Technical Disclosure Commons

Defensive Publications Series

January 06, 2016

SECURITY SYSTEM WITH AUTHENTICATION CODE AND ADAPTIVE PHOTO LOG

Alexander Faaborg

Ariel Sachter-Zeltzer

SECURITY SYSTEM WITH AUTHENTICATION CODE AND ADAPTIVE PHOTO LOG

ABSTRACT

A security system uses a camera to verify that a user trying to unlock a device with an authentication code is an authorized user and linked to that authentication code. The system receives an authentication code from the user trying to unlock the device. The system also captures an image of the user while the user enters the authentication code. The system compares the captured image of the user with one or more stored images of authorized users linked to the entered authentication code to determine whether the captured image matches one of the stored images of authorized users linked to the entered authentication code. Further, the system provides a notification about an unauthorized unlock attempt when the system is unable to confirm the authenticity of the user based on the image comparisons.

PROBLEM STATEMENT

Security systems generally rely on authentication codes distributed to a set of users authorized to have secure access to the security system. The users are required to enter a correct authentication code in order to unlock a device or enter through a secure-lock door. In such a scenario, the security systems can be rendered vulnerable if the authentication codes issued to authorized users are distributed to unauthorized users. The unauthorized users may use the authentication code to unlock the device or an electronic door lock and gain access to a device or location such as a car, a house, or an office. The system may not be able to decipher whether the authentication code was entered by an authorized user or an unauthorized user. Accordingly, a method and system to verify an authorized user entering an authentication code is described.

DETAILED DESCRIPTION

The systems and techniques described in this disclosure relate to a security system that visually verifies that a person using an authentication code to unlock a device is an authorized person. The system can be implemented for use in an Internet, an intranet, or another client and server environment. The system can be implemented locally on a client device or implemented across a client device and server environment. The client device can be any electronic device such as a mobile device, a smartphone, a tablet, a handheld electronic device, a wearable device, etc. or refrigerator, cooler, fridge, cold storage, chiller, any other physical storage appliance which has the ability to store food products, and other physical hardware like a door lock to a room or automobile, an electronic safe lock etc.

Fig. 1 illustrates an example method 100 to use images to verify authenticity of a user trying to unlock a device. The method 100 described herein can be performed by the security system.

As shown in Fig. 1, the system receives 102 an authentication code entered by a user to unlock a device. The authentication code may include a personal identification number (PIN), an alphanumeric password, a magnetic stripe card, a proximity card, a smart card, etc. The system can have the same authentication code for multiple users and/or different authentication codes for different users. The device can be any electronic device such as a mobile device, a smartphone, a tablet, a handheld electronic device, a wearable device, or a computing device, etc., or refrigerator, cooler, fridge, cold storage, chiller, any other physical storage appliance which has the ability to store food products, and other physical hardware like a door lock for a room or car, an electronic safe lock, etc.

Further, the system receives 104 an image of the user captured when the user enters the authentication code. The system may include an image capturing device, such as a still or video camera, capable of capturing images of a user entering an authentication code. The image capturing device can be a front or rear camera of a mobile device, a closed circuit television (CCTV) camera, or a video door-phone camera, etc. The image capturing device can be integrated in the system hardware or it can be a stand alone camera that may be placed either at the door or inside a user's home. The location of the image capturing device is such that it captures at least one image of a user entering the authentication code while attempting to unlock the device. The image capturing device is triggered to capture an image of a user whenever the user tries to unlock the device using an authentication code.

The system then determines 106 whether the received authentication code exists in a set of predetermined authentication codes. When the system is unable to find a match of the received authentication code within the set of pre-stored authentication codes, the unlock attempt is rendered invalid and the system waits to receive another authentication code. Alternatively, or additionally, the system may generate a notification if the number of unsuccessful attempts to enter the authentication code reaches a predetermined threshold. The notification can be sent to an account associated with a verified owner of the device or the house or car in case of a home or auto security system. The system can notify the verified owner using various notification techniques, e.g., a push notification, an email notification, a system generated message, a call, a warning alarm, or any audio/visual notification. The system can automatically set the predetermined threshold or the verified owner can input the predetermined threshold into the system during configuration. For example, the user can set the predetermined threshold as 4 unsuccessful attempts to unlock the device.

When the received authentication code is found within the set of pre-existing authentication codes, the system identifies 108 stored images previously captured when that received authentication code was previously entered at the device. The system may store images corresponding to one or more trusted users authorized to use a particular authentication code to unlock the device in a database. The database can be an adaptive database wherein the images of new trusted users can be added based on a predefined criteria. The predefined criteria for adding images of new trusted users in the database may include several conditions, e.g., entering a valid authentication code for a preset number of times by a single user, or sending a notification for approval to the verified owner for adding the image of a new user as a trusted user in the database. The images of new trusted users are stored corresponding to the valid authentication code entered by that user. This increases the flexibility of the system to accumulate new authorized users, hence reducing the hassle of updating the log of users for the verified owner.

Alternatively, or additionally, the verified owner can manually update the database with images of new authorized users corresponding to a valid authentication code. The system stores images of users corresponding to different valid authentication codes in the database such that images of more than one user can be linked to a single valid authentication code. Further, different images may also correspond to different authentication codes issued to different users. The database can be stored in a memory of the device, in a cloud server, or in an account associated with the device, etc.

The system determines 110 whether the received image of the user matches one of the stored images of authorized users. The face of the user in the received image is matched against faces in the stored images of the authorized users. The system can use various facial recognition

techniques or any other techniques known in the art, in order to determine the match of the received image with the stored images.

When the system determines that the received image of the user matches one of the images of authorized users stored against the corresponding authentication code received from that user, the system unlocks 112 the device. When the system is unable to verify that the user is an authorized user using both the authentication code and the image database, the system provides 114 a notification about the unlock attempt. The system can send the notification to the account of the verified owner of the device, house, office, or car about the unlock attempt. The notification can further include options for various actions such as providing the verified owner with an opportunity to confirm that the new user should have access to unlock the device, triggering an alarm inside the house in the case of a door lock security arrangement, or calling the police or security service agents, etc.

Fig. 2 illustrates an example scenario of an implemented security system 200. The system receives an authentication code, e.g. “YY22”, from a user trying to unlock a device. The code may be entered through a keypad 208, a microphone 210 in conjunction with a speech recognition function, etc. Additionally, the system receives 202 an image of the user captured by an image capturing component 212 while entering the authentication code. The system determines 204 whether the received authentication code is valid by comparing the received authentication code with the pre-stored authentication codes. When the system receives a valid authentication code, the received image of the user is compared 206 to the pre-stored images of users 206a, 206b, 206c, 206d corresponding to the authentication code “YY22”. The system utilizes various face recognition techniques or any other technique known in the art to verify whether the face of the user in the received image matches with one of the stored images of the

users authorized for that authentication code. The system unlocks the device if the received image matches at least one of the stored images of the relevant authenticated users. The system provides a notification about the unlock attempt if the user is not a valid user.

Fig. 3 is a block diagram of an exemplary environment that shows components of a system for implementing the techniques described in this disclosure. The environment includes client devices 310, servers 330, and network 340. Network 340 connects client devices 310 to servers 330. Client device 310 is an electronic device. Client device 310 may be capable of requesting and receiving data/communications over network 340. Example client devices 310 are personal computers (e.g., laptops), mobile communication devices, (e.g. smartphones, tablet computing devices), set-top boxes, game-consoles, and embedded systems. The other devices 310' that can send and receive data/communications over network 340 may include refrigerator, cooler, fridge, cold storage, chiller, any other physical storage appliance which has the ability to store food products, etc. and other physical hardware which may include electronic door lock, electronic safe lock, etc. Client device 310 may be similar to the security system 200 of FIG. 2 and include a camera element 312 to capture images of a user attempting to unlock the device. The database 313 may store images of various authorised users as discussed above in the description. The client device 310 further provides an appropriate graphical user interface (GUI) 314 for presenting an interface, e.g., in the form a virtual keypad such as keypad 208 of FIG. 2, in order to receive authentication code from a user. The client device may have a database 315 for storing the authentication codes/PINs which enable unlocking of the client device. Server 330 may be a web server capable of sending, receiving and storing web pages 332. Web page(s) 332 may be stored on or accessible via server 330. Databases for storing PINs 315' and images 313' can be stored at the server 330. When accessed, databases 315' and 313' may be transmitted and

displayed on a client device, e.g., 310. Native applications 316 may include various security applications for facial recognition and correlating the received images and PINs for authentication of a user to unlock the device. Resources 318 are resources available to the client device 310 and/or applications thereon, or server(s) 330, respectively. Resources 318 may be, for example, memory or storage resources; a text, image, video, audio, JavaScript, CSS, or other file or object; or other relevant resources. Network 340 may be any network or combination of networks that can carry data communication in order to perform communication in case of an unsuccessful/unauthorized unlock attempt at the client device 310.

The subject matter described in this disclosure can be implemented in software and/or hardware (for example, computers, circuits, or processors). The subject matter can be implemented on a single device or across multiple devices (for example, a client device and a server device). Devices implementing the subject matter can be connected through a wired and/or wireless network. Such devices can receive inputs from a user (for example, from a mouse, keyboard, or touchscreen) and produce an output to a user (for example, through a display). Specific examples disclosed are provided for illustrative purposes and do not limit the scope of the disclosure.

Drawings

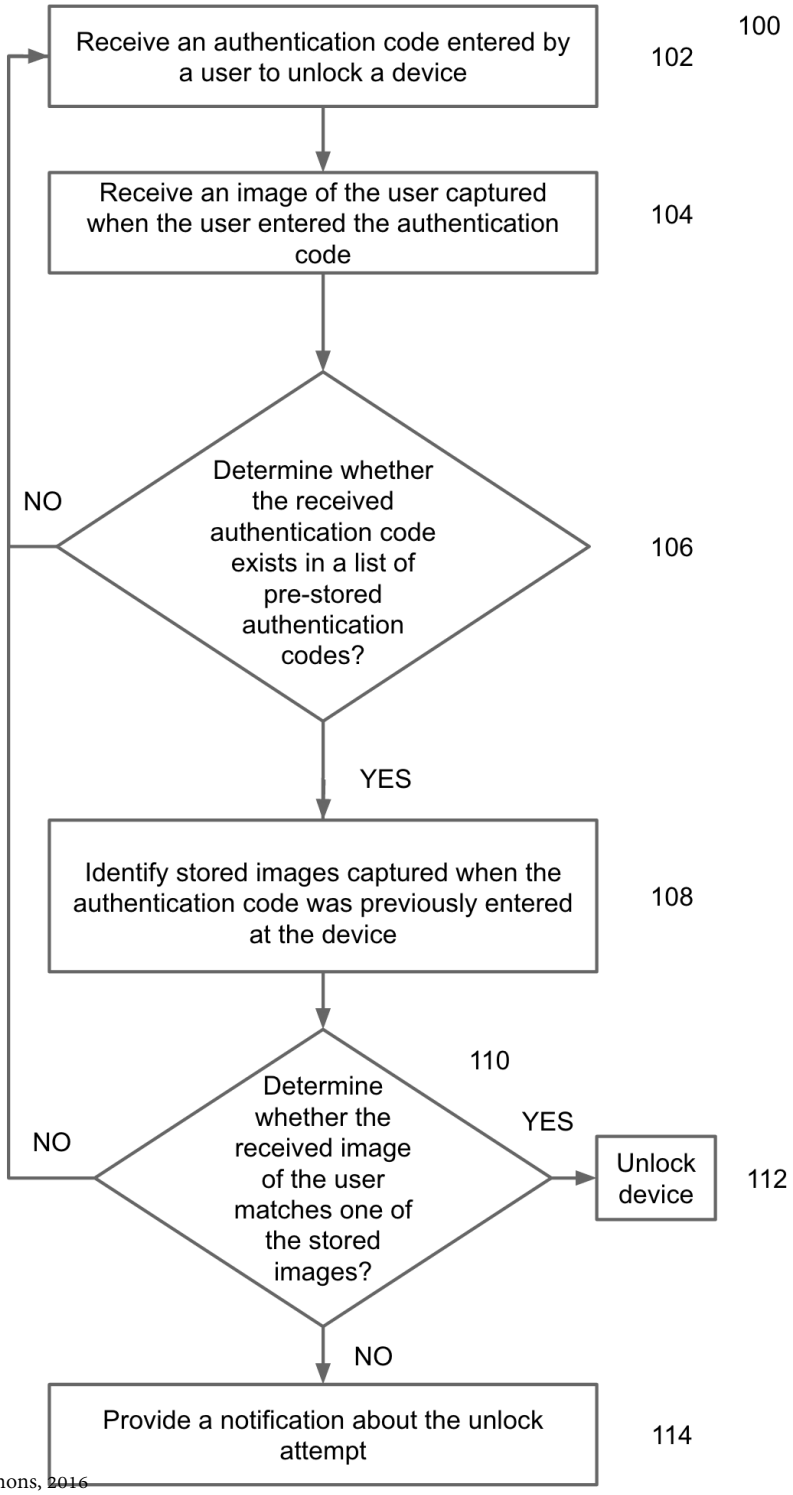
100
Receive an authentication code entered by a user to unlock a device
102
Receive an image of the user captured when the user entered the authentication code
104
Determine whether the received authentication code exists in a list of pre-stored authentication codes?
106
NO
YES
Identify stored images captured when the authentication code was previously entered at the device
108
110
Determine whether the received image of the user matches one of the stored images?
NO
YES
Unlock device
112
NO
Provide a notification about the unlock attempt
114

Fig. 1

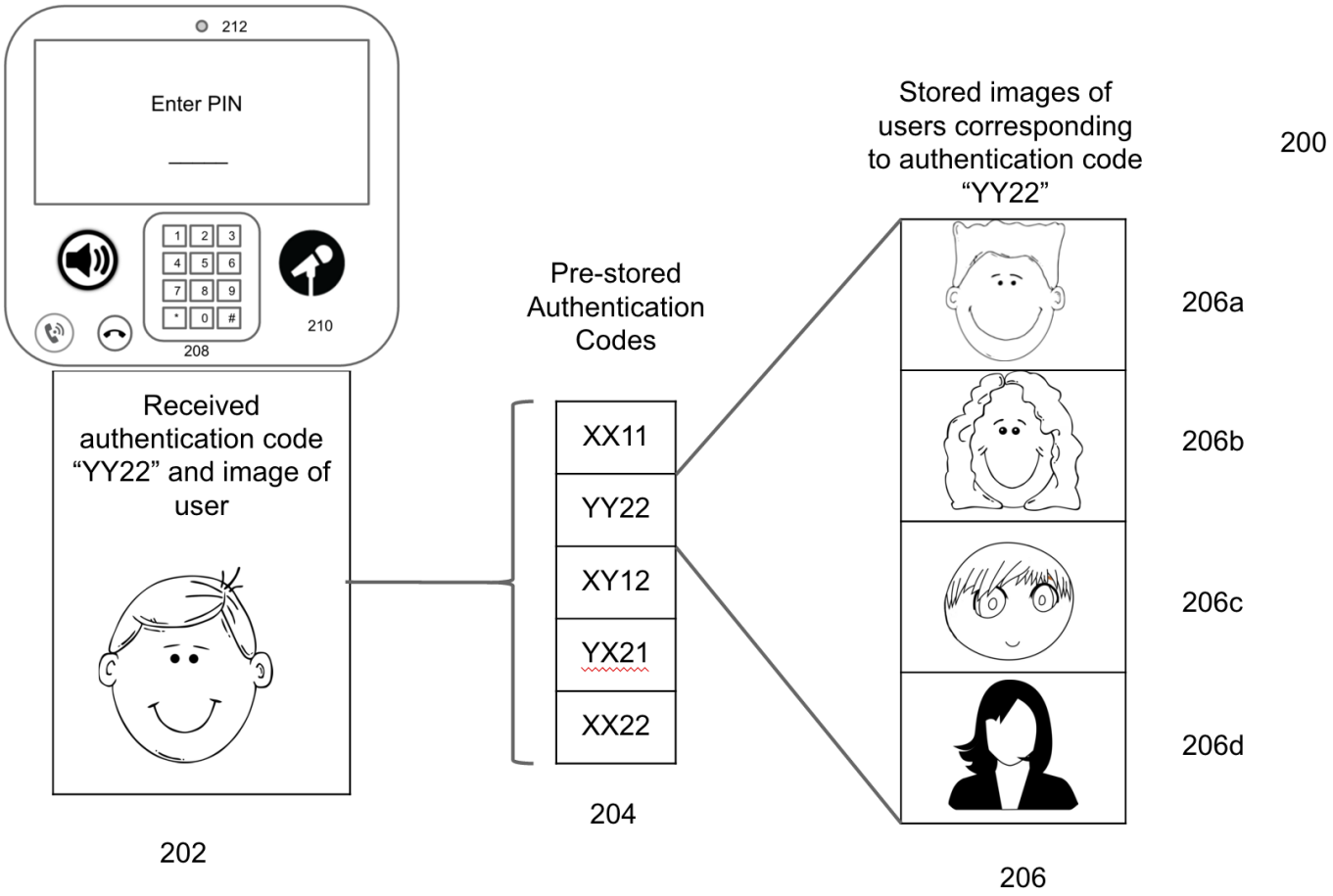
212
Enter PIN
1 2 3
4 5 6
7 8 9
* 0 #
208
210
Received authentication code "YY22" and image of user
202
Pre-stored Authentication Codes
XX11
YY22
XY12
YX21
XX22
204
Stored images of users corresponding to authentication code "YY22"
206a
206b
206c
206d
206
200

Fig. 2

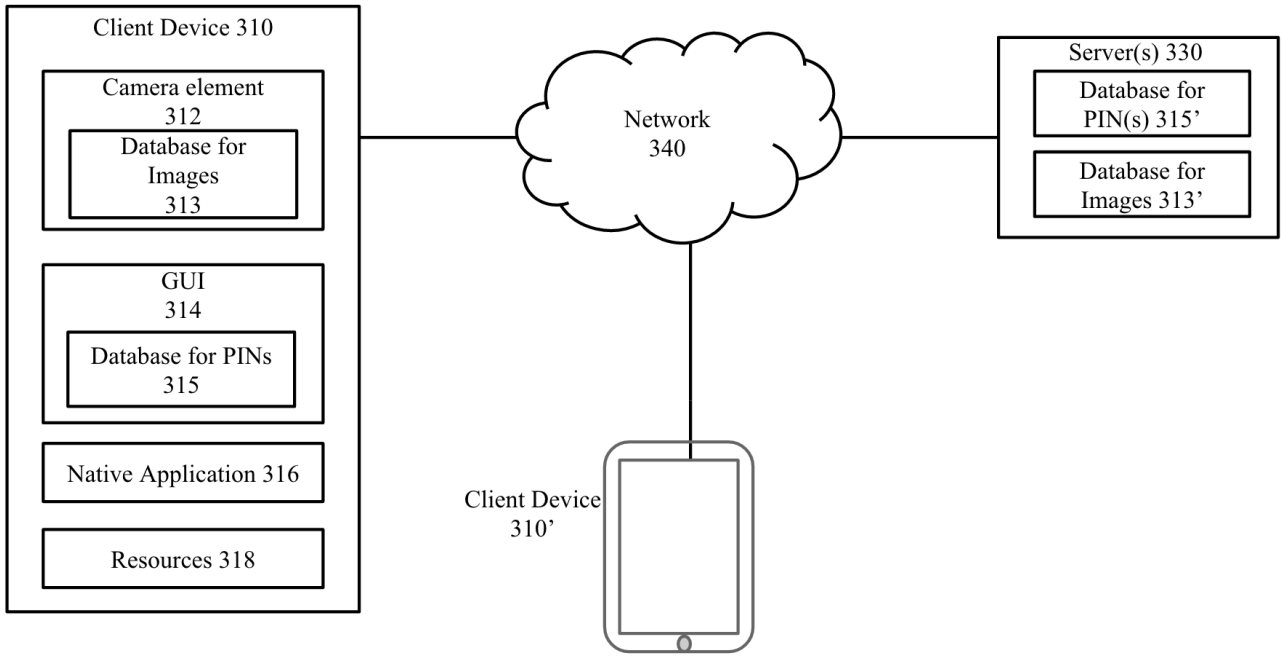
Client Device 310
Camera element 312
Database for Images 313
GUI 314
Database for PINs 315
Native Application 316
Resources 318
Network 340
Server(s) 330
Database for PIN(s) 315'
Database for Images 313'
Client Device 310'

Fig. 3