A location tracking and verification system for the clinical environment

Brent Liu, Jasper Lee, Bing Guo, and Jorge Documet

Wireless tracking technology integrated with facial biometrics can improve security in health care facilities.

In many health care facilities, patient data is managed and stored in picture archiving communications systems (PACS) or other clinically-related electronic systems. Secure management and protection of this information is required to comply with the latest security regulations, such as the US Health Insurance Portability and Accountability Act of 1996 (HIPAA).

As more workstations are implemented in a facility, there is an increased dependence on digital storage and a greater need to secure data. The current use of passwords and user-entered identification is a passive, and therefore imperfect, approach to digital authentication. Also, misidentification of patients continues to be a common problem, especially in large facilities. To manage these challenges, health care facilities need improved security methods that protect their sensitive electronic medical data and accurately identify patients.

Our research has focused on developing a tracking and biometric verification system that brings novel security management technology into the clinical environment. We wanted to design a system-architecture that was part of the clinical work flow and could streamline the management of patient and staff activity, protect against misidentification, and improve digital security. The resulting location tracking and verification system (LTVS) registers facial images and assigns portable tracking devices to incoming patients (see Figure 1). The system architecture consists of a server running the Apache2 web server application, a facial recognition system (FRS), and a tracking system.

Once registered, patients can be automatically identified prior to medical procedures or examinations using facial biometrics. In addition, if a patient has been waiting too long in the waiting area or unauthorized staff is trying to access restricted areas, the LTVS can generate an alert that notifies administrators. By merging tracking and biometric verification technology into one application, administrators can watch clinical activity and monitor all system authentication attempts.

There are different tracking and biometric systems available, so we chose to implement a modular infrastructure in order to accommodate a range of technologies. For tracking, we selected a wireless signal fingerprinting system that uses radio-frequency (RF) technology and a proprietary algorithm to locate objects using standard 802.11b or g (wireless) networking technologies. This type of system has been applied in many industrial environments to synchronize work flow and improve throughput. For biometric verification, we chose facial biometrics because it only requires a workstation, a small camera, and connectivity to the server where the images are stored. (Other available bio-

Figure 1. The location tracking and verification system registers facial images and assigns portable tracking devices to incoming patients. PERL: Practical extraction and report language. API: Application programming interface. DB: Database. HIS, RIS: Hospital/Radiology information system.

Continued on next page
metric systems include digital fingerprinting and iris-scanning.) The combined use of wireless tracking and facial biometric technology provides automatic real-time identification. It offers a dramatic improvement over current systems that rely solely on security cameras and passwords.

Our project development began with a clinical study to identify administrative and security issues. Next, we designed the software infrastructure necessary to satisfy these concerns, working to associate patient data with faces and to generate the necessary alert messages. Some of the key system features include x-y mapping of assigned devices, real-time alerts based on definable rules, and accessing patient information at workstations following a facial biometric scan (see Figure 2).

When designing the LTVS integration infrastructure, we acquired software development kits (SDKs) for the tracking and facial biometric systems and implemented them in two separate programs. The tracking program acquires device location information from the SDK and automatically manages the devices based on logical area restrictions. The facial biometric program is called by the graphical user interface (GUI) code to perform image registry and verification tasks. It returns results such as “successful image registration,” “facial identification,” or “failed attempt.” A PostGreSQL database maintains static and dynamic information for the tracking system, and it acts as the means of communication with the user-interface. A final design step was to accommodate multiple workstations for simultaneous webcam access on a centralized server.

In the latter stages of development, the LTVS was installed at the USC Healthcare Consultation Center II (Los Angeles, CA), an outpatient facility (see Figure 3). Feedback from this implementation was used to improve the tracking, facial biometrics, and user-interface for clinical usage.

The result of this research and development is a centralized management system that integrates third-party tracking systems and facial biometric technology into a user-friendly GUI that is accessible by all computer systems on a clinical network. Patients can be accurately located and identified prior to surgical procedures or examinations. Staff can be located through their wireless-enabled personal digital assistants (PDAs) and laptops. Finally, clinical data is more secure because access to electronic medical information is granted only through authorized location and biometric identification.

In future research, we will consider other forms of biometric verification that may improve the identification process in a clinical environment. For example, fingerprint identification may be a better solution since it is not as light-dependent as facial recognition. The future development of combined biometric and wireless tracking technologies will lead to an even more interdependent relationship between the two: for example, biometric verification may be automatically activated by physical presence, such as a person moving next to a computer or through an entrance to a room.

Author Information

Brent Liu, Bing Guo, and Jorge Documet
Image Processing and Informatics Laboratory
University of Southern California
Marina del Rey, CA

Jasper Lee
Department of Biomedical Engineering
University of Southern California
Los Angeles, CA

Continued on next page
References


