Computers and Electrical Engineering 40 (2014) 1123–1142

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Smart home safety handwriting pattern recognition with innovative technology ☆

Kuang-Yow Lian [a], Sung-Jung Hsiao [a], Wen-Tsai Sung [b,*]

[a] Department of Electrical Engineering, National Taipei University of Technology, Taiwan
[b] Department of Electrical Engineering, National Chin-Yi University of Technology, Taiwan

ARTICLE INFO

Article history:
Received 7 November 2012
Received in revised form 20 February 2014
Accepted 21 February 2014
Available online 18 March 2014

ABSTRACT

Intelligent home security control equipment has become indispensable in daily life. This study uses an innovative handwriting recognition technology to confirm user identity and to manage door security. Smart phones are used for security system management and control actions, and identity confirmation is performed in two stages. In the first stage, the user enters a user name and password into a smart phone and waits for successful identity recognition. In the second stage, the user must write a text or symbol pattern previously set into the smart phone. After successful identification in the second stage, the user is given permission to control the electronic lock and enter the door. The proposed home security system is implemented using a RNN (Recurrent Neural Network) with associative memory for training and recognition. The RNN used in the handwriting recognition step performs some recognition iterative processes.

1. Introduction

In recent years, many smart home security systems have been proposed. For example, Raj presented a security algorithm [18], Kim proposed an automated Clairvoyant access right assignment (CARA) mechanism [19], and Li et al. presented an efficient and secure smart grid wireless communications system [20]. Li et al. also noted that an eavesdropper can monitor the daily life of the house owner and determine when the owner is at home.

Many countries are gradually adopting smart home security control systems [1,2]. The most important part of any home security system is accurately identifying users who enter and leave through the door [3,4]. An entrance guard can be managed using passwords, RFID sensors, fingerprints, and face recognition methods [5]. However, each method has shortcomings. For instance, the keyboard may be too small or difficult for use by elderly or persons with mobility problems. For these users, a keyboard may also be inconvenient for inputting a user name and password. An RFID proximity card can be easily lost or stolen, and this method is passive and fixed. Many people are resistant to fingerprint and face recognition because the body is used as a recognition tool. Some people do not like keeping their fingerprints and facial images in a file that can be accessed by others [6]. Many articles have studied the application of intelligent control and ZigBee family, but did not talk about the use of handwriting recognition [23,24]. Recent studies, some papers mentioned the use of mobile phones to control smart home [25].

☆ Reviews processed and approved for publication by Editor-in-Chief Dr. Manu Malek.

* Corresponding author. Tel.: +886 4 23924505x2150; fax: +886 4 23924419.
E-mail address: songchen@ncut.edu.tw (W.-T. Sung).

http://dx.doi.org/10.1016/j.compeleceng.2014.02.010
0045-7906/

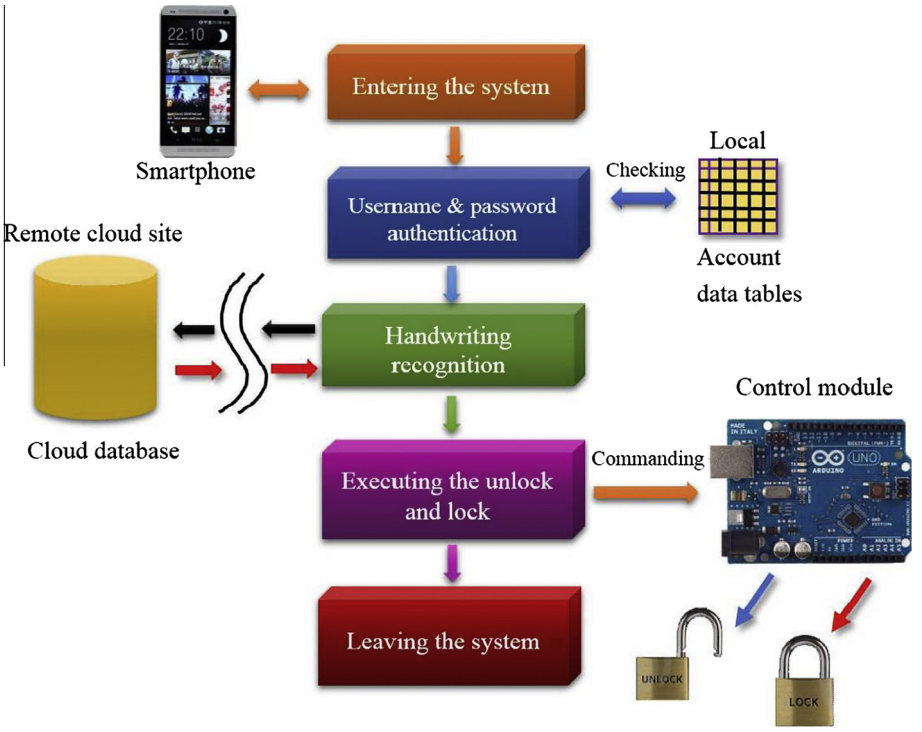

Fig. 1. Home security access control system step flow chart.

To address the above shortcomings, this paper proposes an innovative method of using mobile phones to handwrite identity words or symbols. This research is an extension of work reported in [17]. Cell phones are now widely used for sending voice and text messages and for using the Internet and Facebook [7]. Additionally, most users carry their phones at all times. Fig. 1 shows that the handwriting recognition method is the most critical focus of the system.

Fig. 1 shows the steps of the proposed system.

Step 1: Before entering the home, the user can link the smartphone with the access control system through Wi-Fi.
Step 2: This user inputs login account information including a user name and password in the login page. If the account authentication is successful, the system proceeds to step 3. If the user fails to authenticate three times, the system shuts down and locks the user out. The account information is based on a data table stored in the embedded system. At this stage, the web-based system uses JavaScript code to execute a correct judgment of the account. In exceptional circumstances the designer can use handwriting recognition for verification instead of the user name and password.
Step 3: The third stage is the handwriting recognition stage. The user must enter a previously registered handwriting sample for remote identification. Identification is performed using a remote machine for storing and computing original information stored in the cloud. Local devices can log into the remote system when the input word is recognized. The proposed system is designed for a private cloud, in which disruption is minimal for this function.
Step 4: When system identification is completed, the control module unlocks or locks the door.
Step 5: After completing the above steps, the user is automatically logged out of the system.

The cloud originally used the Windows Azure platform, and the database used the SQL Server. However, SQL Server has many unnecessary features, so the MySQL database was used instead. The table in step 2 is a general text and numerical list containing the username and password data. The graphics black point in the cloud database is defined as "1". The white point is defined as "0". When the user completes step 2, the web program is immediately connected to the handwriting recognition input page. All connected cloud initialization processes are executed in the background. Connecting to the cloud database is a two-way interactive process. The control module is a hardware unit. The control module starts whenever a command is executed.

Cloud computing is an extension of client–server applications that use the Internet to access resources stored on a server or data center in order to manage and reduce the burden on the client [8,9]. This concept resulted from the use of ubiquitous network services. Other purposes of the Cloud are to reduce duplication of large amounts of stored data and to maintain data synchronization.