

# Bridging Biometrics and Forensics

Yanjun Yan and Lisa Ann Osadciw

EECS, Syracuse University, Syracuse, NY, USA

{yayan, laosadci}@syr.edu

## ABSTRACT

This paper is a survey on biometrics and forensics, especially on the techniques and applications of face recognition in forensics. This paper describes the differences and connections between biometrics and forensics, and bridges each other by formulating the conditions when biometrics can be applied in forensics. Under these conditions, face recognition, as a non-intrusive and non-contact biometrics, is discussed in detail as an illustration of applying biometrics in forensics. The discussion on face recognition covers different approaches, feature extractions, and decision procedures. The advantages and limitations of biometrics in forensic applications are also addressed.

**Keywords:** biometrics, forensics, face recognition

## 1. INTRODUCTION

Biometrics used in forensics and general legal matters, such as the drawings of the wanted and the ink fingerprints on legal documents, dates back when paper was invented. With the development of computing devices from last century, the automatic biometric recognition techniques were developed rapidly within the last two decades. Currently biometrics is generally used in secure building entrance system, border control, Civil ID and login verification. The commercial biometric systems by DigitalPersona,<sup>1</sup> Cognitec,<sup>2</sup> L1 Identity,<sup>3</sup> Sensiblevision<sup>4</sup> etc. start to appear around the world. However, the application of biometrics in forensics is not fully studied, nor is biometrics implemented widely in forensics. The relatively parallel development of biometrics and forensics starts to intersect only from early of this decade. Bruegge compared biometrics with forensics<sup>5</sup> in 2004. IEEE started publishing Transactions on Information Forensics and Security in 2006. Richard V. There were several research projects on applying biometrics in forensics such as by Harry Wechsler et. al.<sup>6,7</sup> and Govindaraju, V. et. al.<sup>8,9</sup> However, there have not been much more literature on this issue. This paper aims at bridging biometrics and forensics by discussing their differences and connections, and formulating the conditions when the biometrics can be applied in forensics. Under these conditions, one biometrics, face recognition, is applied in forensic scenarios as an illustration.

Biometrics in general means the statistical study of biological phenomena. It includes all possible bi-measurements on live subjects, such as human, plants and animals. But currently biometrics usually means the measurement on humans. In biometric applications, human characteristics are acquired in order to differentiate human individuals.<sup>10</sup> The measurable characteristics include biological information from body parts and behavior information from movements. Biological measurements can be from face, fingerprint, iris, retina, ear, teeth, hand geometry, skin and possibly many other modalities in development. Behavior information can be from voice, signature or other handwritten scripts, gait, keyboard stroke etc. Many of these measurements have already been utilized in forensics, but in traditional forensics, expert knowledge, manual comparison and sorting are generally needed. Biometrics automates the identification process with accuracy and speed, and it is therefore desirable in forensics.

## 2. BIOMETRICS AND FORENSICS

Biometrics is briefly discussed in this paragraph. There are two kinds of biometric recognition tasks: one is verification, the other is identification. Verification is to decide whether the user is whom he/she claims to be, which is a one-to-one match. Identification is to select the subject identity from all available identities in the database, which is a one-to-many match. In identification, if it is known for sure that the subject is within the database, then it is a closed set problem; otherwise if the subject may be outside of the database, then it is an open set problem. Biometrics is usually applied in real-time, and the decision of acceptance or refusal occurs

immediately, so that the person who tries to access the system will be granted or denied the access right on the spot.

Forensics is discussed in this paragraph. Forensics is defined by Merriam-Webster's dictionary as the application of scientific knowledge to legal problems; especially: scientific analysis of physical evidence (as from a crime scene). In forensics, the evidence from an event is analyzed off-line afterwards, instead of in real-time. What evidence can be found and what analysis can be implemented totally depends on the individual case.

The differences of applying biometrics and forensics are briefed as above, but the appropriate real-time techniques of biometrics can be implemented to off-line analysis of evidences, then biometrics, either verification or identification, can be readily applied in forensics with adaptation.

## **2.1. Differences between Biometrics and Forensics**

Besides the pre-event and post-event natures of biometrics and forensics,<sup>5</sup> one other big difference between biometrics and forensics is that in biometrics, the subjects are usually very cooperative, since they want to get recognized and gain the access; however, in forensics, the criminals do not want to get recorded nor recognized, and they are not cooperative while their biometrics are recorded. The criminals may use masks, wear makeup, make funny expressions or assume weird positions, all of which causes more challenges for biometric identification.

Meanwhile, biometric systems are usually constructed with the state-of-the-art data capturing devices, and once the recognition task is done, the instantly captured data need not to be stored; thus it's affordable to take biometric data with high clarity. However, in forensics, the surveillance system may not be up to date, and as a common practice, a long duration of data are stored; thus the data captured in forensics are commonly with low resolutions and low update rate, which limits the application of certain biometric methods.

On the other hand, biometrics are implemented on live subjects, and intrusive techniques are not desirable. However, in forensics, the biological data may be collected from the deceased, and the techniques can be more intrusive. The reconstruction of live representation from the intrusive measurements is generally needed to implement biometric recognition techniques.

## **2.2. Connections of Biometrics and Forensics**

Although the goals of biometrics and forensics are different, the techniques designed for biometrics can be utilized for forensic purposes.

For instance, in protecting cybersecurity, identity verification is essential. Biometrics identifies the user by whom the user is, instead of what the user has, and is more accurate than using password etc. If there's any event occurring, the identity information within the network is readily usable for forensics.

Another typical scenario in forensics is that the identify of the suspect or victim is unknown, and based on the slim evidence, the possible identities need to be rendered and sorted. This process is analogous to the open set identification in biometrics or image retrieval. If the evidence in forensics is from multiple modalities such as from both face and fingerprint, multi-modal decision can be made based on multi-modal biometrics.

## **2.3. Conditions of Applying Biometrics in Forensics**

There are many different kinds of biometrics. The conditions for a biometrics to work reliably depend on the specific biometrics and the recognition techniques for that biometrics. In general, the conditions of using a biometrics include:

1. The acquired data meets the minimal requirement on clarity, resolution, size or duration.
2. There are enough data to train the classifier off-line. Also, in watch list applications, an accurate watch list should be available.
3. The thresholds or other parameters of the classifier to trade off between the false acceptance rate and false rejection rate should be carefully tuned according to the security level of current situation.

4. Further, given a single biometrics and a specific algorithm to analyze this biometrics, the algorithm needs to be adjusted such as by selecting appropriate features, constructing robust templates and considering suitable compression.

Therefore, the evidence in forensics that can be analyzed by biometric techniques should meet aforementioned conditions. If the original evidence barely meets the aforementioned conditions, enhancement needs to be implemented first. If enhancement is involved, the creditability of the analysis is lowered, but this may help an expert in decision making. Or if the enhanced evidence is still not usable, then this evidence may not be suitable for biometric processing. Some enhancement or reconstruction techniques are discussed as follows.

If the data captured are images such as of face, fingerprint and iris with low resolution, super resolution techniques<sup>11</sup> can be applied on multiple images to construct a high resolution image before these images are used for verification purpose. Super resolution technique takes advantage of camera shifting or aliasing in image capturing process to register the low resolution images in sub-pixel level and interpolate to enhance the resolution.

If sketches are available drawn by forensic artists based on witnesses' description, there are other hallucination techniques to generate a picture-like image for biometric verification purpose.<sup>12-17</sup> For example, in face recognition, the low resolution images are projected onto low resolution eigenfaces to derive their coordinates in the feature space, and the coordinates are utilized in high resolution eigenface space to reconstruct high resolution images.<sup>18</sup>

If partial images are occluded, the aforementioned hallucination techniques,<sup>19,20</sup> combined with expert knowledge, can help forensic artists to reconstruct a facial image. If no images are available, the bone structure etc. may be used to derive the parameters for a 3D face model and finally reconstruct the facial images.

The procedure that is not as important in forensics as in common biometrics is probably the segmentation on the evidence. Segmentation separates the region of interest from its background for further recognition. In biometrics, the segmentation needs to be done quickly and relatively accurately, which is usually done automatically. But in forensics, every piece of evidence may have already been scrutinized by the experts, and a very accurate segmentation can be done manually.

### 3. ILLUSTRATION BY FACE RECOGNITION

As described in sec. 2.3, the same techniques used in biometrics can be used for forensic purposes. Face recognition is non-intrusive and non-contact, and there is a good chance that facial image evidence exists in forensics. In this section, face recognition is discussed in detail to illustrate the application of biometrics in forensics. Currently a surveillance system such as CCTV (Closed Circuit Television) becomes more and more affordable and popular. It is a common practice to monitor secure locations such as banks, ATM branches, shops, hotels, parking lots or a secure living complex. All the saved images or videos become powerful evidences if crime occurs. In the meantime, with the prevalence of cameras and camera cell-phones, when there is something disturbing happening, personally recorded images and videos are spread instantly on websites such as Flickr, YouTube, all of which supplement the surveillance system, and sometimes even intrigue the investigation. The ideal case for forensics is that the faces of the suspects or victims can be detected from the images or videos and recognized by biometric techniques.

#### 3.1. Face Recognition Techniques

Face recognition techniques are roughly classified into the following categories.

- Template based: A typical template-based method is PCA (Principle Component Analysis) based eigenface method, which uses holistic information of the face. The eigenfaces are extracted from the training images.<sup>21</sup> The face images of the people on the watch list are projected onto the eigenface space, and the coordinates are stored as templates to compare with evidence images. There are other transforms based on LDA (Linear Discriminant Analysis) or ICA (Independent Component Analysis), and the templates are associated with the transforms.

- Feature based: Features are descriptions or quantitative measurements of local facial features such as eyes, nose and mouth for direct comparisons.<sup>22</sup> The local features need not to be organs, but are meaningful objects occupying partial image. The local features segmented from the facial image do not have to be used altogether, the features can be further selected for better performance.<sup>23,24</sup> The features can be generalized as responses to Gabor filters etc.<sup>25,26</sup>
- Rule based: A learning algorithm, such as support vector machine (SVM), decision tree, neural network or Bayesian network, is trained on the available dataset, which constitutes an explicit or implicit set of rules. The rules are evaluated over the evidence image to reach a final decision.
- Model based: The most popular models include elastic-bunch-graph (EBG) model and hidden Markov model. In EBG analysis, the bunch graph is constructed from a small set of sample image graphs. Recognition is based on a straightforward comparison of image graphs.<sup>27</sup> In hidden Markov model analysis, the strips tessellate the facial image are assumed to be related by the hidden Markov model. In both models, the model parameters are fitted to the training images, and each subject has a distinctive model. The recognition is based on the fitting of the models. Generally in 3D face modeling and analysis, the model fitting is also essential.<sup>26,28,29</sup>
- Module based: Facial modules are similarly defined or detected as local features, but modules are analyzed as self-contained components.<sup>30</sup> The features, scores or decisions from modules can be also combined together to reach a fused result.<sup>31</sup> The fusion at both score level and decision level is shown to improve the recognition performance.

### 3.1.1. Feature extraction

In this section, the *feature* is defined as a general term to represent whatever quantity that needs to be evaluated in aforementioned face recognition techniques. Namely, the *feature* is the template in template based methods, the *feature* is the local feature measurements in feature based methods, the *feature* is the rule or structure in rule based methods, the *feature* is the fitted model in model based method, or the *feature* is the module output in module based method.

*Feature* extraction is implemented off-line before the evidence is analyzed by a particular processing technique. The *features* are associated with this particular processing technique, which involves the following two steps.

**Training set construction:** The knowledge of the face recognition system comes from the training data, which must be representative of the users, or subjects on the watch list. If such a training dataset is not big, all data should be used. However, the learning curve assumes such a pattern that adding images into the training set does not improve *feature* extraction after reaching a certain point. Therefore, if an optimal training set can be selected such that not much further information can be extracted if more training images are added, the calculation power in processing more training images is saved, and the overfitting problem is alleviated.<sup>32</sup>

**Feature selection:** When the training dataset is representative enough, the *features* that have bigger differentiation power are further selected and used in actual evaluation. The *features* that are representative but not very differentiating can be omitted. *Feature* selection helps the recognition performance. On the other hand, *feature* selection shares the same advantages of constructing an efficient training set to save calculation power and alleviate overfitting problem. Even though the objective functions of the two steps are different, *feature* selection is concurrent with training set construction to some extent. When the training set is small, the percentage of selected features is big; when the training set is big, the percentage of selected features is small.

### 3.1.2. Recognition

After the *features* are extracted, the recognition decision is made by classifier. In some recognition methods, such as by SVM, the features and classifier are co-designed. This section is focused on classifier design. The classifier for face recognition can be a binary classifier to differentiate the imposter and the user, or a multi-ary

classifier with each user belonging to a hypothesis. Multi-ary classifier design involves the division of the high dimensional feature space and is complicated by the curse-of-dimensionality problem. Depending on the security level, the thresholds for a multi-ary classifier should be more carefully selected than binary classifier.

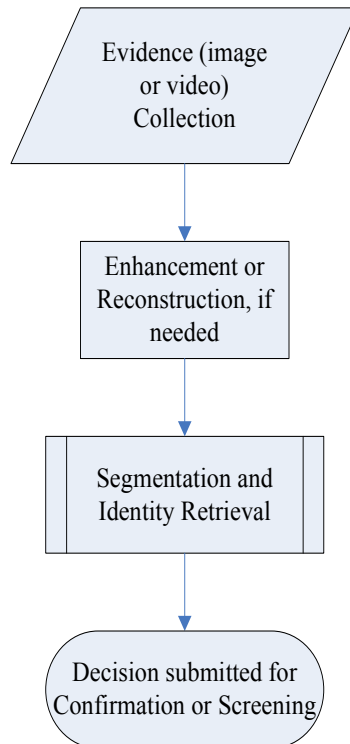
When there are multiple classifiers such as in modular mono-modal biometrics or multi-modal biometrics, the threshold for each classifier is adjusted according to the performance of each classifier, which is effective in improving the fused result.<sup>33</sup>

### 3.2. Face Recognition in Forensics

In forensic scenarios, face recognition can be used to verify an identity or retrieve possible identities from a database. Verification is implemented by face recognition techniques described in sec. 3.1 so long as the to-be-verified identity is known to the face recognition system. Identity retrieval is more complex, especially when the database is huge. Currently the driver's license system, passport system, US-VISIT border control program are all digitized, and the images constitute a huge database as a potential retrieval database.

A challenge in face recognition is scalability. When the database is small, the recognition is accurate, but when the database is much bigger, the feature space is more densely partitioned, and the recognition is more challenging. Given a big potential retrieval database captured by the government, data compression<sup>34</sup> and pyramid searching<sup>35-38</sup> are essential for identity retrieval. Each image is decomposed by the wavelet transform, and the lower band coefficients constitute a shrunk version of the original image. The computation cost is lowered when testing image is compared with the database by lower resolution versions. A video or sequence information is also usable to enforce the recognition result<sup>39,40</sup> by consistency checking and scenario identification.

The procedure of applying face recognition in forensics is illustrated in Figure 1. The enhancement or reconstruction is implemented as in sec. 2.3. Face region is segmented and processed by a face recognition technique as in sec. 3.1.



**Figure 1.** Procedure of applying biometrics, such as face recognition, in forensics

A preventive and more automatic application of face recognition is to monitor a region of interest in real time. It's still a challenge for face recognition system to identify an individual of interest from a big crowd, but a face recognition system can identify and track a few subjects, sometimes with gait recognition or other biometrics. Face recognition system can also reside in a sensor network. The information from face recognition and tracking can be used for a higher level processing to interpret what the scene is.

#### 4. DISCUSSIONS

Face recognition is illustrated as a biometrics for forensic usage in previous sec. 3, other biometrics share similar processing procedure. The advantages of biometrics in forensics are: (1) Biometrics is hard to falsify. (2) After the commonly time-consuming training, biometric evaluation of evidence is automatic and fast. (3) The accuracy of biometrics keeps increasing with the intense research in this area. (4) The false acceptance rate and false rejection rate can be adjusted according to the security level.

The limitations of biometrics in forensics are (1) The biometric traits may not be available. What kind of biometrics can be applied can not be foreseen. (2) The construction of biometric systems takes resources and time. It's desirable that such systems can be shared within the nation, or at least the database or core processing can be shared, but this involves privacy, bureaucracy, licensing and law regulation. (3) By nature, the false acceptance and false rejection contradict with each other in biometrics and any other decision system. The development of biometrics keeps lowering the equal-error-rate, but there will never be perfect performance by biometrics alone. Damage control should be considered.

Biometrics is used for security purposes, and the security of such biometric systems themselves should also be taken care of. As an analogy, biometric system is a complex yet very convenient "key" to a secure room or application, but this key has to be protected well. Biometric "keys" will not be lost, but the forged "keys" may spoof the systems. Each person's biometric *features* are unique, and once these *features* are tampered, the loss is permanent. Therefore, the encryption of *features* or cancelable biometrics<sup>41</sup> should be generally considered and definitely implemented in highly secured applications.<sup>42</sup> The security should be ensured while protecting privacy.

#### 5. CONCLUSIONS

This paper provides a comprehensive guide bridging biometrics and forensics with detailed discussion on how they are different, how they are connected, and under what conditions biometrics can be applied in forensics. An example of face recognition is illustrated to show the application of biometrics in forensics, where different face recognition techniques are compared, feature extraction and decision procedure are described, and the specific adaptation of face recognition for forensics is provided. The advantages and limitations of biometrics in forensics are also addressed.

#### REFERENCES

1. DigitalPersona, "A leading provider of biometric authentication solutions for enterprise networks, developers and consumer oems, founded in 1996," <http://www.digitalpersona.com/>.
2. CogniTec, "The face recognition company," <http://www.cognitec-systems.de/>.
3. L1 Identity Solutions, "A company merged from Viisage, Identix, Integrated Biometric Technology, SecuriMetrics and Iridian etc. It provides technology, solutions, products and services that protect and secure personal identities and assets," <http://www.l1id.com>.
4. SensibleVision, "FastAccess login system based on face recognition," <http://www.sensiblevision.com>.
5. R. V. Bruegge, "Biometrics and forensics: Similarities and differences," in *Biometric Consortium Conference BC 2004*, (Hyatt Regency Crystal City, Arlington, VA USA), September 2004.
6. C. Liu and H. Wechsler, "Evolutionary pursuit and its application to face recognition," *Pattern Analysis and Machine Intelligence, IEEE Transactions on* **22**(6), pp. 570-582, 2000.
7. H. Wechsler, *Reliable Face Recognition Methods: System Design, Implementation and Evaluation (International Series on Biometrics)*, Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2006.

8. L. M. Lorigo and V. Govindaraju, "Offline arabic handwriting recognition: a survey," *Pattern Analysis and Machine Intelligence, IEEE Transactions on* **28**(5), pp. 712–724, 2006.
9. S. T. Chaohong Wu and V. Govindaraju, "Robust point-based feature fingerprint segmentation algorithm," in *2nd International Conference on Biometrics*, (Seoul, Korea), 2007.
10. National Science and Technology Council Subcommittee on Biometrics Documentation, "Frequently asked questions," 2007.
11. S. C. Park, M. K. Park, and M. G. Kang, "Super-resolution image reconstruction: a technical overview," *Signal Processing Magazine, IEEE* **20**(3), pp. 21–36, 2003.
12. S. Baker and T. Kanade, "Hallucinating faces," 2000.
13. W. Liu, D. Lin, and X. Tang, "Hallucinating faces: Tensorpatch super-resolution and coupled residue compensation," in *Computer Vision and Pattern Recognition, IEEE Computer Society Conference*, pp. II: 478–484, 2005.
14. Y. Li and X. Lin, "An improved two-step approach to hallucinating faces," in *ICIG 2004: Proceedings of the Third International Conference on Image and Graphics (ICIG04)*, pp. 298–301, IEEE Computer Society, (Washington, DC, USA), 2004.
15. W. Liu, D. Lin, and X. Tang, "Face hallucination through dual associative learning," in *ICIP05*, pp. I: 873–876, 2005.
16. C. Su, Y. Zhuang, L. Huang, and F. Wu, "Steerable pyramid-based face hallucination," *Pattern Recognition* **38**, pp. 813–824, June 2005.
17. K. Jia and S. Gong, "CCTV face hallucination under occlusion with motion blur," in *Imaging for Crime Detection and Prevention, 2005. ICDP 2005. The IEE International Symposium on*, pp. 85 – 88, (Queen Mary Univ. of London, UK), June 2005.
18. X. Wang and X. Tang, "Hallucinating face by eigentransformation," *SMC-C* **35**, pp. 425–434, August 2005.
19. K. Jia and S. Gong, "Hallucinating multiple occluded face images of different resolutions," *Pattern Recogn. Lett.* **27**(15), pp. 1768–1775, 2006.
20. K. Jia and S. Gong, "Face super-resolution using multiple occluded images of different resolutions," in *AVSBS05*, pp. 614–619, 2005.
21. M. Turk and A. Pentland, "Eigenfaces for recognition," *Journal of Cognitive Neuroscience* **3**(1), pp. 71–86, 1991.
22. R. Brunelli and T. Poggio, "Face recognition: Features versus templates," *IEEE Transactions on Pattern Analysis and Machine Intelligence* **15**, pp. 1042–1052, October 1993.
23. B. Heisele, P. Ho, and T. Poggio, "Face recognition with support vector machines: global versus component-based approach," in *Computer Vision, 2001. ICCV 2001. Proceedings. Eighth IEEE International Conference on*, **2**, pp. 688 – 694, July 2001.
24. B. Heisele, P. Ho, J. Wu, and T. Poggio, "Face recognition: component-based versus global approaches," *Comput. Vis. Image Underst.* **91**(1-2), pp. 6–21, 2003.
25. B. S. Manjunath, R. Chellappa, and C. V. D. Malsburg, "A feature based approach to face recognition," in *Proceedings of IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, pp. 373–378, 1992.
26. J. Cook, V. Chandran, S. Sridharan, and C. Fookes, "Gabor filter bank representation for 3d face recognition," in *DICTA '05: Proceedings of the Digital Image Computing on Techniques and Applications*, p. 4, IEEE Computer Society, (Washington, DC, USA), 2005.
27. L. Wiskott, J.-M. Fellous, N. Krüger, and C. von der Malsburg, "Face recognition by elastic bunch graph matching," in *Proc. 7th Intern. Conf. on Computer Analysis of Images and Patterns, CAIP'97*, Kiel, G. Sommer, K. Daniilidis, and J. Pauli, eds., 1296, pp. 456–463, Springer-Verlag, (Heidelberg), 1997.
28. H. Schneiderman, *A Statistical Approach to 3D Object Detection Applied to Faces and Cars*. PhD thesis, Robotics Institute, Carnegie Mellon University, Pittsburgh, PA, May 2000.
29. Y. Sun and L. Yin, "A Genetic Algorithm Based Feature Selection Approach for 3D Face Recognition," in *The Biometric Consortium Conference*, (Hyatt Regency Crystal City, Arlington, Virginia USA), September 2005.

30. A. Pentland, B. Moghaddam, and T. Starner, "View-based and Modular Eigenspaces for Face Recognition," in *Proc. of IEEE Conf. on Computer Vision and Pattern Recognition (CVPR'94)*, (Seattle, WA), June 1994.
31. Y. Yan and L. A. Osadciw, "Fusion for Component based Face Recognition," in *Proceedings of CISS 07*, (Johns-Hopkins University, Baltimore, Maryland, USA), March 2007.
32. Y. Yan and L. A. Osadciw, "Sampling design for face recognition," in *Proceedings of SPIE, Defense and Security 2006: Security, Law Enforcement and Defense*, **6202**, (Orlando, Florida, USA), April 2006.
33. K. Veeramachaneni, L. Osadciw, and P. Varshney, "An adaptive multimodal biometric management algorithm," *Systems, Man and Cybernetics, Part C, IEEE Transactions on* **35**, pp. 344–356, Aug. 2005.
34. D. S. Taubman and M. W. Marcellin, *JPEG 2000: Image Compression Fundamentals, Standards and Practice*, Kluwer Academic Publishers, Norwell, MA, USA, 2001.
35. Y. Rui, T. Huang, and S. Chang, "Image retrieval: current techniques, promising directions and open issues," *Journal of Visual Communication and Image Representation* **10**, pp. 39–62, apr 1999.
36. J. Ruiz del Solar and P. Navarrete, "Faceret: An interactive face retrieval system based on self-organizing maps," in *The Challenge of Image and Video Retrieval, International Conference on Image and Video Retrieval*, pp. 157–164, 2002.
37. E. L. van den Broek, P. M. F. Kisters, and L. G. Vuurpijl, "Design guidelines for a content-based image retrieval color-selection interface," in *Proceedings of the conference on Dutch directions in HCI*, p. 14, ACM Press, (New York, NY, USA), 2004.
38. Ritendra, "Image retrieval: Ideas, influences, and trends of the new age," *ACM Transactions on Computing Surveys, preprint*, 2008.
39. O. Arandjelovic and A. Zisserman, "Automatic face recognition for film character retrieval in feature-length films," in *Proceedings of the 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05) - Volume 1*, pp. 860–867, IEEE Computer Society, (Washington, DC, USA), 2005.
40. T. L. Berg, A. C. Berg, J. Edwards, M. Maire, R. White, Y.-W. Teh, E. Learned-Miller, and D. A. Forsyth, "Names and faces in the news," *Computer Vision and Pattern Recognition, IEEE Computer Society Conference on* **02**, pp. 848–854, 2004.
41. N. Ratha, J. Connell, R. M. Bolle, and S. Chikkerur, "Cancelable biometrics: A case study in fingerprints," in *ICPR '06: Proceedings of the 18th International Conference on Pattern Recognition*, pp. 370–373, IEEE Computer Society, (Washington, DC, USA), 2006.
42. A. Adler, "Sample images can be independently restored from face recognition templates," in *Electrical and Computer Engineering, 2003. IEEE CCECE 2003. Canadian Conference on*, **2**, pp. 1163 – 1166, May 2003.