Biostatistics and Biometrics
Open Access Journal
ISSN: 2573-2633

Juniper Publishers
key to the Researchers

Mini Review
Volume 1 Issue 4 - May 2017
DOI: 10.19080/BBOAJ.2017.01.555572

Biostat Biometrics Open Acc J

Precise Multimodal Biometric Fusion Method Using Copula and QR Codes

Saif Al Zahir*

Department of Electrical and Computer Engineering, University of Victoria, Canada

Submission: March 17, 2017; **Published:** May 09, 2017

***Corresponding author:** Saif Al Zahir, Department of Electrical and Computer Engineering, University of Victoria, Canada, Email: saifalzahir@gmail.com

Abstract

Biometrics authentication is the process of identifying an individual using some of his/her physiological and/or behavioural traits. These traits include but not limited to their voice, facial features, fingerprints, irises, signatures, DNA, just to name a few. While single modality biometric methods have to deal with noisy sensor data, specificity of the biometric trait and intolerable error rates, the multimodal biometric systems suffer from storage requirements, processing time, convoluted security issues, and the computational complexity. In this paper, we present a new method that provides a solution to error rate problem and security issues. The proposed method uses Quick Response codes, QR codes, to embed the fused biometrics data and wrap it with a secure encryption technique such as DES or AES. To validate and authenticate the biometrics we use the Gaussian copula, which is near perfect method for measuring data sequences similarity. Our experimentation results show that the proposed method provide near perfect verification due to the error correction capability of the QR codes. When implemented it on images (two sequences: original and distorted), our results scored perfect recall rate on a sample of 260 cases from the CoMoFoD database.

Keywords: Biometrics authentication; Multimodal; data quality; score-level fusion; Gaussian copula; QR codes

Introduction

The term “biometrics” is originated from the Greek word “bio” which means life and the word “metric” which means to measure. Biometrics encompasses a wide range of physiological and behavioral measurements [1]. It includes, but not limited to, DNA matching, face recognition, iris recognition, fingerprints, voice verification, hand geometry identification, hand written material, signatures and behavioral biometrics such as individuals walking styles or odor [1,2]. The fundamental premise of biometric authentication or verification is that every person is unique and can be identified by his or her intrinsic and inherent physical and behavioral traits.

Biometric methods can be classified into two classes: (i) single modality; and (ii) multimodal [2,3]. Fusing data streams of several single biometrics is a challenging and promising approach to improve the overall recall rate efficiency of the system. Systems that use biometric fusion are called multimodal biometric systems. In addition, it should be noted that fusion consists not only of multiple measures, but also it may include intra-modal fusion, i.e., fusing data of the same biometric modality but not the set of features used to extract the identity of the subject, or can simply be using the same features set but employing different classifiers and thresholds. Fusion methods include simple-sum, min-score, max-score, which are well-established methods, as well as matcher weighting, and user weighting that are somewhat new and less popular.

Biometrics for the most part is permanent and naturally cannot be easily changed. This distinguishes it from a standard password. This type of biometrics authentication cannot be lost, damaged, or easily shared with others, as can password or other verification systems because people maintain their physiological or behavioral characteristics for a long time unless they perform surgical operations to change them. In addition, employing biometric authentication has no labor expenses associated with password resets thereby decreasing the system management operation costs [3]. Although there are many published articles in the literature on biometrics, there are still no coordinated efforts in reaching a benchmark database for such important topic of research.

Fusion in Biometrics

There exist many levels where fusion can be used to merging biometric traits. The main three possible levels of fusion are: (i) fusion at the sensor level. In this case, the consolidation of evidence is captured at the input of the multiple sensors (i.e.,

sources), prior to feature extraction; (ii) fusion at the feature extraction level. In this type, data is obtained from each sensor (source) and the data is used to compute the feature(s) of the sequence (vector). If the features are

independent, then it is preferable to concatenate these sequences in one sequence; (iii) fusion at the matching scores level. In this approach, each subsystem provides a matching score indicating the proximity of the feature sequence (vector) with the original data or what is called the template vector. These scores may be combined to form a super matching score [1-3]. There are other fusions types in the literature that can be performed at different levels of the fusion system.

The proposed method is of the second type where we perform the fusion at the level of feature extraction. This method is insensitive to the method of fusion, the length of the fused data as long as it can fit into the QR code. Finally, it is worthwhile emphasizing that in our method that once we upload the fused biometric sequence or scores into our container (i.e., the QR code), this sequence will be secure and can be recovered even if the data is subjected to partial damage or distortion as shown in Figure 1.

Figure 1: An example of a distorted QR code that can be recovered.

The Proposed Method

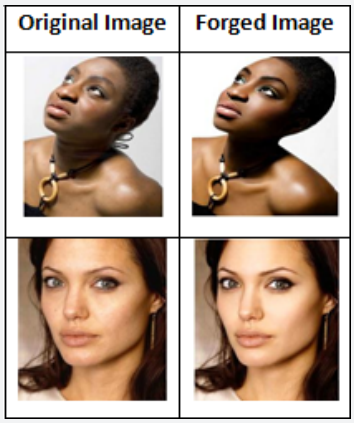

Figure 2: An example of image retouching forgery.

Biometric authentication is becoming ade facto alternative to traditional authentication methods such as password or PIN numbers because it is essentially the user's traits rather than adopted information. As such, biometrics is not susceptible to misplacement or loss. Examples of biometric modalities are fingerprint, face, voice, and hand geometry. Figure 2 shows a simplified scheme of our method. The main components of the proposed method are: (i) sensors (input sources); (ii) sequential fuser; (iii) QR codes embedding; and (iv) the Gaussian copula algorithm used for testing and verification and authentication at the database level. In the following sections, weexpla in the two major components of the system, namely the Gaussian Copula and QR codes as the other two components are well established in the literature.

Gaussian Copula

Copula functions are important tools for modeling dependence of random variables. Copula is derived from the Latin word 'Copulare', which means join, connect, or tie. It is widely known as a family of distribution functions. The main idea behind copula theory is that the cumulative distribution function (CDF) of a random vector can be represented in the form of uniform marginal cumulative distribution functions, and a copula that connects these marginal cumulative distribution functions. Sklar's theorem [4] defined the idea of Copula as follows:

For any two random variables X and Y, their joint probability distribution F(x, y), is given by:

$$F(x,y) = C((F(x), F(y)) = C(u,v) \quad (1)$$

where C(u,v) is the copula function, u=Fx(x), v=Fy(y) are marginal probability distributions, F(x,y) is the joint distribution [5]. The copula density function, c(u,v), is given by:

$$c(u,v) = \partial C(u,v) / \partial u \partial v \quad (2)$$

In this work we estimate the data (independent variable) quality of the distorted data by computing the copula based mutual information between the reference (i.e., original sequence) and distorted blocks of the biometrics. Using copula functions has a main advantage which is, they can join pares of data distributions regardless of their shape or size [4]. Copulas functions are used in various applications such as economics and finance, climate, oceanography, hydrology, geodesy, evolutionary computation [6], and Image processing applications such as image change detection, image quality and image registration [7]. Although all copula functions produced similar results, we will limit ourselves to the use of the Gaussian copula in this research. Other copula functions are the Marshall-Olkin, Clayton, Frank, and Gumbel, just to name a few.

Gaussian Copula mutual information we used is given by:

$$MI_{Gaussian} = ½ \ln(1 - \rho 2) \quad (3)$$

where $MI_{Gaussian}$ is the mutual information, and ρ is the Pearson correlation between the reference and distorted images.

How to cite this article: Saif Al Z. Precise Multimodal Biometric Fusion Method Using Copula and QR Codes. Biostat Biometrics Open Acc J. 2017;1(4): 555568. DOI: 10.19080/BBOAJ.2017.01.555572.

Two random variables X and Y are said to be independent if, and only if, their joint probability density function (PDF) equals the product of their marginal PDFs. Therefore on the other hand, if $F(x,y) \neq f_x(x) f_y(y)$, where $f_x(x)$ and $f_y(y)$ are marginal densities and F(x,y) is the joint probability density function means that X and Y are dependent. Estimating mutual information is convenient way to quantify statistical dependencies. Mutual information can be calculated as follows [7]:

$$I(X,Y) = S[f_x] - S[f_{x|y}] \quad I(X,Y) = S[f_x] - S[f_{x|y}]$$

whereI(X,Y)is the mutual information between the two random variables X and Y. The value of equals zero only in case of independent variables. By defining the entropy of the distribution of X as follows:

S [fx] = $\int f_x(x) \log \log f_x(x)\, dx$ and the average conditional entropy $S[f_{x|y}] = \int f_y(y)\, dy \int dx f_{x|y}(x) \log f_{x|y}(x)$

where $f_{x|y}(x)$ represents the conditional probability of the variable X given variable Y, $I(X,Y) = S[f_x] - S[f_{x|y}]$ the identity describes the mutual information as the average reduction in the uncertainty in X given knowledge of variable Y [7] .

In a separate research [7] we showed that copulas are considered one of the best and least complex method to perform similarity and/or dissimilarity between two independent variable, two image for instance. Figure 3 shows an example of two images that have been tampered with (i.e., forged) using a retouching forgery method. This type of forgery changes the luminance values of the pixels only and does not alter any other feather of the image. This is a hard type of forgery to detect. Fortunately, our Gaussian copula algorithm can easily detect this type.

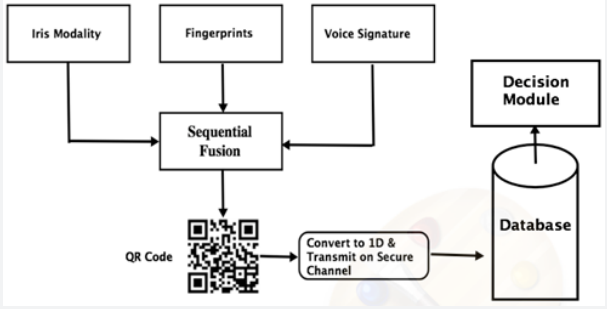

Figure 3: A simplified schematic of multimodal fusing biometric.

Quick response, QR codes

The QR-code component comes immediately after the fusion module in the proposed method. QR codes are two-dimensional (2D) codes that consist of a grid of square cells allowing more information to be encoded in a smaller amount of space. These are also referred to as "stacked" or "matrix" codes. This matrix is readable by QR scanners, mobile phones with a camera, and smart phones.

There are different versions of QR codes. Currently they are 40 versions of QR codes that have different capacities and features. These versions are determined by a numeral in a chart, followed by an error correction level. By following the two, the version number is reached. QR Codes Version-40 can store up to 4,296 alphanumeric characters of arbitrary text [8]. They are also capable of storing contact information, graphical raw data, a signature, or an image. Hence, QR codes are perfect to store biometric sequences. Decoding the information can be done with any mobile camera phone that has a QR reader application. Such software is free and can be downloaded from the Internet.

QR codes support four levels of error correction to enable recovery of missing, misread, or obscured data. Greater redundancy is achieved at the cost of being able to store less data. Table 1 Shows the four levels and their error recovery capability. As biometric-oriented security systems have room for improvement, particularly in their accuracy, tolerance to various noisy environments. Biometric data is customary noisy at the different levels in the systems loop, which makes QR codes a perfect container for them.

Discussion and Analysis

Experimental results concerning identity verification are based on the accuracy of a recognition method and are generally measured in terms of two potential types of errors and the recall rate. The types of errors are: false negatives and false positives. False positives being the cases where a claimed identity is accepted, but should not be, while false negatives being the case where a claimed identity is not accepted, while it should be.

Almost all methods use thresholding techniques on the similarity score for determining whether two faces are similar or significantly dissimilar. The higher the threshold, the higher the precision is. However, a high threshold also decreases the recall rate of the system as it increases the number of false negatives. To our knowledge, no article in the literature has reported a perfect recall results. In our cases, our two components, the copula algorithm produced perfect results on similarity and our second component i.e., the QR code can correct errors up to 30% which guarantees a near perfect recovery of the fused sequence.

Conclusion

In this paper, we presented a new method to improve the recall rate efficiency and security of a fused biometrics. The proposed method uses QR code to host the fused data sequence. As QR code has the capability of error correction in the range of 7% up to 30% at the H level, the recall rate almost perfect on our sample of 260 cases from the CoMoFoD database. Such error

How to cite this article: Saif Al Z. Precise Multimodal Biometric Fusion Method Using Copula and QR Codes. Biostat Biometrics Open Acc J. 2017;1(4): 555572. DOI: 10.19080/BBOAJ.2017.01.555572.

correction capability ensures an improved recovery rate even if the sequences were damaged or partially distorted. In addition, the added security level of encryption provided addition layer of security and make the method a formidable and robust system. It is technically feasible to add this layer on top of the QR code to ensure that access to the biometrics data is restricted which is imperative for some applications such a security and medical data. The proposed method has a low computational requirement compared to other systems as both the copula function and QR codes are a low complexity functions.

References

1. Rodrigues Ricardo N, Lee Luan Ling, Venu Govindaraju (2009) Robustness of multimodal biometric fusion methods against spoof attacks. Journal of Visual Languages & Computing 20(3): 169-179.
2. Karthik N, Yi Chen, Anil K Jain (2006) Quality-based score level fusion in multibiometric systems. 18th IEEE International Conference on Pattern Recognition 4.
3. Norman P, Bengio S (2006) Database, protocols and tools for evaluating score-level fusion algorithms in biometric authentication. Pattern Recognition 39(2): 223-233.
4. Sklar A (1959) Distribution Functions of n Dimensions and Margins. Publications of the Institute of Statistics of the University of Paris 8: 229-231.
5. Wajid R, Mansoor AB, Pedersen M (2013) A study of human perception similarity for image quality assessment, Colour and Visual Computing Symposium (CVCS), IEEE, Gjøvik, Norway.
6. Salinas-Gutiérrez R, Hernández-Aguirre A, Villa-Diharce ER (2011) Dependence trees with copula selection for continuous estimation of distribution algorithms. Proceedings of the 13th annual conference on Genetic and Evolutionary Computation, GECCO.
7. AlZahir S, Hammad R (2015) New gage for measuring image quality. 28th IEEE Canadian Conference on Electrical and Computer Engineering, CCECE, Halifax, Canada.
8. http://www.qrcode.com/en/index.html

How to cite this article: Saif Al Z. Precise Multimodal Biometric Fusion Method Using Copula and QR Codes. Biostat Biometrics Open Acc J. 2017;1(4): 555568. DOI: 10.19080/BBOAJ.2017.01.555572.