Hybrid Face Recognition Algorithm for Wireless Sensor Network

Matheel E. Abdulmunem and Fatima B. Ibrahim

Hybrid Face Recognition Algorithm for Wireless Sensor Network

Matheel E. Abdulmunem¹ and Fatima B. Ibrahim²

¹Computer Science Department -University of Technology –Baghdad- Iraq.
²Information and Communication Engineering Dep. - Al-Khwarizmi College of Engineering
Baghdad University -Baghdad Iraq
¹matheel_74@yahoo.com
²fatima_0987@yahoo.com

Received: 6 November 2016 Accepted: 12 February 2017

Abstract

Since computing technology increasing as part of our daily life activity, there is a need for new branches of applications. Developing the Wireless Sensor Network (WSN) application to adequate to work within the access control of smart home is the main aim of this paper. In this paper, a new approach of face recognition is proposed to work with WSN depending on Gabor filter and the computation of Eigen faces. Centralized algorithm principle is depended on work to carry the work load to the base station node with a flat architecture based on the principle of gossiping routing protocol. The feature vector that is traveling on the network is compressed to only 15 components with recognition rate reaches to 100% and reduction in computation complexity of Eigen faces.

Keywords: Wireless Sensor Network, Eigen faces, Gabor filter, DC components.
Hybrid Face Recognition Algorithm for Wireless Sensor Network

Matheel E. Abdulmunem and Fatima B. Ibrahim

Introduction

Wireless sensors can be placed in homes by exploiting the home network to automatically and smartly manage houses. Smart refrigerator, cook, wash and others more helping applications such as security, access control, monitoring, etc. may be used and combined in smart home. Home algorithms can be adopted in wider building and can facilitate our life in sides of remotely meeting, looking children up and others [1, 2]. Mainly, the WSN/Wireless Multimedia Sensor Network (WMSN) stack contains four layers that they are: Physical, Link, Network, and Application. IEEE 802.15.4 standard IEEE-TG15.4 are the standards for the lower layers of physical layer and link layer while no standard exists for the upper layers but they round about some regular features. The responsibility of physical layer is to provide access techniques. Medium access control is the working of link layer. Definitely the network layer has the responsibility of routing the date over the network. In the application layer
different styles of applications can be adopted to be used [3]. The common of WSNs demonstration the (source, sink) architecture, in which it may contain any number of:

1. Source nodes, which sensed and generated data, generally by using sensors to measure and sensed factors and phenomenon of the surrounding environment such as humidity, temperature or radiation.

2. Sink nodes, that collect the whole gathered data by source nodes and process them.

3. Intermediate nodes (containing the source nodes) that support the communication of data from sources to sinks [4, 5].

The data generated at the source nodes is either in a proactively manner or in a response to such a request. For the sink nodes that are frequently mentioned as a base station, there is a suggestion that they may have highly powered and they are linked to databases through satellite links or they can have extra resources than other nodes [5].

Energy is an important aspect of WSN. Receiving and sending a message are a cost operation for energy which take the most energy of node. Most protocols take the following arithmetic model to compute the power consumed [6]:

\[ E_nT(K) = E_{elec} * K + E_{amp} * K \cdot d^2 \]  \hspace{1cm} (1)

\[ E_nR(K) = E_{elec} * K \]  \hspace{1cm} (2)

Where

\( E_{elec} \) is the transmitter electronic that the energy waste for receiving and transmitting per bit.

\( E_{amp} \) is the transmit amplifier that the energy needed per bit per square meter to accomplish satisfactory Signal to Noise Ratio (SNR).

\( d \) is the distance from sender node to receiver node.

\( K \) is the packet size in bit.
Where face recognition is a challenging problematic task in the area of pattern recognition and image processing; it is a challenge mission in terms of hardware that is generating physical implementation and software that is emerging algorithmic solutions [7]. In 1991, Turk and Pentland [8] had presented a near real time face recognition system by computing the Eigen faces using Principle Component Analysis (PCA) algorithm on the trained data set. Their recognition rate is good but sensitive to lighting and orientation variations. Since that time many researchers took on this technique in their work of developing the face recognition systems and boosting it with preprocessing or on part of its flow. Haghighat et al [9] had used Gabor filter and PCA. They downed sampling the huge features accomplished by Gabor filter to produce a relatively smaller feature vector used with PCA. Abdulminuim and Ibrahim [10] prove the Gabor DC-based approach in reducing the dimension of the huge features to a small feature vector.

**Proposed approach**

Complex Gabor filter works in time and frequency domain. Complex Gabor function is Fourier transform kernel plus Gaussian function. Filters are generated at different scales and orientations. For feature extraction process, the original image has been convoluted by the set of Gabor filters of different scales and orientations producing a large frequency spectrum representing in an image size by number of filters by two (real and imaginary).

The suggested method is depending on reducing the spectrum array by extracting the high energy DC component from each Gabor filter applied. Then the amplitude (absolute) value is computed. This has been representing the feature vector of a given face. Two scales and five orientations have been considered. This procedure produces an efficient small in size full of information features that traveling in the network with less communication power consuming to preserve the WSN power. The basic flow of the work is presented in figure (1). Zero mean and unit variance metric is the motivational factor for the normalized method suggested. In this method higher moment level are calculated. Skewness, the third standardized central moment, is known as the measure of symmetry – or as more accurate asymmetry – of the dataset. The perfect of symmetric normal distribution has skewness value of zero. Negative skewed value indicates a left skewed distribution while positive skewed value indicates a
right skewed distribution. In general, for fast and accurate recognition and classification, normal distribution for the features is aimed. Kurtosis, the fourth standardized central moment, generally is known as the measure of combined weight for the distribution and its tails. The perfect normal distribution has kurtosis value of zero. In practical side as the value of kurtosis is approaching (close) to zero, the normal distribution is a lot considered. That what is aimed. Generally, the suggested transform has better operation with small data size reflecting the aspect of skewness and kurtosis. Therefore, as the data in the feature vector has enough small size, the transform work perfectly in this space. The drawback and limitation of this suggested transform has been appeared in the computation complexity of the third and fourth moment. Also the previous mentioned limitation of the accuracy of skewness and kurtosis with the large data size. For these reasons this method is applied to small data size and specifically, it is suggested to the numbers coming from complex numbers generated by Gabor filter. Algorithm (1) is explained the suggested ZSZK transform.

**Algorithm (1):** Zero Skewness Zero Kurtosis (ZSZK) algorithm

**Input:** X vector to be normalized.

**Output:** $X_n$ normalized vector.

**Begin**

**Step1:** compute m mean value by:

$$m = \frac{1}{n} \sum_{i=1}^{n} X_i$$

**Step2:** compute std standard deviation value by:

$$std = \sqrt{\frac{1}{n-1} \sum_{i=1}^{n} (X_i - m)^2}$$

**Step3:** compute the skewness value sk by:

$$sk = \frac{\sum_{i=1}^{n} (X_i - m)^3}{n std^3}$$

**Step4:** compute the kurtosis value kt by:

$$kt = \frac{\sum_{i=1}^{n} (X_i - m)^4}{n std^4}$$

**Step5:** normalize the vector X where i=1..n, by:

$$X_{ni} = \frac{X_i - sk}{kt}$$

**End.**
Figure (1): Basic flowchart for GB-based ZSZK method.
A multihop routing protocol based on Gossip routing protocol is suggested to route the packets in the network. The routing protocol overcomes the random selection of nodes of the traditional gossip routing protocol. Proposed Energy Gossip Protocol (PEGP) selects the one destination node that has the higher remaining energy.

**Implementations, experiments and results.**

In the work the entry sensor node is considered to have a camera to compute the face image and send it to the base station node that complete the extraction of the features and make the decisions of acceptance / refuse the face. The work is tested on Matlab® 2010a using FACES94 database. The database has images of 153 individual’s grouped to male, female and male_staff each has 20 image taken while he/she is spoken with a little variation to position. The image is colored with resolution of 180×200. In the work the images are converted to grayscale images as a first step.

Reducing the traveling data in WSN is the main aspect to preserve the power of the network. Referring to the aforementioned in [10] of the computational complexity of Gabor filter is $O(N^2 \times M^2)$ where $N$ is the dimensions of image and $M$ is the dimensions of mask filters with all the proved results we got. The reduced feature vector is traveling over the WNS reaching to the base station node. In base station it would be the PFV that applied to (Feature Eigen Face) FEF algorithm to compute the FEFs. In FEF algorithm, this feature vector has a dimensionality reduction also. The performance has been appeared in two ways, recognition rate and the selected FEVs which mean that the features selected have high energy.

This method is tested over several sets of training and testing dataset. Each training dataset has different numbers of images per individual. Experiments have shown that there is no effect of increasing the number of training images per individual for more than two images in recognition criteria. There is no effect at all in the number of selected FEFs.

For the GB method, the training of 20 images (2 images per individual) is resulted in FMI shown in figure (2) and weight of each input image in the training set is shown in figure (3).
Figure (2): Feature Mean Image (FMI) of GB method.

![Feature Mean Image (FMI) of GB method.](image)

Figure (3): Training dataset weight in feature face space of GB method.

![Training dataset weight in feature face space of GB method.](image)
The method without any normalization in real gives recognition rate of 98% and with the normalization transform the rate ups to 100%. Applying ZSZK normalization to GB method has an efficient effect. While the vectors have maintained their shape with narrower range to simplify the calculations. A safe distance between vectors has been kept to give each vector its identity. The details are shown in figure (4).

![Normalized Feature Vectors](image)

**Figure(4): ZSZK normalization on features of GB method.**

The influence of the application methods on the PEGP routing protocol that depending on Gossip protocol can be shown in the network remaining time and node remaining time to keep nodes live. This influence is due to the changing in the packet size while the execution run time over the nodes is relatively small that can be discounted especially when computation time had lower load of energy consuming than other parts sensor node.

In spite of the comparatively large time consumed to calculate the feature vector in this method but it stays satisfied in term of computation of the sensor node. Also its smaller transmitted data size makes it an efficient method. Figure (5) shows the network energy maintained after transmitting 2000 packets in the network. In figure (6) the nodes still alive...
have presented. Figure (7) clarifies the number of hops in each transmission of packets. Figure (8) displays the total time of the overall 2000 simulation rounds.

Figure (5): Remaining network energy using GB method.

Figure (6): Nodes still alive in network using GB method.
Figure(7): End to end delay (no. of hops) of network using GB method.

Figure(8): Transmiting data delay in network using GB method.
Testing for an authenticated individual shown in figure (9-a) and the distance errors with the FEFs is shown in figure (9-b). It is clear that recognizing the faces is obviously discriminatory to the classes. And testing for unauthenticated individual shown in figure (10-a) and the distance errors with the FEFs is shown in figure (10-b). It is clear that all the values are high (i.e. exceed the threshold value).

Figure (9-a): input tested facial image of authorized individual

Figure (9-b): Euclidean distance of the testing image in (a) with FEF manipulated by Gabor filter.
Hybrid Face Recognition Algorithm for Wireless Sensor Network

Matheel E. Abdulmunem and Fatima B. Ibrahim

Figure (10-a): input tested facial image of unauthorized individual

Figure (10-b): Euclidean distance of the testing image in (a) with FEF manipulated by Gabor filter.
Conclusion

This paper has presented a face recognition technique working on WSN and based on hybrid method of Gabor filter and the computation of Eigen faces. A good normalization transforms proves its efficiency on improving the recognition rate to 100%. The routing protocol preserves the nodes energy palpably. The suggested system is fast with a less size of data traveling in the network. This is due to the reduction of partially feature vector that is travelled the network. The computation on the base station node is also reduced in complexity due to the small size of features used to compute the Eigen faces. While the face recognition algorithm proved to work with WSN, it will be suitable to work with low cost hardware implementation, real time system and other multimedia networks. The method can be enhancement with an authentication protocol.

References


