DETECTING FINGERPRINT ALTERATIONS BY ORIENTATION FIELD AND MINUTIAE ORIENTATION ANALYSIS

John Ellingsgaard[1,2], Ctirad Sousedik[1], Christoph Busch[1]

[1]Norwegian Biometrics Laboratory
Gjøvik University College
Teknologiveien 22
2815 Gjøvik, Norway
ctirad.sousedik@hig.no
christoph.busch@hig.no

[2]Technical University of Denmark
Anker Engelunds Vej 1
2800 Kgs. Lyngby, Denmark
jellingsgaard@hotmail.com

ABSTRACT

The ever wider application of automatic fingerprint recognition systems to law enforcement and immigration control purposes has motivated attempts to avoid identification by fingerprint alterations. The subjects can try to change their fingerprint patterns in many ways, varying from fingertip abrading, burning and cutting up to sophisticated surgical procedures, and therefore a necessity exists for an automatic detection of altered fingerprints. This paper proposes a novel method for fingerprint alteration detection based on analysis of anomalies in minutia orientations and the fingerprint ridge structure caused by scarred regions.

1. INTRODUCTION

The long and rich history of fingerprint biometrics in forensic sciences has proven the fingerprint to be a reliable means of uniquely identifying an individual. Nowadays, large international databases, containing hundreds of millions of records, enable reliable tracking of criminal records as well as efficient immigration control. The increasing usage of fingerprints at country borders has significantly increased the motivation of blacklisted individuals to avoid successful identification by altering their fingerprints. Apart from the well-known attacks using an artificial fingerprint, individuals can also try to alter their fingerprint patterns to such extent that the automatic system is unable to link them with their originally enrolled reference fingerprint samples. Fingerprint alterations vary from abrading, cutting and burning the fingertips, up to sophisticated surgical operations that can provide a new valid fingerprint pattern for an individual. One of the first recorded attempts to perform a fingerprint alteration was the case of the bank robber, John Dillinger, who tried to avoid identification by burning his fingerprints with an acid as early as in 1934 [1]. More recently, individuals have been registered having their fingerprints altered using a surgical procedure that involves a Z-shaped cut of the fingertip skin and exchanging the position of the two skin pieces. In 2009, a woman having her fingerprints fully transplanted between her left and right hand has been recorded in an attempt to cross Japanese borders. On a larger scale, fingerprint alterations have been reported regarding the EU asylum seeker register, EURODAC. Changes to the fingerprint pattern by burning, abrading or cutting have been identified for hundreds of subjects.

Given the extent and level of automation involved in the usage of fingerprints for forensic and immigration control at present, there is a need to automatically spot subjects that have intentionally altered their original fingerprint pattern. The recent international standardization efforts in this area that are conducted in ISO/IEC JTC SC37 define the fingerprint alteration detection as part of the task of Presentation Attack Detection that involves detection of various attempts to deceive fingerprint biometric systems by means of a non-genuine representations [2].

This paper suggests a novel method for detection of such altered fingerprints by analyzing the captured image representation and revealing inconsistencies in the ridge flow.

The text is organized as follows: The summary of the existing publications regarding fingerprint alteration detection is given by Section 2. Section 3 presents the proposed analysis and detection approach and its performance is evaluated in Section 4. Conclusions and suggestions for future work are given by Section 5.

2. RELATED WORK

A limited amount of previous work exists on the topic of detection and analysis of altered fingerprints. Feng et al. [3] compute the fingerprint orientation field and decompose it into singular and continuous components. The singular component is determined by positions and characteristics of the singular points in the analysed fingerprints. Using the singular decomposition and the original orientation field, a continuous component can be computed. An SVM classification

978-1-4799-4370-8/14/$31.00

into altered and unaltered fingerprints is performed using histograms of curvatures present in the continuous component of the orientation field. The authors claim that, unlike in unaltered fingerprints, the altered fingerprints yield for continuous orientation field components in which the continuous flow of the orientations is not preserved. The approach was tested using a synthetic database of altered fingerprints. Yoon et al. [4] approach the problem both by analysis of anomalies in the orientation field and minutia distributions. The orientation field is extracted and its polynomial approximation is computed. For the altered fingerprints, the difference between the polynomial approximation and the original orientation field is be greater than for the unaltered fingerprints, since the polynomial presentation is not able to represent the anomalies precisely. In addition, the authors observed that the scarring, often present in altered fingerprints, generates accumulations of minutiae that are not observed in unaltered fingerprints. A histogram based on the distributions of minutia in the fingerprints is used as the second part of a feature vector for SVM classification into unaltered and altered fingerprints. The method was tested on a large-scale non-public government database containing 4433 samples of altered fingerprints. Petrovici and Lazar [5] propose a method based on reliability of the fingerprint orientation field. The authors observed that for the unaltered fingerprints, a small number of actual fingerprint singular points can be detected with a high degree of confidence. For the altered fingerprints, on the other hand, the anomalies provide for a larger number of detected singular points, typically with a low degree of confidence. Due to the lack of a public database of altered fingerprints, the authors demonstrate their method on a set of unaltered fingerprints and examples of altered fingerprints. The authors have also experimented with a classifier based on the Mahalanobis distance for the fingerprint alteration detection [6]. In this approach, the fingerprint orientation field is extracted and divided into blocks. Separately for the altered fingerprints and the unaltered fingerprints in the training set, the blocks with low orientation field reliability are used to compute a model of a block. The fingerprints are classified into altered and unaltered as based on the Mahalanobis distance of the orientation field blocks in a test fingerprint from the models representing altered or unaltered fingerprints. A synthetic database of fingerprint alterations has been used by the work. Petrovici [7] has also proposed a method for generating of synthetically altered fingerprints from unaltered fingerprint samples. Tiribuzi et al. [8] have proposed a method based on minutia distributions and entropies of orientations in fingerprints. The fingerprint orientation field is divided into blocks, and for each of the blocks, entropy of the orientations is calculated. Considering 3 different scale settings, 3 different orientation entropy maps are extracted. From the orientation entropy maps along along with a minutia density map, histograms are computed and used to classify fingerprints as altered or unaltered. The approach was tested on a database of synthetically generated altered fingerprints.

3. ALTERATION DETECTION METHOD

3.1. Dataset

In biometric research, it is commonly expected that proposed methods are based on publicly accessible datasets, such that research results can be reproduced. For the research addressed in this work such a dataset does not exist. Due to the nature of the target characteristic of interest, it is neither possible to ask volunteers in large numbers to alter their fingerprints nor conduct a dedicated data collection. Seemingly, a possibility would be in using the forensic and immigration control databases. However, the individuals typically seek to avoid criminal prosecution or blacklisting by immigration control authorities, and the altered fingerprints, if identified, are still subject to legal protection. This limitation forced the researchers working in this field to test their methods either using synthetically generated datasets of altered fingerprints or to benchmark them with the very few datasets that do contain altered fingerprint sample. The proposed method was tested on a dataset of non-synthetic altered fingerprints composed from the following sources:

- Brno [9]. A collection of fingerprints containing a wide variety of dermatological diseases.
- GUC-100 [10]. An *in-house* database from Gjøvik University College (GUC) in Norway. A few images containing dermatological diseases have been used as altered.
- Samischenko [11]. The book *Atlas of the Unusual Papilla Patterns* by S.S. Samischenko contains a large collection of fingerprint images with unusual fingerprint patterns together with some natural ones. The database contains fingerprints from fingers altered by burns, acid burns, transplantation, miscellaneous injuries, and diseases.
- NIST SD14 - fingerprints that have been identified as altered in the NIST Special Database 14

Moreover we added non-altered images from public sources [10] FVC 2004 [12]. For the FVC 2004 Images from DB1 (set A) of the public fingerprint database collected for the Fingerprint Verification Competition 2004 (FVC 2004) have been used as unaltered images. The resulting dataset contains 116 altered and 180 unaltered fingerprint images normalized to the size 512×480 pixels.

3.2. Preprocessing

All fingerprint samples have been preprocessed in order to enhance the image and minimize the amount of background that

would have a disturbing effect on the algorithm. The initial cropping of the fingerprint foreground area was done using the *Nfseg* algorithm from the NIST Biometric Image Software (NBIS) package [13]. A finer segmentation into blocks of size 8×8 pixels containing the background or the fingerprint pattern is done using the per-block standard deviation approach. On the resulting map of foreground blocks, a series of morphological $open$ and $close$ operations is applied in order to close the holes in the foreground area that represents the fingerprint and remove isolated, erroneously detected, foreground blocks. The morphological operation step is essential in order to obtain a fingerprint area containing low-quality blocks of the scarred and mutilated areas, as the blocks containing the scarred regions are often discarded as the background by the standard deviation approach. The fingerprints are then rotated to the longitudinal orientation by using the approach taken by Merkle et al. [14] and resized to 512×480 pixels.

For the Singular Point Density Analysis described further on, the image is also subjected to histogram equalization and enhanced using the following block-wise FFT approach described by Watson et al. [15]. The image is divided into 8×8 blocks $B(\mathbf{x})$ where each of the blocks is considered with an 8-pixel margin, providing for a set of 8×8 overlapping blocks of size 24×24 pixels. Each of the blocks is FFT-enhanced according to the following equation

$$B'(\mathbf{x}) = FFT^{-1}(FFT(B(\mathbf{x})) \cdot |FFT(B(\mathbf{x}))|^k) \qquad (1)$$

where $k = 0.45$ is the enhancement constant. The enhanced image is then re-assembled using the central 8×8 pixels in the blocks $B'(x, y)$.

3.3. Singular point density analysis

The patterns caused by scarring and mutilations introduce anomalies in the pixel-wise orientation field of the fingerprint scan. The anomalies can be perceived as additional singularities in the orientation field that can be identified by approaches intended for detection of actual singular points in genuine fingerprints. The Poincaré index [16], $P(x, y)$, is typically used as the first step in identifying the singular, core and delta, points in a fingerprint.

$$P(x, y) = \sum_{k=0..7} a(d_k, d_{(k+1) \bmod 8}), \qquad (2)$$

$a(d_i, d_j)$ represents the angle between point orientations d_i and d_j selecting the direction of the orientations so that $|d_j - d_i| \leq \pi/2$, while k is the index of orientation points surrounding the position (x, y). In high quality unaltered fingerprints, the values of the Poincaré index can be interpreted as follows

$$P(x, y) = \begin{cases} 2\pi, & \text{if } (x, y) \text{ belongs to a whorl} \\ \pi, & \text{if } (x, y) \text{ belongs to a loop} \\ -\pi, & \text{if } (x, y) \text{ belongs to a delta} \\ -2\pi, & \text{if } (x, y) \text{ belongs to a } \textit{diamond} \text{ shape} \\ 0, & \text{otherwise} \end{cases} \qquad (3)$$

Due to the anomalies that exist in the altered fingerprint images, the Poincaré index yields a significantly larger number of points as candidates for singular points as regards the altered fingerprint images in comparison to the unaltered fingerprint images. Therefore, the amount and distribution of the points detected by the Poincaré index provide for a measure to distinguish between altered and unaltered fingerprints. However, low quality areas in genuine fingerprint scans can increase the number of falsely detected singular points in a similar fashion [17]. In order to filter out the singular point candidates detected in low quality areas of a fingerprint sample and preserve only the singular point candidates from the altered areas, the Gabor filter based quality assessment has been applied.

In the quality assessment approach by Olsen et al. [18], the fingerprint image is convolved with a 2D Gaussian core, and the result is subtracted from the original image in order to obtain its high-pass filtered representation. The representation is convolved with 2D Gabor filters of $n = 8$ evenly spread orientations θ.

$$\theta = \pi \frac{k-1}{n}, \quad k = 1, .., n \qquad (4)$$

A pixel-wise standard deviation is computed among the images in the resulting Gabor filter response bank, providing for the quality image G_{std}. The Gabor quality matrix, G_{std}, is then transformed into the interval $[0, 1]$ according to

$$Q_G(x, y) = \begin{cases} G_{std}(x, y)/T, & \text{if } G_{std}(x, y) \leq T \\ 1, & \text{otherwise} \end{cases} \qquad (5)$$

where T is a given threshold ($T = 0.01$).

Given a fingerprint image quality map $Q_G(x, y)$, a quality dependent singular point density image $P_d(x, y)$ is computed by multiplication of the two maps as follows

$$P_d(x, y) = P(x, y) \cdot Q_G(x, y) \qquad (6)$$

The final representation is obtained by convolution of the image $P_d(x, y)$ with a uniform circular window of radius $r = 30$ pixels and smoothening by using a Gaussian filter of 30×30 pixels. The pipeline is illustrated by Fig. 1.

3.4. Minutia orientation analysis

An altered fingerprint typically exhibits anomalies in the ridge orientation flow caused by scarring along the cuts and mutilations. In an unaltered fingerprint, it is very unlikely to

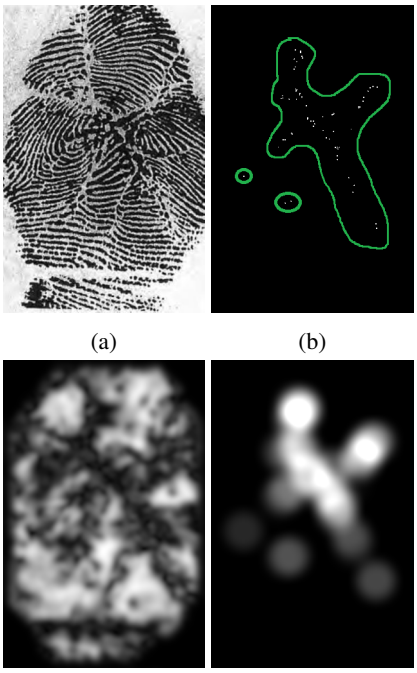

Fig. 1. (a) Original [11], (b) Poincaré index response, (c) Quality image Q_G, (d) The resulting Singular Point Density map

find minutiae of very different orientations in close proximity. In altered fingerprints, the scars introduce additional clusters of minutiae that often do not follow the expected orientation flow. The Minutia Orientation Analysis extracts patterns based on differences of orientation of minutiae in close proximity to one another.

For the analysis, a *mindct* minutia extractor, subjected to slight modifications, has been used. In order to remove falsely detected minutiae, the *mindct* includes a filtering step that greatly reduces the number of initially detected minutiae. However, the additional minutiae generated by scarring and other anomalies in the altered fingerprints are typically detected with a low level of confidence and removed during the filtering procedure. In order to preserve the low-confidence minutiae, the following slight modifications were performed on the *mindct* minutia extractor. The functionality that removes minutiae arising from momentary discontinuities in the ridges or valleys has been disabled entirely. In addition, the angle parameter for removal of minutiae arising from short islands or lakes in the ridge flow has been experimentally tuned to $157.5°$, in order to reduce the amount of minutia candidates removed in the scarred regions.

The minutia orientation differences are computed as follows. Let $\mathbf{S_m} = \{(\mathbf{x}, \theta)\}$ be the set of fingerprint minutiae containing the minutia's position $\mathbf{x} = (x, y)$ and orientation $\theta \in [0, \pi)$. For each minutia $m \in \mathbf{S_m}$, the minutiae around its center within the radius r are considered. Within the radius r, a minutia is found that provides for largest difference $\Delta\theta_m$ between its orientation and the orientation of the minutia m as shown by Fig. 2.

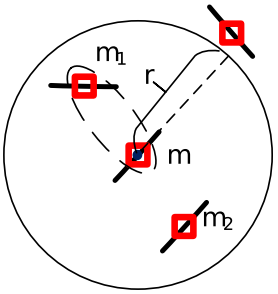

Fig. 2. Selection of the minutia with maximum difference in orientation compared to minutia m, within the radius r

The orientation difference $d(\theta_i, \theta_m)$ is defined as follows

$$d(\theta_i, \theta_m) = \min(|\theta_i - \theta_m|, \pi - |\theta_i - \theta_m|) \tag{7}$$

The resulting set $\mathbf{S_{diff}}$ contains minutia positions $\mathbf{x}$ and the above mentioned maximum orientation differences $\Delta\theta_m$ to the minutia within the radius r

$$\mathbf{S_{diff}} = \{(\mathbf{x}, \Delta\theta_m) | (\mathbf{x}, \theta) \in \mathbf{S_m}\} \tag{8}$$

The values $\Delta\theta_m$ in the set $\mathbf{S_{diff}}$ are then transformed into the interval $[0, 1]$ according to definition

$$\mathbf{M_{diff}} = \{(\mathbf{x}, \theta_t) | (\mathbf{x}, \Delta\theta_m) \in \mathbf{S_{diff}} \wedge \theta_t = s(\Delta\theta_m)\} \tag{9}$$

where the function $s(\theta)$ is defined as

$$s(\theta) = \begin{cases} \theta/T, & \text{if } \theta \leq T, \\ 1, & \text{otherwise} \end{cases} \tag{10}$$

and T is a predetermined threshold (T is set to $\pi/4$).

A density map $M_{dens}(\mathbf{x})$ of the size of the fingerprint image is computed as follows

$$M_{dens}(\mathbf{x}) = \sum_{(\mathbf{x_0}, \theta_t) \in \mathbf{M_{diff}}} \theta_t K_r(\mathbf{x} - \mathbf{x_0}) \tag{11}$$

where $K_r(\mathbf{x} - \mathbf{x_0})$ is a circular window function centered at $\mathbf{x_0}$ with a radius r (r is set to 30 pixels).

The image M_{dens} is then filtered by a Gaussian filter of size 30×30 and its values transformed by means of the function n defined as

$$n(v) = \begin{cases} v/T, & \text{if } v \leq T, \\ 1, & \text{otherwise} \end{cases} \tag{12}$$

with a parameter T ($T = 6.9$). The resulting image is illustrated by Fig. 3c.

(a) (b) (c)

Fig. 3. (a) Original [11], (b) detected minutia, (c) resulting minutia orientation difference density

Table 1. Classification results.

Method	Analysis	TADR	FNADR
Yoon et al.[19]	OFA	93.7%	3.2%
	MDA	77.5%	7.9%
Proposed	SPDA	92.0%	2.3%
	MOA	81.6%	5.5%
Feature level fusion	**OFA/SPDA**	**94.6%**	**2.4%**

4. RESULTS

Both the resulting density maps from the Singular Pont Density Analysis (SPDA) and Minutia Orientation Analysis (MOA) are classified using the approach used by Yoon et al. [19]. The density maps are cropped into a rectangular shape, normalized into the interval $[0, 1]$ and divided into 3×3, in total 9, blocks. For each block, a 21-bin histogram is computed that represents the distribution of the density values in the interval $[0, 1]$. For each of the density maps, all the histograms for all of the blocks are then concatenated into a single 189-dimensional feature vector that can be used for classification.

For performance comparison, the approach by Yoon et al. [19] was fully reimplemented. The method provides for two additional density maps resulting from the Orientation Field Analysis (OFA) and Minutia Distribution Analysis (MDA) that yield for a 189-dimensional feature vector each. The results of the classification using Support Vector Machines, averaged over 10 independent selections of training and testing data, are listed in Table 1. For the altered fingerprints 30% of the data were randomly chosen as the training set, and 70% of the data as the testing set.

The results are presented in terms of the True Altered Detection Rate (TADR) and False Non-Altered Detection Rate (FNADR) metrics [2]. The TADR metric is the proportion of altered presentation characteristics correctly classified as being altered. The FNADR metric is the proportion of altered presentation characteristics incorrectly classified as being non-altered.

The feature level fusion of the newly proposed SPDA approach and the existing OFA approach provided for the best performance, outperforming the method by Yoon et al.[19]. In addition, two new approaches to fingerprint alteration detection have been introduced, providing for performance fully comparable to to the methods introduced by Yoon et al.[19].

5. CONCLUSION AND FUTURE WORK

A novel method for detecting altered fingerprints has been developed that performs competitively with the state-of-the-art method by Yoon et al.[19], achieving TADR of **92.0%** and FNADR of **2.3%** on the classification dataset. In addition, the classification performance can be further improved to TADR of **94.6%** and FNADR of **2.4%** by combining the approach of Yoon et al. [19] and the proposed method. The future work would involve testing on a larger dataset of altered fingerprints from government sources such as the FBI database of altered fingerprints that has been used by Yoon et al.[19] as a second source of validation. In addition, a further investigation is possible regarding identification of the pixel-wise orientation field anomalies, currently performed by means of the Poincaré index, by using analysis of the entropies of the orientations.

6. ACKNOWLEDGEMENTS

The authors would like to thank Anil Jain (Michigan State University), Christophe Champod (Universite de Lausanne), Martin Drahansky (Brno University of Technology, Faculty of Information Technology - STRaDe) and FN Olomouc that kindly provided access to the altered fingerprint data used in this work. This work is carried out under the funding of the EU-FP7 INGRESS project (Grant No. SEC-2012-312792).

7. REFERENCES

[1] Harold Cummins, "Attempts to alter and obliterate finger-prints," *Journal of Criminal Law and Criminology*, vol. 25, pp. 982–991, 1935.

[2] ISO/IEC 5th WD 30107 International Organization for Standardization, *Information Technology - Biometrics - Presentation attack detection*, ISO/IEC, 2013.

[3] Jianjiang Feng, A.K. Jain, and A. Ross, "Detecting Altered Fingerprints," in *Pattern Recognition (ICPR), 2010 20th International Conference on*, aug. 2010, p. 16221625.

[4] Soweon Yoon, Jianjiang Feng, and A.K. Jain, "Altered Fingerprints: Analysis and Detection," *Pattern Analysis*

and Machine Intelligence, IEEE Transactions on, vol. 34, no. 3, pp. 451464, march 2012.

[5] A. Petrovici and C. Lazar, "Identifying fingerprint alteration using the reliability map of the orientation field," *The Annals of the Univeristy of Craiova. Series: Automation, Computers, Electronics and Mechatronics*, vol. 7(34), no. 1, pp. 45–52, 2010.

[6] A. Petrovici and C. Lazar, "Detection of altered fingerprints using a mahalanobis distance based classifier," in *Control Systems and Computer Science (CSCS18), 2011 Proceedings of 18th International Conference on*, 2011, pp. 604–611.

[7] A. Petrovici, "Simulating alteration on fingerprint images," in *Biometric Measurements and Systems for Security and Medical Applications (BIOMS), 2012 IEEE Workshop on*, 2012.

[8] M. Tiribuzi, M. Pastorelli, P. Valigi, and E. Ricci, "A multiple kernel learning framework for detecting altered fingerprints," in *Pattern Recognition (ICPR), 2012 21st International Conference on*, 2012, pp. 3402–3405.

[9] "Fingerprint database. Alterations caused by diseases.," March 2013, Faculty of Information Technology at Brno University of Technology and the research group STRaDe in collaboration with dermatologists from FN Olomouc.

[10] Davrondzhon Gafurov, Patrick Bours, Bian Yang, and Christoph Busch, "GUC100 Multisensor Fingerprint Database for In-house (Semipublic) Performance Test," *EURASIP Journal Information Security*, vol. 2010, pp. 3:1–3:11, Jan. 2010.

[11] S.S. Samischenko, *Atlas of the Unusual Papilla Patterns / Atlas Neobychnykh Papilliarnykh Uzorov*, Urisprudentsiia, Moscow, 2001.

[12] Maio Maltoni Cappelli, D. Maio, D. Maltoni, J. L. Wayman, and A. K. Jain, "FVC2004: Third Fingerprint Verification Competition," in *in Proceedings of the First International Conference on Biometric Authentication*, 2004, pp. 1–7.

[13] C. Watson, M. Garris, C. Tabassi, and R. M. Wilson, "NIST Biometric Image Software," december 2012, http://www.nist.gov/itl/iad/ig/nbis.cfm.

[14] Johannes Merkle, Heinrich Ihmor, Ulrike Korte, Matthias Niesing, and Michael Schwaiger, "Performance of the Fuzzy Vault for Multiple Fingerprints (Extended Version)," *CoRR*, vol. abs/1008.0807, 2010.

[15] C. I. Watson, G.T. Candela, and P.J. Grother, "Comparison of FFT Fingerprint Filtering Methods for Neural Network Classification," *NISTIR*, vol. 5493, 1994.

[16] Masahiro Kawagoe and Akio Tojo, "Fingerprint pattern classification," *Pattern Recogn.*, vol. 17, no. 3, pp. 295–303, June 1984.

[17] Jie Zhou, Fanglin Chen, and Jinwei Gu, "A novel algorithm for detecting singular points from fingerprint images," *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, vol. 31, no. 7, pp. 1239–1250, July 2009.

[18] M.A. Olsen, Haiyun Xu, and C. Busch, "Gabor filters as candidate quality measure for NFIQ 2.0," in *5th IAPR International Conference on Biometrics (ICB)*, 2012, pp. 158–163.

[19] Soweon Yoon, Jianjiang Feng, and Anil K. Jain, "Altered Fingerprints: Analysis and Detection," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 34, no. 3, pp. 451–464, 2012.