Platz 7
10587 Berlin, Germany

Antonio Krüger
Institute for Geoinformatics
University of Münster
Robert-Koch-Str. 26-28
48149 Münster, Germany

Abstract

The exploitation of finger and hand tracking technology based on infrared light, such as FTIR, Diffused Illumination (DI) or Diffused Surface Illumination (DSI) has enabled the construction of large-scale, low-cost, interactive multi-touch surfaces. In this context, access and security problems arise if larger teams operate theses surfaces with different access rights. The team members might have several levels of authority or specific roles, which determine what functions and objects they are allowed to access via the multi-touch surface. In this paper we present first concepts and strategies to authenticate and interact with subregions of a large-scale multi-touch wall.

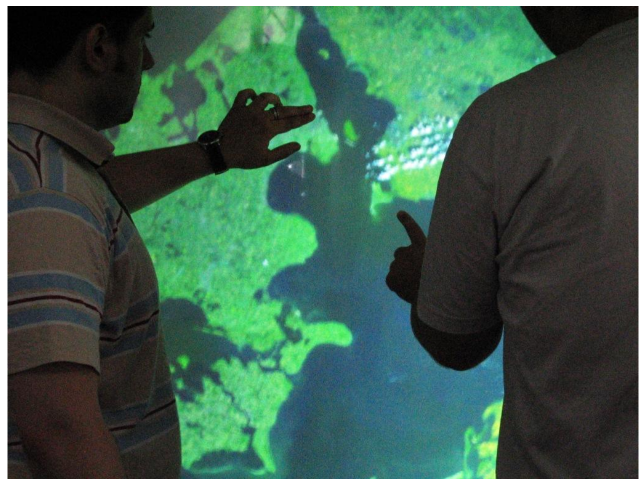

Figure 1. Multi-user interaction with a multi-touch wall in an emergency scenario without dedicated access control.

1. Introduction and Motivation

Authentication of users is an important feature of a modern operating system which grants different rights to different users and is often crucial to protect data from being manipulated consciously or unconsciously by other users or malicious programs (such as a virus). On desktop machines access is often granted on a machine level (login) on a file system level (permissions) or on application level (password to access a certain program) [1]. Following the PC paradigm (one user has access to one physical machine) these authentication processes can safely assume that the user is allowed to use the whole screen space after successful authentication. On a machine with a GUI this usually implies full access to the desktop. One advantage of large interactive surfaces is their easy accessibility for multiple users either interacting at the same time as well as shortly after each other [3]. Interactive surfaces of several square meters, such as interactive walls, pose a novel authentication problem if several users want to interact with different access rights at the same time at different locations of the surface: their rights to manipulate certain data might be restricted to the region in front of them rather than to a particular application or functionality or piece of data. In this paper we would like to address how current authentication concepts can be extended by spatial authentication to define regions of control of particular users. One application scenario is that of a large interactive version of a Geographic Information System (GIS) which is used by crisis management officers with different roles (such as head of firemen, police, and experts) who try to handle the consequences of a catastrophic event threatening public security, such as a flood or a chemical accident (see figure 1). The interactive map provides the different users an overview on the situation and allows them also to manipulate certain variables, such as the positions of fire brigade trucks and mobile chemical sensors. In this scenario authentication is not only critical but also needs to be easy and simple to prevent the staff being distracted by complicated login procedures and allowing them to interact as freely as possible with the interactive map.

Multi-touch interactions are a well studied area of

HCI. The website `http://www.billbuxton.com/multitouchOverview.html` of Bill Buxton is giving a great overview on hardware setups and interaction patterns. The reminder of the paper is organized as follows: The next section will discuss authentication concepts for large interactive surfaces, followed by a section that identifies implementation requirements. We will conclude with a discussion and outlook to future research questions.

2. Authentication concepts

Spatial authentication requires two basic steps: (1) User identification and (2) definition of the region of influence. On interactive surfaces based on infrared tracking step (1) is not an easy task, since only the touch points can be tracked and usually no more information is revealed to the users. There are at least three principle solutions to the problem of user identification: (1a) using biometric identification, such as the identification of the form of a finger joint, the whole hand, or even characteristic movement patterns of touches, (1b) the definition of a particular gesture that serves as a code and (1c) the use of an external device or token, such as a RFID-tag or a mobile phone [5]. In the second step, the region of authentication has to be identified, which defines the area of manipulation for each identified user. In the cases of identification methods 1a and 1b, the system has a rough position of the user in front of the wall and depending on certain bio-mechanical user defaults (length of arms, heights of shoulders) a natural area of influence can be defined as a circular area which is defined by a radius of the length of one arm with a centre in front of the user. Interesting questions arise if multiple users interact simultaneously and close to each other so that these regions would potentially overlap. Depending on the type of interactive surface, it might be useful to allow users to define the regions on their own, e.g. by applying a lasso-like gesture after successful identification. The crisis management scenario we have in mind requires users to move in front of the interactive surface, leave the surface to access other facilities in the room (such as a table with manuals or other documentation) and then come back to the surface. In these cases the regions of influence might not be fixed to a certain location but have to move along with their users. If users leave the interactive surface, the region of influence has to be closed automatically to prevent access by unauthorized users.

3. Implementation requirements

To implement such a spatial authentication schema different additional technologies for the identification process could be used. For user biometric identification (1a) the multi-touch surfaces can be equipped with capacitance fingerprint readers with the disadvantages of requiring additional hardware. Overcoming this problem an optical finger print reader can be integrated into the interactive surface, e.g. having a steerable camera directly under the interactive surface sensing the fingerprints. Other technology such as different tracking system can track the users interacting with the interactive surface. Again with most of the system, like the UWB tracking system Ubisense, the users need to be instrumented with additional hardware. Tracking the user would also has the advantage that by attaching the tag on a defined position the system would be able to define a natural area of influence which itself is defined by a radius of the length of one arm with a centre in front of the user. Allowing no user instrumentation pressure sensing plates around or in front of the interactive surface can solve the user identification problem (similar to the ideas present in the DiamondTouch [2] project). Sensing the user position with pressure plates having the additional advantage that by analyzing gait pattern and postures the system can identity users out of a predefined set up patterns [4]. Using an external device or token, such as an RFID-tag or a mobile phone as described by Schöning et al. in citeavischoening has the disadvantages that the link between user and device cannot be verified by the system, i.e. such a scheme assumes that the external device is operated by its owner and not by another person.

4 Discussion and Future work

In this paper we present first concepts and strategies to authenticate and interact with sub-regions of a large-scale multi-touch wall. We address the two main challenges that have to be tackeld: User identification and the definition of the region of influence. We highlighted different technologies that can be used for the authentication process. In the future we are planning to implement several authentication mechanisms with different technologies and evaluate them with real users in an emergency scenario.

References

[1] M. Burrows, M. Abadi, and R. Needham. A logic of authentication. *ACM Trans. Comput. Syst.*, 8(1):18–36, 1990.

[2] P. Dietz and D. Leigh. DiamondTouch: a multi-user touch technology. *Proceedings of the 14th annual ACM symposium on User interface software and technology*, pages 219–226, 2001.

[3] S. Elrod, K. Pier, J. Tang, B. Welch, R. Bruce, R. Gold, D. Goldberg, F. Halasz, W. Janssen, D. Lee, et al. Liveboard: a large interactive display supporting group meetings, presentations, and remote collaboration. *Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 599–607, 1992.

[4] T. Oberg, A. Karsznia, and K. Oberg. Basic gait parameters: reference data for normal subjects, 10-79 years of age. *J Rehabil Res Dev*, 30(2):210–23, 1993.

[5] J. Schöning, M. Rohs, and A. Krüger. Using mobile phones to spontaneously authenticate and interact with multi-touch surfaces. In *AVI 2008: Workshop on designing multi-touch interaction techniques for coupled private and public displays*, May 2008.