November 22, 2017

Authentication based on bioelectrical parameters

Matthew Robbins

Authentication based on bioelectrical parameters

ABSTRACT

Some current mobile devices authenticate users by verifying the user's fingerprint, the user's face, etc. Smartphones and other mobile devices are increasingly being designed to be smaller and thinner, with displays occupying a proportionately larger area of the surface of the device. Consequently, there is less area available near the top and bottom of the screen to place fingerprint or camera-based authentication hardware.

When users permit use of such data, techniques of this disclosure make advantageous use of unique electrical parameters of the human body, e.g., resistance, capacitance, and/or inductance between the fingers of a user's hand to authenticate the user. Standard electrical sensors are placed unobtrusively on the sides of the mobile device and are configured to measure a bioelectrical signature of the user. In this manner, user authentication is performed without use of traditional hardware, e.g., fingerprint or face recognition sensors, thereby freeing up additional space for display.

KEYWORDS

- Biometric authentication
- Bioelectrical signature
- Authentication
- Electrical sensor
- Mobile device
- Smartphone

BACKGROUND

Biometric user authentication in current mobile devices is based on technologies that require relatively large sensor areas. For example, both fingerprint and face recognition sensors comprise pixel arrays to collect a two- or three-dimensional image of the user’s fingerprint or face. These sensors consume valuable real estate on the front and/or back surface of a mobile device and within the device. As these sensors are commonly mounted on the front or back of the device, they impose limits on device thickness and design. Making a higher amount of free space available on the front surface of the device is even more challenging due to the demand for large screens that stretch from side-to-side and top-to-bottom without a bezel that is found in older generation devices.

DESCRIPTION

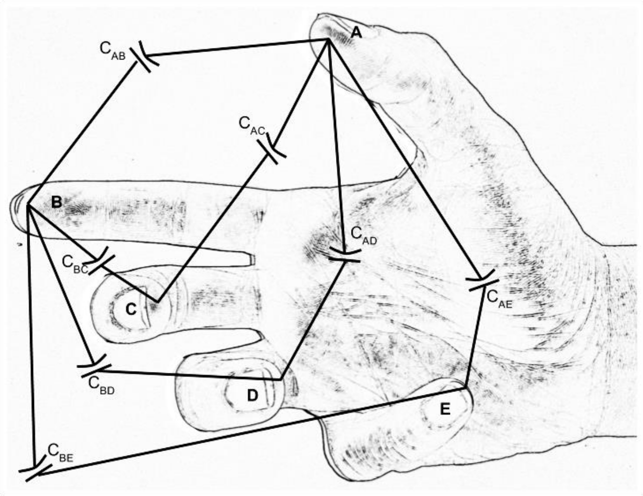

Fig. 1: Capacitances between fingers of the hand

The human body exhibits several unique bioelectrical patterns. For example, as shown in Fig. 1, there is a capacitance between every pair of fingers of a hand. Denoting the fingers as A, B, C, D, and E, the capacitance between a pair of fingers, e.g., A and B, is denoted C_{AB}. There being ten pairs of fingers for a hand (for simplicity, not all pairs are shown in Fig. 1), a capacitive characteristic for the human hand can be established, e.g., as a vector [C_{AB}, C_{AC}, … ,

C_{DE}] including up to ten entries. Such a vector is generally unique to a person, and can serve as an authenticating signature.

In a similar manner, a resistive signature (Fig. 2) and an inductive signature (Fig. 3) can be established.

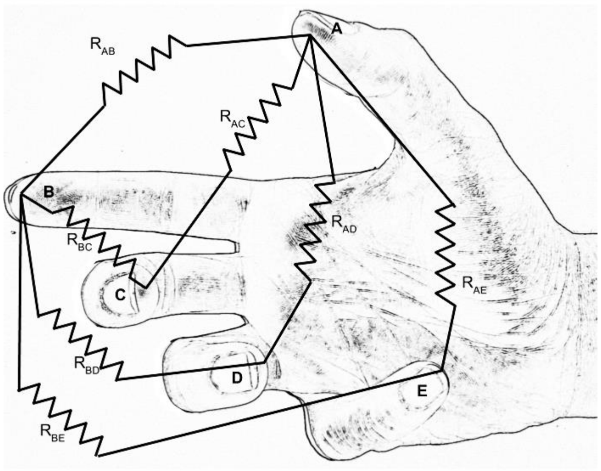

Fig. 2: Resistances between fingers of the hand

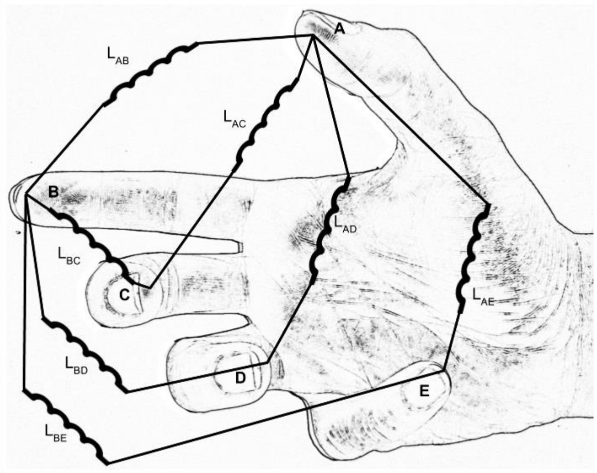

Fig. 3: Inductances between fingers of the hand

Considering capacitances, resistances (denoted by the letter *R*), and inductances (denoted by the letter *L*) between fingers of the hand, a signature vector of length up to thirty can be established, e.g., [C_{AB}, C_{AC}, … , C_{DE}, R_{AB} , R_{AC}, … , R_{DE} , L_{AB}, … , L_{DE}]. In addition to resistance, capacitance, and inductance, other bioelectrical parameters can be used to augment the signature vector. A longer signature vector, e.g., one that uses a combination of fingers and different parameters can improve the accuracy of the authentication.

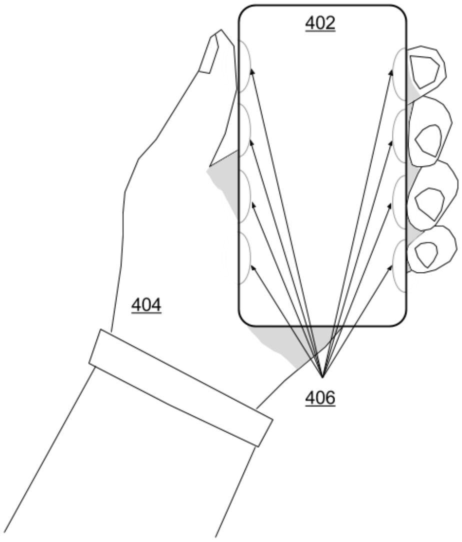

Fig. 4: Mobile device with bioelectrical signature authentication

Fig. 4 illustrates an example of authentication using the techniques of this disclosure. A user grasps a mobile device (402) using their hand (404). With user’s prior consent and permission for computation and use of bioelectrical signature for authentication, bioelectrical sensors (406) measure bioelectrical parameters of the user, e.g., resistance, capacitance, and/or inductance between the fingers of the hand. If the user refuses permission, no bioelectrical parameters are measured; instead, other authentication techniques are utilized. Further, bioelectrical parameters used for authentication may only be stored locally on the mobile device and used specifically for the purpose of authentication. The user is provided with options to select the authentication technique to use and to turn the sensors off.

Using the bioelectrical parameters, a signature vector is formed and the user is authenticated if the signature vector matches a pre-stored vector for the user. Although the sensors are shown representationally as being visible on the surface of the phone, in practice the sensors can be situated below the surface of the screen. With such an arrangement, no screen area is occupied by the bioelectrical sensors. The techniques of this disclosure apply to mobile phones as well as other consumer devices, e.g., wearable devices, laptops, tablets, home devices, etc.

Further to the descriptions above, a user may be provided with controls allowing the user to make an election as to both if and when systems, programs or features described herein may enable collection of user information (e.g., information about a user's social network, social actions or activities, profession, a user's preferences, or a user's current location), and if the user is sent content or communications from a server. In addition, certain data may be treated in one or more ways before it is stored or used, so that personally identifiable information is removed. For example, a user's identity may be treated so that no personally identifiable information can be determined for the user, or a user's geographic location may be generalized where location information is obtained (such as to a city, ZIP code, or state level), so that a particular location of a user cannot be determined. Thus, the user may have control over what information is collected about the user, how that information is used, and what information is provided to the user.

CONCLUSION

Techniques of this disclosure measure the bioelectrical parameters of a user that provides permission for such measurement, and use the parameters to authenticate the user. Bioelectrical sensors are placed unobtrusively on a device in such a manner that screen area is not occupied. Techniques of this disclosure thereby accurately authenticate a user while freeing up screen space.