October 08, 2018

Authentication Using Sparse Modeling of Fingerprint Images

Firas Sammoura

Matthew Robbins

Authentication using sparse modeling of fingerprint images

ABSTRACT

Fingerprint sensors often have difficulty authenticating users if the user's fingers are wet or moist, e.g., due to sweat. This disclosure presents robust techniques for fingerprint identification based on the K-SVD algorithm, which is a technique to represent images in a sparse manner. A K-SVD dictionary is created out of enrolled fingerprint images. A fingerprint that is to be authenticated is segmented into blocks, and each block is projected against the dictionary. A heat map of highest projection coefficients is formed, and overall match-score is calculated. The overall match-score is used to authenticate the fingerprint. The dictionary stores the essential features of the enrolled fingerprints, and the enrolled fingerprint images are deleted. Fingerprint authentication is made possible without actual storage of the enrolled fingerprints, which serves to improve security.

KEYWORDS

- biometric authentication
- fingerprint identification
- sparse modeling
- singular value decomposition
- K-SVD
- orthogonal matching pursuit
- dictionary update

BACKGROUND

Fingerprint sensors often have difficulty authenticating users under specific operating conditions, e.g., if the user's fingers are wet, moist, or sweaty. This is true of most fingerprint sensors, including those based on capacitive or ultrasonic technologies. Specifically, moist fingers create fingerprint images with regions of low contrast, e.g., as shown in Fig. 1.

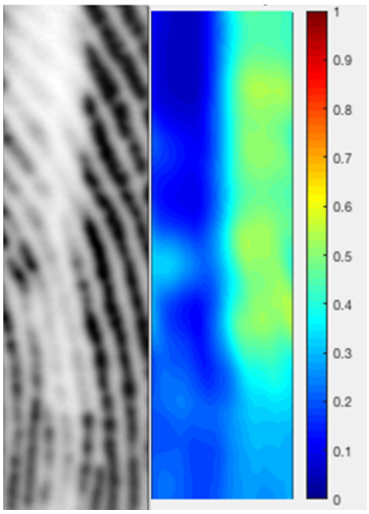

Fig. 1: An example low-contrast fingerprint image, with heat map corresponding to level of contrast

DESCRIPTION

This disclosure presents robust techniques for fingerprint identification based on sparse modeling of fingerprint images. The K-SVD algorithm is used to build a dictionary of enrolled fingerprint images. The dictionary comprises building-block features of the fingerprint. A fingerprint that is to be authenticated is projected, e.g., using dot-product, against the dictionary to detect match.

The K-SVD algorithm [1][2] is a method of representing images in a sparse manner. It is based on a mathematical technique used to orthogonally factorize matrices, known as singular value decomposition (SVD). Under K-SVD, a given image (**x**), segmented into overlapping

blocks and arranged vectorially, is represented as the matrix product of a *K*-column dictionary matrix (**D**) and a sparse matrix ($\underline{\boldsymbol{\alpha}}$):

$$\underline{\mathbf{x}} = \mathbf{D}\underline{\boldsymbol{\alpha}}$$

The dictionary **D** is trained using singular value decomposition over a number of training images, such that at the end of training it encapsulates features of the training images. Training is typically an iterative process wherein each dictionary update is followed by the discovery of an optimally sparse $\underline{\boldsymbol{\alpha}}$, using, e.g., orthogonal matching pursuit. The initial value of **D** is typically a discrete cosine transform matrix. The *K* columns of **D** are also referred to as the atoms or elements of the dictionary. An example of an image and its corresponding 64-element dictionary is shown in Fig. 2.

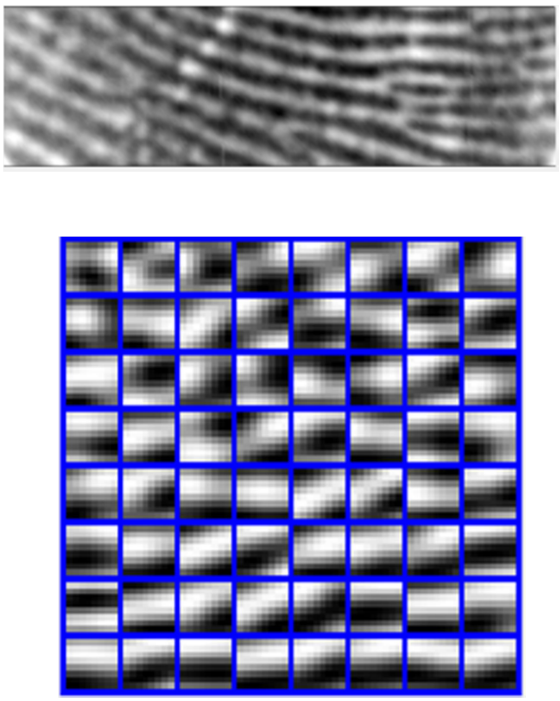

Fig. 2: (a) An example image, and (b) corresponding 64-element dictionary

At the close of training, e.g., when the dictionary **D** converges, any image with statistics similar to those of the training images is sparsely representable. As a further step, an image that is presented after training can itself update anew the dictionary, achieving even greater sparsity.

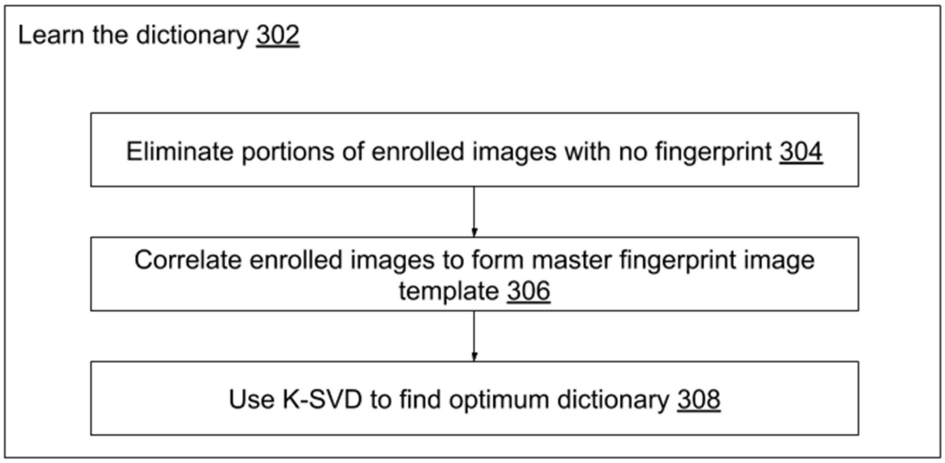

Fig. 3: Learning the dictionary from a set of enrolled fingerprint images

Per the techniques of this disclosure, as illustrated in Fig. 3, the set of enrolled fingerprint images is used to learn the dictionary (302). At the end of learning, the major features of the enrolled fingerprints are embedded within the dictionary. The dictionary is later used to authenticate fingerprints presented for verification.

Portions of fingerprint images that have no fingerprint are eliminated using segmentation techniques (304). Enrolled images are correlated to find, and correct for, their respective translations or rotations. Once translations/rotations are corrected, a master fingerprint image template is formed (306). K-SVD is used to find an optimum dictionary (308). Every element of the dictionary is normalized.

During learning, an objective is to map each image block to an atom (element) of the dictionary. Another objective is to find the optimum number of the *K* uncorrelated dictionary elements/atoms that best represent the image blocks. The choice of the *NxN* block size for the

biometric matcher dictionary is relatively large, e.g., $N=32$, so as to increase the dimensionality of the problem and the uniqueness of the dictionary to the finger signature. For different fingers, dictionaries are separately learned, then concatenated. The dictionary can be adapted periodically offline.

Once the dictionary is trained, there is no need to store the enrolled fingerprint images or any extracts thereof. The dictionary essentially stores building-block features of the enrolled images. Fingerprint authentication is made possible without actual storage of the enrolled fingerprints, which serves to improve security.

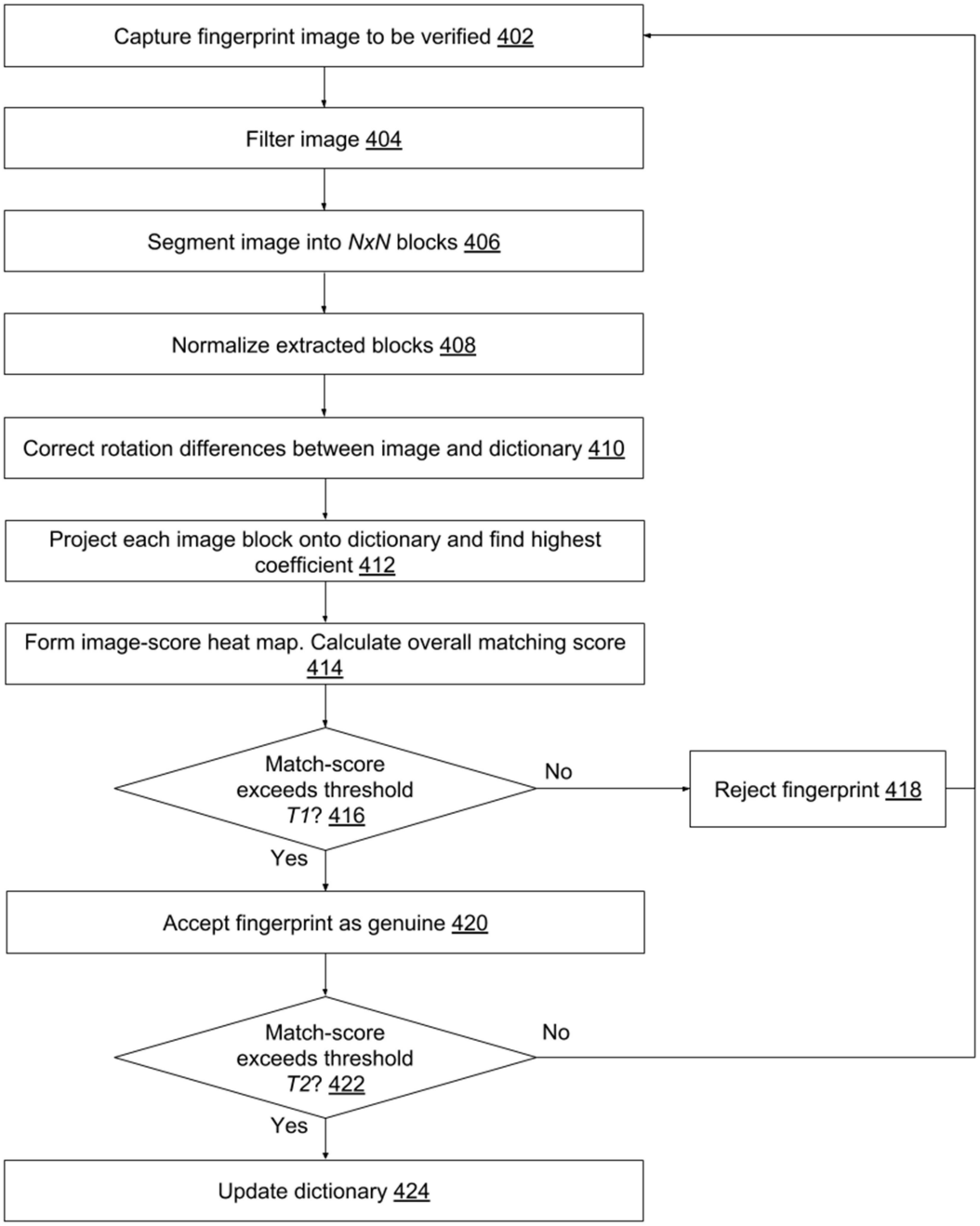

Fig. 4: Fingerprint authentication

Fig. 4 illustrates fingerprint authentication per techniques of this disclosure. An image of the fingerprint to be authenticated is captured (402), filtered (404), and segmented (406) into *NxN* blocks. For high-quality images, the filtering step may be omitted. The extracted blocks are normalized (408). One or more image blocks are checked against dictionary elements to find

rotation differences between image and dictionary (410), and these differences are corrected. Each image block is projected onto the dictionary, using, e.g., matrix multiplication. The resulting projection coefficients are ranked, and the highest one is selected (412).

A heat map is created out of the highest projection coefficients of the image blocks. An overall matching score is calculated from all the blocks across the image (414). The matching score is used for authentication as follows. If the matching score exceeds a predetermined threshold *T1* (416), the fingerprint is accepted as genuine (420); if not, the fingerprint is rejected (418). If the matching score meets a second threshold *T2* (422), the associated fingerprint image is used to update the dictionary (424) with features not thus far present in the dictionary.

Update of the dictionary (424) with a recently captured image of high matching score is done as follows. The captured image is segmented to extract the foreground portion of the fingerprint. A basis, e.g., candidates for potential dictionary atoms, is determined for the new image. A cross-correlation is performed between the existing dictionary and the new (candidate) dictionary elements. If the cross-correlation is greater than a predetermined threshold, e.g., 0.99, then the candidate dictionary element is redundant and need not be added. If the cross-correlation is lesser than the threshold then the candidate dictionary element is added to the threshold. If a dictionary element was not used for the past n, where n is, e.g., 30, filtering operations, it is removed.

The number K of atoms in the dictionary is determined as follows. The number of dictionary atoms is initialized to a small number, e.g., 64 or thereabouts. A figure-of-merit is defined that captures the sparsity of the K-SVD representation of the image. Several iterations of dictionary update are performed before evaluating the figure-of-merit. If the figure-of-merit is

greater than unity, then the number *K* of atoms in the dictionary is increased. This process is repeated until the figure-of-merit is close to unity.

An image rotation is detected at 410 using *P N3xN3* blocks and verified using a dictionary of *L N2xN2* blocks, where *N3>N2* or *N3<N2*.

Although the techniques herein have been described in the context of fingerprint authentication, they apply generally to other forms of image-based biometric identification.

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

Fingerprint sensors often have difficulty authenticating users if the user's fingers are wet or moist, e.g., due to sweat. This disclosure presents robust, smart, and fast techniques for fingerprint identification based on the K-SVD algorithm, which is a technique of sparse modeling of images. A K-SVD dictionary is created out of enrolled fingerprint images. A fingerprint that is to be authenticated is segmented into blocks, and each block is projected

against the dictionary. A heat map of highest projection coefficients is formed, and overall match-score is calculated. The overall match-score is used to authenticate the fingerprint. The dictionary stores all essential features of the enrolled fingerprints, and the enrolled fingerprint images are deleted. Fingerprint authentication is made possible without actual storage of the enrolled fingerprints, which serves to improve security.

REFERENCES

[1] Aharon, Michal, Michael Elad, and Alfred Bruckstein. "K-SVD: An algorithm for designing overcomplete dictionaries for sparse representation." *IEEE Transactions on signal processing* 54, no. 11 (2006): 4311.

[2] Rubinstein, Ron, Alfred M. Bruckstein, and Michael Elad. "Dictionaries for sparse representation modeling." *Proceedings of the IEEE* 98, no. 6 (2010): 1045-1057.