March 2020

Camera-assisted Fingerprint Registration and Authentication

MinDa Deng

Craig Hesling

Camera-assisted Fingerprint Registration and Authentication

ABSTRACT

This disclosure describes the use of a camera, e.g., webcam, during fingerprint registration and fingerprint based authentication of users on laptops. Images from the camera are utilized to guide finger placement and fingerprint capture during fingerprint registration and to provide additional information during subsequent fingerprint based authentication. A user interface is provided to guide the user to position the laptop lid at an angle such that the fingerprint reader lies within an angle of view of the laptop webcam. Images obtained from the webcam are utilized to estimate the position of the finger placement and to determine the fingerprint model associated with the user. During fingerprint authentication, the webcam is used to estimate finger identity and position to determine an order of checking the acquired fingerprint against the registered fingerprint templates. This enables secure authentication since additional time can be allocated to the authentication algorithm for each match attempt. Motion detection is utilized to determine that a user is about to perform fingerprint based authentication to automatically activate the webcam.

KEYWORDS

- Biometric authentication
- Fingerprint
- Fingerprint sensor
- Fingerprint reader
- Motion sensor
- Webcam
- Hinged device

BACKGROUND

Fingerprint based authentication is a commonly included feature in computing devices such as laptops. Fingerprint based authentication is performed by comparing a user's fingerprint to previously obtained and stored fingerprint template(s) of registered users. During registration, fingerprints of multiple fingers of users that are authorized to access the device are captured and stored as templates. When a user attempts to access the device using fingerprint authentication, the live fingerprint is compared against the multiple fingerprint templates stored on the device. A detection threshold is commonly used to match the live fingerprint with a previously stored (registered) fingerprint template. When users place their fingers on the fingerprint sensor (reader), they can use any of their fingers for authentication, as long as a fingerprint from that finger was previously registered.

There is usually a tradeoff between speed and security (accuracy) in the authentication process since the fingerprint is matched against all stored fingerprint templates. Heuristic algorithms are utilized to determine an order of checking; however, performing the comparison can still be time-consuming when the registry includes a large number of fingers and/or users. Fingerprint readers (sensors) with smaller surface areas pose additional challenges since the portion of the finger placed by the user on the reader may not precisely match the area of the finger placed during registration.

DESCRIPTION

This disclosure describes the use of a camera (e.g., a laptop webcam) during fingerprint registration and fingerprint based authentication of users on computing devices such as laptops. Per techniques of this disclosure, images from the webcam are utilized to guide finger

placement and fingerprint capture during fingerprint registration and to provide finger pose information during subsequent fingerprint based authentication.

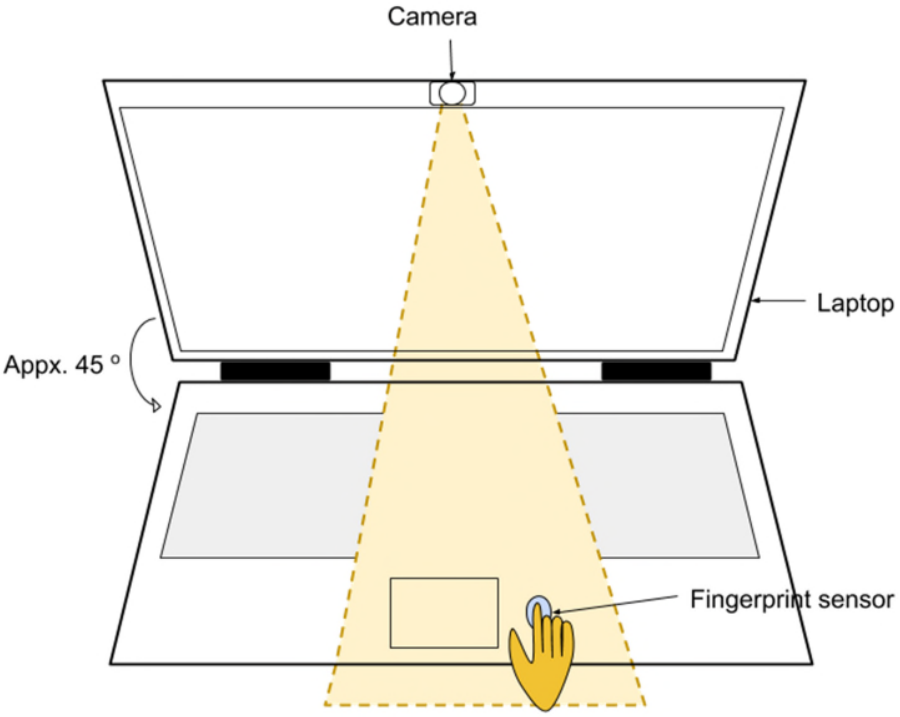

Fig. 1: Camera-assisted Fingerprint Registration and Authentication

Fig. 1 illustrates example use of webcam assisted fingerprint authentication, per techniques of this disclosure. This illustrative example depicts a user registering their fingerprint(s) on a hinged device such as a laptop. A user interface (not shown) is provided to guide the user to position the laptop lid at an approximate angle of 45 degrees to the laptop base such that the fingerprint reader (sensor) lies clearly within an angle of view of the laptop camera (webcam).

Images obtained from the camera are utilized to determine an estimated position of finger placement with respect to the fingerprint reader. The position information is utilized in the determination of the fingerprint model associated with the user. The position information is

also utilized to reject fingerprint readings taken from unintended areas, for example, from finger portions below the finger joint or from a different finger, etc.

When fingerprint based authentication is attempted subsequently for user access to the computing device, the camera is utilized to estimate user pose (finger identity and position relative to the sensor). For example, images from the webcam can be utilized to determine which of the user's fingers is placed on the fingerprint reader. The user pose is utilized to determine the sequence of checking the acquired fingerprint against the registered fingerprint templates. This enables secure authentication since additional time can be allocated to the authentication algorithm for each match attempt in addition to enabling use of a higher match threshold in the authentication. This provides higher accuracy of authentication without sacrificing speed.

Additionally, motion detection techniques can be utilized to determine that a user is about to perform fingerprint based authentication and to activate the camera. For example, a motion sensor can be placed in or near the fingerprint sensor, which can trigger the camera operation to obtain images of the finger pose.

Techniques of this disclosure can also be used to enforce system policy for authentication. For example, single user access and/or a policy that specifies the presence of a particular user for high security applications is enabled by use of camera images in conjunction with the fingerprint based authentication. A fingerprint sensor can be placed in the device lid such that it is difficult for the user to touch the sensor in the expected orientation unless the device is in the expected orientation with respect to the user and in view of the camera.

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 the user's fingerprint or finger pose, user's image). 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. Thus, the user has control over what information is collected about the user, how that information is used, and what information is provided to the user.

CONCLUSION

This disclosure describes the use of a camera, e.g., webcam, during fingerprint registration and fingerprint-based authentication of users on laptops. Images from the camera are utilized to guide finger placement and fingerprint capture during fingerprint registration and to provide additional information during subsequent fingerprint-based authentication. A user interface is provided to guide the user to position the laptop lid at an angle such that the fingerprint reader lies within an angle of view of the laptop webcam. Images obtained from the webcam are utilized to estimate the position of the finger placement and to determine the fingerprint model associated with the user. During fingerprint authentication, the webcam is used to estimate finger identity and position to determine an order of checking the acquired fingerprint against the registered fingerprint templates. This enables secure authentication since additional time can be allocated to the authentication algorithm for each match attempt. Motion detection is utilized to determine that a user is about to perform fingerprint-based authentication to automatically activate the webcam.