ISSN No. 0976-5697

Volume 5, No. 7, September-October 2014

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Soft Biometrics Techniques – A Technical Review

Suhail Tomar
Computer Science and Engineering Department, SRM University, Kattankulathur, Kancheepuram Dist., Tamilnadu, India.

K. Senthil Kumar
Asst. Professor, Computer Science and Engineering Department, SRM University, Kattankulathur, Kancheepuram Dist., Tamilnadu, India.

D. Malathi
Professor, Computer Science and Engineering Department, SRM University, Kattankulathur, Kancheepuram Dist., Tamilnadu, India.

Abstract: Soft biometrics are a new form of biometric identification which use physical or behavioral traits that can be naturally described by humans. Soft biometric is not like other biometric approaches as it allows identification based totally upon verbal descriptions, and this bridges the semantic gap between biometrics and human description. The term semantic gap here means, the gap which exists between how machines and people recognize humans. Soft biometrics bridge this gap, allowing conversion between human descriptions and biometrics. Now a days the soft biometrics are used in surveillance purposes by allowing identification based on human descriptions. Soft biometrics traits include characteristics like height, weight, hair length, hair colour, marks, tattoos, gender etc. These traits can be described using human understandable labels and these labels can be used in human identification. One of the major advantage of soft biometrics is that it can be obtained at a distance without subject cooperation and knowledge even from the low quality video footage. In this paper, we have compared techniques used to implement the soft biometrics and also advantages of soft biometrics over hard biometrics. This paper briefly explains the techniques which can be useful in implementing the soft biometrics in real world scenario.

Keywords: Soft biometrics, distinctiveness, permanence, traits, semantic gap, surveillance, identification.

I. INTRODUCTION

Biometrics is a science of automatically recognizing of peoples on the basis of physical or behavioral characteristics. A large variety of biometric systems have been developed for automatic recognition of individuals based on their physiological or behavioural characteristics. These systems make use of a single or a combination of traits like face, gait, iris, etc., for recognizing a person.Although these traits have been successfully incorporated in operational systems, but still there are several challenges that are yet to be addressed. For example, we can’t utilize these traits as because the input data is of low quality or when the distance between the sensor and subject increases. Thus, the use of alternate human attributes may be necessary to establish an individual’s identity.

Previously the methods for identification mostly uses hard biometric traits, specifically fingerprint and face to identify a particular person. However, the use of these biometric traits is not only inconvenient to the subject, but is also not always feasible due to the subject’s posture in front of the sensor. To overcome this problem, a new framework for human identification i.e. soft biometrics comes in picture. In soft biometrics, the identification can be done from the distance without users consent also.

Identification to be performed at a distance has received significant interest due to the ever increasing surveillance infrastructure. Biometrics traits like facial marks, tattoos and gait offer a suitable physical attribute to uniquely identify people from a distance. When these measurements are linked with the human descriptions, these biometrics suffer from the semantic gap which is the difference between how people and how biometrics represent and describe humans.

Soft biometrics bridges this gap, allowing conversions between gait biometrics and verbal descriptions. Soft biometrics is having applications in identifying a subject from surveillance footage by the help of descriptions given by the eyewitness. When the terrorist and criminal activities will increase, identifying peoples accurately becomes a critical task. By allowing identification of humans at a distance from the surveillance footage would detect known criminals. Popular biometrics is capable of identifying humans from a distance, for example face and gait recognition, but both of these suffer from the semantic gap. It is common in eyewitness reports that a physical description of a criminal is available, this description cannot be translated to a machine understandable biometric. So in such cases soft biometrics are needed as it bridges this gap, allowing conversions between human descriptions and biometrics. One possible application for such a technique is to automatically search surveillance footage for people who best match a given human description.

The organization of the paper is as follows. The major techniques which are used to practically implement the soft biometrics are explained in sections A, B and C. Section II deals with drawbacks and comparisons of three soft biometric techniques. Conclusion and future work are given in Section III.

A. *Facial Mark Based Matching:*

Soft biometric traits enclosed in a face (e.g., gender and facial marks like moles, scars etc) are ancillary information and are not fully distinctive by themselves in face-recognition tasks but when this information is combined with face matching score then the overall face-recognition will improve. The soft biometrics traits can be used in four different ways i.e.

a. Supplement existing facial matchers to improve the identification accuracy
b. Enable fast face image retrieval
c. Enable matching or retrieval with partial or off frontal face images
d. Provide more descriptive evidence about the similarity or dissimilarity between face images, which can be used in court.

Utilization of demographic information and facial marks for improving face image matching and retrieval performance is proposed in this research work. Gender and ethnicity are considered in demographic information whereas scars, moles and freckles are considered in facial marks. In this research work the demographic information and facial marks together considered as soft biometric traits. The characteristics like moles, scars and freckles embedded in face images are captured by facial marks, which are not utilized in the conventional face recognition systems. Face matcher and mark based matcher are combined together to provide improved recognition accuracy. An Automatic facial mark detection system has been proposed and it uses

a. The active appearance model for locating primary facial features (e.g., eyes, nose, and mouth),
b. The Laplacian-of-Gaussian blob detection, and
c. Morphological operators

Now, we move towards the experimental results provided on the basis of FERET database in which 426 images of 213 subjects are stored. Two mugshot databases from the forensic domain having 1225 images of 671 subjects and 10000 images of 10000 subjects, respectively are also considered. These databases shows that the use of soft biometrics is able to improve the face recognition rate of state-of-the-art commercial face matcher, faceVACS[12].
Previously in conventional face matching systems, only the numeric matching scores are generated on the basis of similarities between two face images. In the facial mark based matching, the accuracy rate is improved as it provides specific and more meaningful evidence about the similarities of two images. This is the reason behind the importance of facial marks in the forensic applications as by the help of these facial marks we can get more specific information which will improves the recognition rate. When face matcher is properly combined with soft biometric traits, then it is expected to improve the face recognition rate. If the facial images are of low resolution or partially damaged, then the soft biometric traits can be considered for identification. The demographic information do not change over the lifetime, so this information (gender and ethnicity) can be used to narrow down the amount of candidate face images present in the database. When the images are taken from surveillance videos then in some cases face images are not included or at low resolution, then at that time soft biometrics traits can be considered and used for face matching or retrieval. Hence by the help of soft biometric traits like gender and ethnicity, we can perform identification from the surveillance video footage. Some of the examples of facial marks are shown in Fig. 1.
Hence, the facial marks and the demographic information also become useful in the case of soft biometrics.

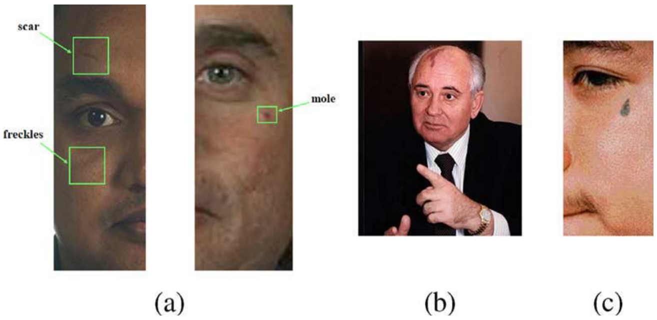

Figure. 1. Examples of facial marks

a) Scar, mole, and freckles (FERET database)
b) Large birthmark (http://www.wnd.com/index.php?fa=PAGE.view&pageId=63558)
c) Tattoo(http://blog.case.edu/colin.mulholland/2007/09/20/a_way_of_expression)

B. *Comparative Descriptions Based Matching:*

The major advantages of soft biometric are that it can be obtained at a distance even from the low quality video footage and soft biometrics is having relationship with human description: humans naturally use soft biometric traits to identify and describe each other. Hence it allows identification and retrieval based solely on a human description of the subject, provided by an eyewitness. Other biometrics like face and gait are the biometrics used in surveillance but they are having drawback that they suffers from low frame rate or resolution. Soft biometric traits can be obtained from the data derived from low quality sensors, including surveillance cameras. It doesn’t requires cooperation from the subject and are non-invasive—making them ideal in surveillance applications. We can better understand this by an example.

Fig. 2 shows an example of a typical CCTV video frame showing looters at the 2011 London riots. We can see that even the picture is at low resolution but still a detailed human description of the subjects can be given and this is the usefulness of implementing soft biometrics. On the other hand, automatic facial recognition would struggle with the low resolution and non-frontal viewpoint.

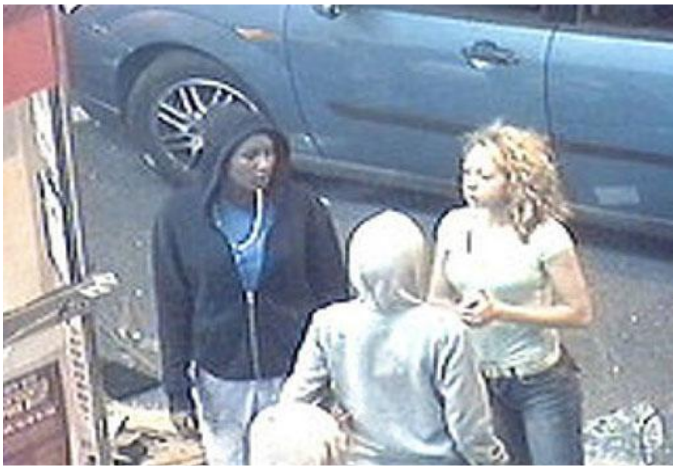

Figure. 2. Surveillance frame displaying common surveillance problems

When performing identification, the human descriptions are required as without that we can’t perform the task. Now the eyewitness will describe the physical properties of the subject but they can be considered as inaccurate and unreliable [4], [5] as they consists of either absolute categorical labels (e.g., 'tall') or estimates of human characteristics (e.g., 190 cm). To overcome the problem of predicting inaccurate measurements [6], labels are used and they are considered as a more robust method of obtaining accurate and reliable human descriptions [7]. One major problem associated with the absolute categorical labels is their highly subjective nature. A label's meaning is based on the person's own attributes and their own perception of population averages and variation. This can vary, making absolute labels less reliable.

The drawbacks of absolute categorical labels are removed by the help of Comparative human descriptions. Comparison will be made between the appearance of two subjects and it is a very natural process and may be more reliable than the use of absolute labels because comparisons are assigned based on a specified benchmark resulting in a more objective description.

In this research work a set of relative measurements describing the subject can be accurately obtained from comparative labels (that are derived from comparing one person with another, e.g., 'taller') and used as a biometric signature.

Relative measurements of the subjects' traits can be inferred from comparative human descriptions using the Elo Rating System. Elo rating system is based on Thurstone's Case V model [8]. Elo ratings were designed to quantify the skill of chess players. The performance of a chess player cannot be measured absolutely. Instead the player's (relative) skill level is inferred from matches against other players [9]. To get the relative measurements, the subjects are compared within the population for a particular trait. This can be done by the Elo Rating System. We are using this method of comparing subjects to overcome the problem of inaccuracy in absolute categorical labels. The relative measurements were normalized to a range of 0-1 and used to train the Support Vector Machine (SVM). Support Vector Machine is a method used for classification of both linear and nonlinear data. It uses a nonlinear mapping to transform the original training data into higher dimension. In the new dimension, it searches for the linear optimal separating hyperplane i.e. a decision boundary separating the tuples of one class from another. SVM is based on ranking algorithms used within search engines [10]. The ranking function could then be used to determine the ordering between all of the images. In other words we can say that SVM classifier can be used to compare the data which is present in the training phase to the data in the testing phase. Hence, in this way the comparative descriptions are become helpful in identification of a human on the basis of categorical labels.

C. Ranking Based Matching:

In Soft biometrics, identification is performed from a distance and this is useful as due to increase in use of surveillance infrastructures, deployed in society. Gait and face are also capable of identifying person from a distance but they suffer from low frame rate and low image resolution of most CCTV cameras. The advantages of using soft biometrics is that it uses the images of low resolution for extracting biometric signatures and it also require less cooperation from the subject as the signature can be obtained without their consent, which makes it appropriate for surveillance applications. Once the unknown subject's biometric signature has been found, then the biometric system performs identification on the basis of labeled set of biometrics signature stored in the database. Here the term label means that the identity of the subjects in the database.

The identification is performed by checking (calculating) the similarities between the input signature generated from a unknown subject's and the signature which is already stored in the database. We call the input biometric signature as **probe** and the database as **gallery** [2]. Now the concept of ranking comes in picture as each identity stored in the database will be ranked based on the similarities and it produces an ordered list of identities. The probability of correct identity is more for rank 1 and decreases as we go down in the ordered list.

All the above mentioned things are for identification, if we want verification of an individual identity then in such case, the input biometric signature is labeled with an identity. Now the comparison is performed between the input biometric signature and the signature stored in the database having the same identity label. If the similarity measure is above the threshold (It is chosen to define the similarity required for a "match.") then it is a **"match"** or an **"accept"** is said to have occurred, otherwise it is a **"non match"** or a **"reject"** [11]. When the task of verification will be performed, then two kinds of errors can arise. When the input signature is incorrectly matched against a different identity in the database then a false accept (FA) said to be occurred. A false reject occurs when the input signature is incorrectly "rejected" even matched with the correct identity in the database. These kinds of errors arise when the biometric signatures of two subjects are very similar or the biometric signature of a single subject varies with time.

The threshold determines the number of FA and FR errors. The chosen threshold must minimize the FA and FR errors by separating the intra-class distributions as optimally as possible so that the best performance can be achieved [2].

The intra-class term here represents the variation between multiple observations of an individual. When it is low for a biometric trait, then the trait is said to demonstrate permanence and repeatability and when it is high, then that biometric trait can be successfully used to distinguish between peoples [11].

Hence, by using ranking also we can implement soft biometrics in the real world scenario.

II. DRAWBACKS

Comparison of Facial Mark, Comparative Descriptions and Ranking Based Techniques are given in Table 1. The facial mark based matching is having drawback like mark detection accuracy is less as when the user-specific mask does not effectively remove sources of false positives, true marks with lower contrast will be missed in the mark detection process. So, the future work for this is to improve the accuracy of mark detection.

In the comparative description based matching the image retrieval efficiency is less and the system is not performing the identification automatically from a video footage. So, certain measures are to be taken to make the image retrieval more efficient and to make the whole system automated

At last the ranking based matching is also having drawbacks like the system is not automated as it requires the human description to identify a person. Without describing by a human we can't identify a person.

III. CONCLUSION AND FUTURE WORK

This paper provided a short survey on techniques used to implement the soft biometrics and it also provide advantages of soft biometrics over hard biometrics. This paper briefly explains the techniques which can be useful in implementing the soft biometrics in real world scenario. Soft biometric traits can be typically described using human understandable labels and measurements, allowing for retrieval and recognition solely based on verbal descriptions. Soft biometrics bridges the semantic gap by allowing conversion between human description and biometrics.

Table 1. Comparison of Facial Mark, Comparative Descriptions and Ranking Based Techniques

No.	Facial Mark Based	Comparative Descriptions Based	Ranking Based
1.	Demographic Information (Gender & Ethnicity) with facial marks (scars, marks & freckles) is used to identify a person.	Comparative Categorical Labels are used to identify a person. (16 comparative and 3 absolute labels)	Categorical Labels are used as identity of the subject in the database. Each identity in the database will be ranked based on this similarity measure.
2.	Automatic Facial mark detection method is used to improve the recognition accuracy[3].	Elo Rating System is used to give Relative Measurement as a output which will be treated as signature. SVM classifier is used for classification.	Ranks are given to the identity on the basis of similarity measures and thresholds are used to determine the FA & FR.
3.	Can be used to identify identical twins.	Cannot be used to identify identical twins.	Cannot be used to identify identical twins.
4.	Procedure is automatic, does not require human's description.	Not automatic, as it requires human's description.	Not automatic, as it requires human's description.
5.	Matching score is generated and can be combined with any face matcher to improve the overall face-recognition accuracy.	Relative Measurement is used as the signature and can be used to identify a person by comparing data in the training set to testing set.	The input signature i.e. the feature set extracted from the biometric data is only compared against those biometric signatures in the database having the same identity label.

Soft biometrics requires less computation as compared to 'hard' biometrics, no cooperation from the subject and is non-invasive making them ideal in surveillance applications and hence these are the reasons which are making it more efficient as compared to hard biometrics. The techniques used in this paper are facial mark based, comparative description based and ranking based.

In the facial mark based technique, identification is performed by the help of demographic information with facial marks. This technique is fully automatic as it will perform the task of identification automatically without any human description. The accuracy of state-of-the-art commercial face matcher, faceVACS is improved due to two reasons, first one is the use of demographic information i.e. gender and ethnicity and second is by combining it with mark based matcher. After combining the face matcher with mark based matcher, the accuracy is again improved due to incorporating additional soft biometric traits. Improving accuracy of faceVACS is not an easy task as it is the best face matcher available in the market. Face recognition accuracy using FaceVACS matcher, proposed facial mark matcher and their fusion is 91.08%, 91.55%, 91.55% and 92.02% for no demographic, gender, ethnicity and both (gender and ethnicity) respectively[3].

Future work for the facial mark based matching is:

a. Improving the mark detection accuracy,

b. Extending the automatic mark detection to off frontal face images and

c. Studying the image resolution requirement for reliable mark extraction.

The second technique which is used is the comparative description based matching in which some sort of comparative labels (that are derived from comparing one person with another, e.g., 'taller') are used as a biometric signature. The biometric signature is called as relative measurement as it can be inferred from comparative human descriptions using the Elo Rating system. In this, the relative measurements were also obtained automatically from video footage using a support vector machine, allowing video data to be searched automatically using a human description. Comparisons between subjects from the Soton gait database were collected. Each eyewitness was asked to compare a single target to multiple subjects. It was found that comparative descriptions differed on 17 percent of occasions when compared against absolute categorical descriptions. The relative measurements were shown to strongly represent actual trait measurements; results comparing actual height to the inferred relative height showed a correlation of 0.87. Recognition of subjects from a soft biometric database demonstrated the discriminative power of relative measurements, achieving a recognition accuracy of 92 percent with ten comparisons. This increased to 95 percent with 20 comparisons [1]. Future research will attempt to improve the retrieval results allowing automatic identification from video footage.

The technique which is explained at last is the ranking based matching in which if an unknown person's biometric signature has been determined, the system must then identify the subject based on a database containing a labeled set of biometric signatures. This is done by calculating the similarity between the probe and the signatures within the gallery. Each identity in the database has given a rank on the basis of similarity measures. Here in this a concept of threshold is used as if the similarity measure is greater than the threshold, then a **"accept"** is said to have occurred else, it is said to be a **"reject".**

The two kinds of errors can be arises in the verification of a identity named as false accept (FA) and false reject (FR). These errors can be minimized by the help of thresholds.

IV. REFERENCES

[1] Daniel A. Reid, Mark S. Nixon, and Sarah V. Stevenage, “Soft Biometrics; Human Identification Using Comparative Descriptions”, IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 36, no. 6, June 2014

[2] D.A. Reid, S. Samangooei, C. Chen, M.S. Nixon, and A. Ross, “Soft Biometrics for Surveillance: An Overview,” Handbook of Statistics, vol. 31, chapter 13, pp. 327-351, 2013.

[3] Unsang Park and Anil K. Jain, “Face Matching and Retrieval Using Soft Biometrics”, IEEE TRANS. Information Forensics and Security, vol. 5, no. 3, Sept. 2010.

[4] E.F. Loftus, Eyewitness Testimony. Harvard Univ. Press, 1996.

[5] C.A. Meissner, S.L. Sporer, and J.W. Schooler, “Person Descriptions as Eyewitness Evidence,” Handbook of Eyewitness Psychology, vol. 2, pp. 3-34, 2007.

[6] J.C. Yuille and J.L. Cutshall, “A Case Study of Eyewitness Memory of a Crime,” J. Applied Psychology, vol. 71, no. 2, pp. 291-301, 1986.

[7] S. Samangooei and M.S. Nixon, “Performing Content-Based Retrieval of Humans Using Gait Biometrics,” Multimedia Tools and Applications, vol. 49, no. 1, 2010.

[8] L.L. Thurstone, “A Law of Comparative Judgment,” Psychological Rev., vol. 34, no. 4, pp. 273-286, 1927.

[9] A.E. Elo, The Rating of Chessplayers, Past and Present. Batsford, 1978.

[10] T. Joachims, “Optimizing Search Engines Using Clickthrough Data,” Proc. Eighth ACM SIGKDD Int’l Conf. Knowledge Discovery and Data Mining (SIGKDD ’02), pp. 133-142, 2002.

[11] D.A. Reid, S. Samangooei, C. Chen, M.S. Nixon, and A. Ross, “Soft Biometrics for Surveillance: An Overview,” Handbook of Statistics, vol. 31, chapter 13, pp. 327-351, 2013.

[12] FaceVACS Software Developer Kit Cognitec systems GmbH [Online].

Available: http://www.cognitec-systems.de