International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 14 Issue 1 –APRIL 2015.

Fingerprint combination based on Different Quality Sparse Representation for Authentication

ANISHYA SIVARAM

Department of Computer Science and Engineering, Gnanamani college of Technology, Pachal, Namakkal.

anishyasivaram@gmail.com

P.KUPPUSAMY ,*M.E,Ph.D, Head of the Department,*

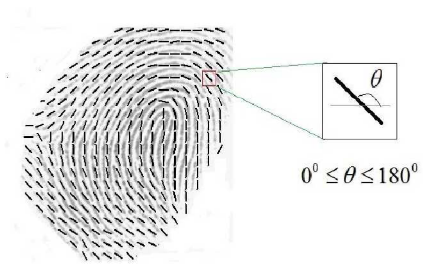
Department of Computer Science and Engineering, Gnanamani College of Technology, Pachal, Namakkal.

ABSTRACT:

Sparse based compression is a new technique for compressing fingerprints. Creating an over complete dictionary from a set of fingerprint patches is used to represent them as a sparse linear combination of dictionary atoms. For this purpose, the first step is to construct a dictionary for predefined fingerprint image patches. For a new fingerprint images, its patches are represented according to the dictionary by computing *l*0-minimization and then quantize and encode it. The experiments demonstrate that the technique is more efficient compared with several competing compression techniques (JPEG, JPEG 2000, and WSQ), especially at high compression ratios. The experiments also show that the proposed algorithm is robust to extract minutiae. In the authentication, the system requires two query fingerprints from the same two fingers which are used in the enrollment. A two-stage fingerprint matching process is proposed for matching the two query fingerprint against a combined minutiae template.

INTRODUCTION:

Person RECOGNITION by means of biometric feature is an important technology in the society, because biometric identifiers can't be shared and they intrinsically represent the individual's bodily identity. Among several biometric recognition technologies, fingerprint recognition is the most commonly used one for personal identification due to the uniqueness, universality, collectability and invariance. Every day huge amount of fingerprints are collected and stored for wide range of applications, including forensics and access control. In 1995, the size of the FBI fingerprint card archive contained over 200 million items and archive size was increasing at the rate of 30000 to 50000 new cards per day. Large volume of data consumes huge amount of memory. Thus Fingerprint compression is a key technique to solve the problem. Fingerprint Compression Based on Sparse Representation for authentication illustrates how to use sparse representation to compress fingerprint images and provides authentication. This process includes a dictionary construction, chosen fingerprint compression, quantization and coding, analysis of the algorithm complexity and performing authentication. As much as information is stored in the dictionary its size will increase. Therefore, to obtain a dictionary with a modest size, the pre-processing is used. Due to transformation, rotation and noise, the fingerprints of the same finger may look very different. Due to reason each fingerprint image is pre-aligned, independently of the others. The pre-alignment technique translates and rotates the fingerprint according to the position of the core point. Reliable detection of the core is very difficult in fingerprint images with poor quality. Compared with natural images, the fingerprint images have simpler structure and are composed of ridges and valleys. In the local regions, they look the same. To solve the above two problems, the whole fingerprint image is sliced into square and non-overlapping small patches. For these patches, there are no problems of transformation and rotation. And the size of the dictionary is not too large because the patches are relatively smaller.



Finger print representation

The above figure shows the fingerprint image and its corresponding orientation image computed over a square-meshed grid. Each element denotes the local orientation of the fingerprint ridges.

Construction of the Dictionary

The dictionary is constructed in three ways. First, construct a training set. And the dictionary is obtained from the set. A greedy algorithm is used to construct the training samples.

- Initially the dictionary is empty and first patch is added to the dictionary.
- Then next patch is considered and check whether it is similar to any patches in the dictionary. If yes, the next patch is tested; otherwise,it is added into the dictionary.The similarity measure between two patches is calculated by solving the optimization problem.

*S(P*1*, P*2*)* = min *t*_ *P*1_*P*1_2 *F* − *t* ∗*P*2 _*P*2_2 *F* _2 *F*

where _ • _2 *F* is the Frobenius norm. *P*1 and *P*2 are the corresponding patch matrices of P1 and P2,. *t*, is a scaling factor used as a parameter of the optimization problem.

- Repeat the second step until all patches have been tested. The mean value of each patch is calculated and subtracted from the corresponding patch, after that the dictionary is constructed. Next, details of the three methods are given.
- The first method: choose fingerprint patches from the training samples at random and arrange these patches as columns of the dictionary matrix.
- The second method: Divide the interval [00, . . . ,1800] into equal-size intervals. Each interval is represented by an orientation (the middle value of each interval is chosen). Choose the same number of patches for each interval and arrange them into the dictionary.
- The third method: it is the K-SVD method. The dictionary is constructed by iteratively solving an optimization problem. *Y* is consisted of the training patches, *A* is the dictionary, *X* are the coefficients and *Xi* is the i^{th} column of *X*. In the sparse solving stage, compute the coefficients matrix *X* using MP method, which guarantees that the coefficient vector *Xi* has no more than *T* non-zero elements. Then, update each dictionary element based on the singular value decomposition (SVD).

min*A*,*X* _*Y* − *AX*_2 *F s.t.*∀*i*, _*Xi* _0 < *T*

Compression of a Given Fingerprint

For a given fingerprint, slice it into square patches as the same size with the training patches. Make the patches fit the dictionary better, the mean of each patch is to be calculated and subtracted from the patch. Then compute the sparse representation for each patch by solving the *l*0 problem. Those coefficients whose absolute values are less than a given threshold are treated as zero. For each patch, four kinds of information need to be recorded. They are the mean value, the number about how many atoms to use, the coefficients and their locations. This method reduces the coding complexity and improves the compression ratio.

Coding and Quantization

Entropy coding of the atom number of each patch, the mean value of each patch, the coefficients and the indexes is performed by using a static arithmetic coder. The atom number of each patch is separately coded. The mean value of each patch is also separately coded. The quantization of coefficients is performed using the Lloyd algorithm, learnt off-line from the coefficients which are obtained from the training set by the MP algorithm over the dictionary. The first coefficient of each block is quantized with a larger number of bits than other coefficients and entropy-coded using a separate arithmetic coder. Here the first coefficient is quantized with 6 bits and other coefficients are quantized with 4 bits.

Analysis of the Algorithm Complexity

The algorithm consists of two parts, the training process and the compression process. The training process is off-line, thus the complexity of compression process is analyzed.

Suppose the size of the patch is $m \times n$ and the number of patches in the dictionary is *N*. Each block is coded with *L* coefficients. *L* is the average number of non-zero elements in the coefficient vectors. To represent each patch with respect to the dictionary, every iteration of the MP algorithm includes *mnN*scalar products. The total number of scalar multiplications of each patch is *LmnN*. Given a fingerprint image with $M1 \times N1$ pixels. The number of patches of the fingerprint image is approximately equal to $M1\times N1/m\times n$. Therefore, the total number of scalar multiplications for compressing a fingerprint image is $M1\times N1\ /m\times n \times LmnN$, ie, $LM1N1N$. The compressed technique doesn't include the dictionary and the information about the models. It consists of only the encoding of the atom number of each patch, the mean value of each patch, the coefficients plus the indexes. In practice, only the compressed stream needs to be transmitted to restore the fingerprint. In both encoder and the decoder, the dictionary, the quantization tables of the coefficients and the statistic tables for arithmetic coding need to be stored. This leads to less than 6 Mbytes. The compression rate equals the ratio of the size of original image and that of the compressed stream.

PROPOSED SYSTEM:

In proposed system, construct a base matrix whose columns represent features of the fingerprint images, by referring the matrix dictionary whose columns are called atoms; for a given fingerprint, divide it into small blocks called patches whose number of pixels are equal to the dimension of the atoms; use the method of sparse representation to obtain the coefficients; then, quantize the coefficients and then encode the it and other related information using lossless coding methods. In most instances, the evaluation of compression performance of the algorithms is restricted to Peak Signal to Noise Ratio (PSNR) computation.. In most Automatic Fingerprint identification System (AFIS), the main feature used to match two fingerprint images are minutiae (ridges endings and bifurcations). Therefore, the difference of the minutiae between pre- and post-compression is considered here.

Matching Algorithm:

First the finger print compression introduced after that compressed images two finger combination based new finger print create for high secure privacy protection. We propose here a novel system for protecting fingerprint privacy by combining two different fingerprints into a new identity. In the enrollment, two fingerprints are captured from two different fingers. Then extract the minutiae positions from one fingerprint, the orientation from the other fingerprint, and the reference points from both fingerprints. Based on this extracted information and our proposed coding strategies, a combined minutiae template is generated and stored in a database. In the authentication, the system requires two query fingerprints from the same two fingers which are used in the enrollment. A two-stage fingerprint matching process is proposed for matching the two query fingerprint against a combined minutiae template.

Mathematics

For the following implementation, let us assume we are dealing with a standard 2D array of data or matrix. The dimensions of the correct image matrix and the dimensions of the degraded image matrix must be identical.The mathematical representation of the **PSNR** is as follows:

$$PSNR = 20\log_{10}\left(\frac{MAX_f}{\sqrt{MSE}}\right)$$

Figure 1 - Peak Signal-to-Noise Equation

where the **MSE** (Mean Squared Error) is:

$$MSE = \frac{1}{mn}\sum_{0}^{m-1}\sum_{0}^{n-1}\|f(i,j) - g(i,j)\|^2$$

Figure 2 - Mean Squared Error Equation

This can also be represented in a text based format as:

MSE = (1/(m*n))*sum(sum((f-g).^2))

PSNR =20*log(max(max(f)))/((MSE)^0.5)

Legend:

f represents the matrix data of our original image

g represents the matrix data of our degraded image in question

m represents the numbers of rows of pixels of the images and i represents the index of that row

n represents the number of columns of pixels of the image and j represents the index of that column

MAX_f is the maximum signal value that exists in our original "known to be good" image

Motivation for Use as an Image Quality Metric

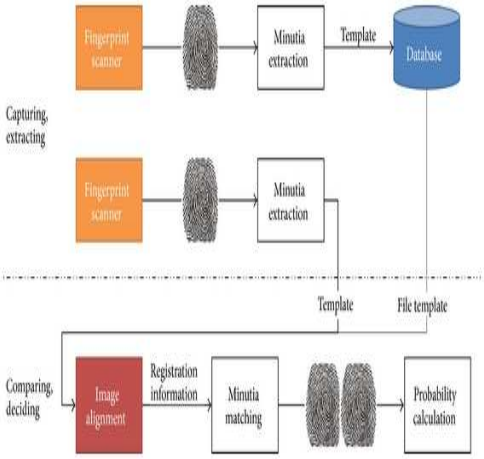
The mean squared error (MSE) for our practical purposes allows us to compare the "true" pixel values of our original image to our degraded image.

The MSE represents the average of the squares of the "errors" between our actual image and our noisy image. The error is the amount by which the values of the original image differ from the degraded image. The proposal is that the higher the

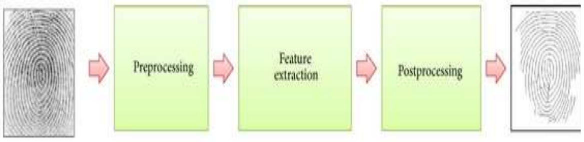
PSNR, the better degraded image has been reconstructed to match the original image and the better the reconstructive algorithm. This would occur because we wish to minimize the MSE between images with respect the maximum signal value of the image.

Matching Application:

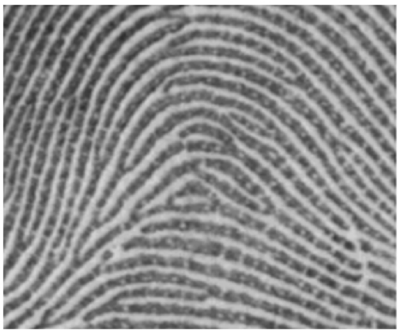
The fingerprint recognition mechanism goes through two steps of feature extraction and fingerprint matching.



The feature extraction step is the step for configuring minutiae data files to be used in the fingerprint matching step and is conducted in three steps of preprocessing, minutiae extraction, post processing, as shown in Figure.



A fingerprint image is classified into one of the images with a lot of noises. A fingerprint is a body part going through a lot of state changes such as injuries or moisture. Thus, fingerprint images obtained through the device are likely to be mixed with noises. In the image improvement step, the work clarifying the distinction between ridges and valleys is carried out by reducing noises . The most commonly used method is to use adaptive filter. It uses the fact that if knowing ridge local orientation around applied pixels and applying adaptive filter, ridges with the same direction become clear. In this process, the bridge of neighboring rides resulting from noises is removed and the result of connecting broken ridges is often shown. Directional Fourier filter , Gabor filter and so forth, are widely used adaptive filters, and the method using mask operation is also use.When image improvement work is finished, the process of extracting ridges is started. Fingerprint images usually have grayscale of 256 but this can be simplified into the binary information of ridges and valleys as binarized image of Figure.



There is a difficulty that binarization cannot be done by using single intensity threshold because all fingerprint images do not have constant image contrast in the process of making binary images, and even the contrast ratio of the same person’s fingerprints varies every time the device is pressed on. Therefore, the dynamic thresholding method is applied depending on image distribution pixel values and through it, the whole image is binarized into the ridge part and nonridge part.The final step of preprocessing to extract minutiae is the thinning step and this refers to the work reducing the width of ridges obtained after binarization into one pixel like minutiae extraction after thinning of Figure. This process must not only fully maintain coconnectivity of found ridges but minimize wrong minutiae information that may occur through this step. Many algorithms have been using this method because minutiae can be found quickly and easily through simple mask operations with thinned fingerprint images.Recently, due to the rapid growth of the Internet with the development of computers, the need for personal authentication system at the private level which is easy to use while providing reliable security level has increased. Thus, developers came to develop algorithms and systems by focusing on the private demand of personal authentication, and many biometric authentication systems are currently commercialized and used. However, unlike other authentication methods, these biometric authentication systems have the disadvantage that they cannot be changed (keys or passwords are easy to change). Confidential authentication should be possible to change. In addition to the personal information leakage problem caused by biometric information leak, the biometric authentication technique such as fingerprint recognition cannot be changed. When their fingerprint information was leaked, all information recognized by computers can be copied and used. All the secrets entered by their fingerprint information come to nothing. Fingerprint information is no longer available, and it is highly likely to be abused. Therefore, their authentication information should be possible to change. This study tries to propose the authentication system that can be changed by using number-based password and fingerprint biometric authentication.

SIMULATION RESULT:

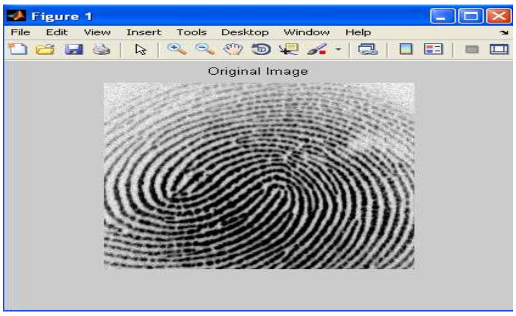


Fig 1: Input Image

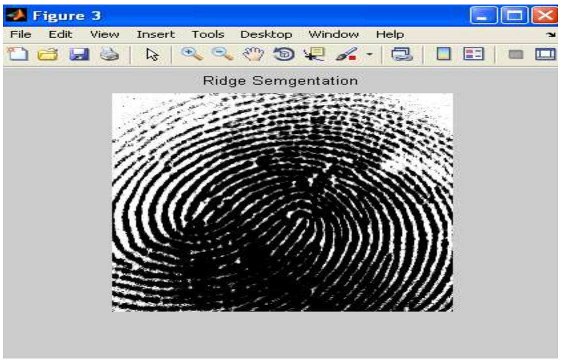


Fig 2: Ridge Segmentation

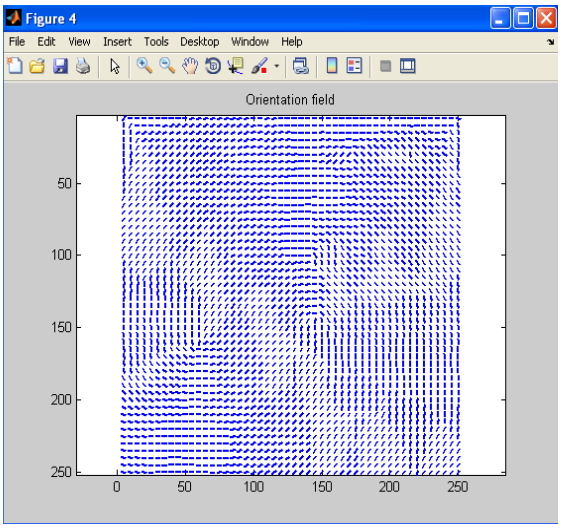


Fig 3: Orientation Field Extraction

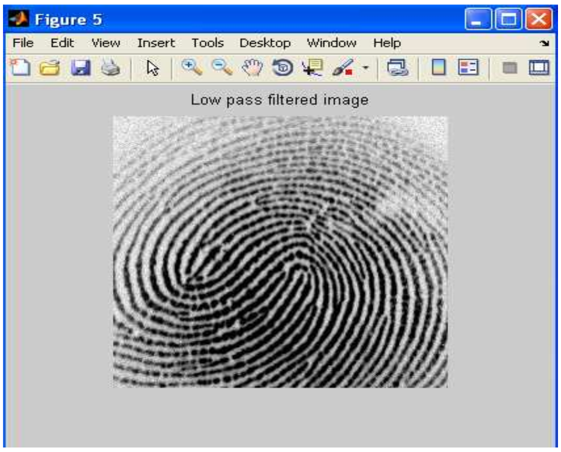


Fig 4: Low pass Filter Image

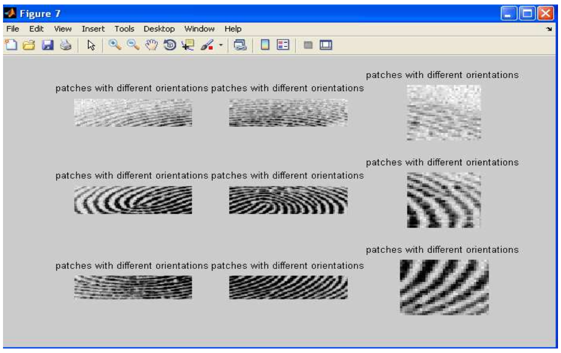


Figure 7
File Edit View Insert Tools Desktop Window Help
patches with different orientations
patches with different orientations
patches with different orientations
patches with different orientations
patches with different orientations
patches with different orientations
patches with different orientations
patches with different orientations
patches with different orientations

Fig 5: Patches with different Orientation

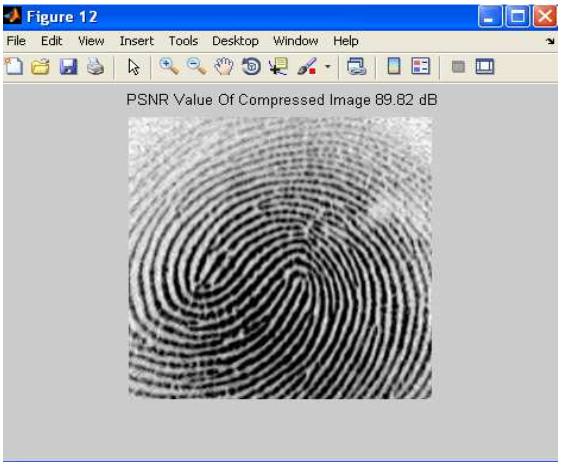


Figure 12
File Edit View Insert Tools Desktop Window Help
PSNR Value Of Compressed Image 89.82 dB

Fig 6: Compressed image

ADVANTAGE OF PROPOSED SYSTEM

- Includes authentication mechanism
- More efficient

CONCLUSION:

Finger print compression introduced after that compressed images two finger combination based new finger print create for high secure privacy protection. Here a novel system for protecting fingerprints privacy by combining two different fingerprints into a new identity. In the enrollment, fingerprints are captured from fingers. Then extract the minutiae positions from one fingerprint, the orientation from the other fingerprint, and the reference points from both fingerprints. Based on this extracted information and our proposed coding strategies, a combined minutiae template is generated and stored in a database. In the authentication, the system requires two query fingerprints from the same two fingers which are used in the enrollment. A two-stage fingerprint matching process is proposed for matching the two query fingerprint against a combined minutiae template.

ACKNOWLEDGEMENT

I would like to thank all the faculties and students of Computer Science and Engineering Department, Gnanamani College of Technology for their guidance and support and facilities extended to me.

REFERENCE PAPER:

[1] Fingerprint compression based on sparse representation by GuangqiShao,YanpingWu,YongA,Xiao Liu and TiandeGuo

[2] Fingerprint Compression Using ContourletTransform and Multistage Vector QuantizationS. Esakkirajan, T. Veerakumar, V. SenthilMurugan and R. Sudhakar

[3] Fingerprint Classification and Matching Usinga FilterbankBySalilPrabhakar

[4] Image Super-Resolution as Sparse Representation of Raw Image PatchesJianchao Yang, John Wright, Yi Ma, Thomas Huang University of Illinois at Urbana-ChampaginBeckman Institute and Coordinated Science Laborator

[5] K-SVD: An Algorithm for Designing OvercompleteDictionaries for Sparse Representation Michal Aharon, Michael Elad, and Alfred Bruckstein

[6] On the use of independent component analysis for image compression Artur J. Ferreiraa,_, Ma´ rio A.T. Figueiredo

[7]The JPEG-2000 Still Image Compression Standard(Last Revised: 2002-1225) by Michael D. Adams,AssistantProfessor,Dept. of Electrical and Computer Engineering,University of Victoria,P. O. Box 3055 STN CSC, Victoria, BC, V8W 3P6,CANADAE-mail: mdadams@ece.uvic.caWeb: www.ece.uvic.ca/˜mdadams

[8] The JPEG Still Picture Compression StandardGregory K. WallaceMultimedia Engineering,Digital Equipment Corporation,Maynard, Massachusetts

[9]WSQ GRAY-SCALEFINGERPRINT IMAGE COMPRESSION SPECIFICATION,Criminal Justice Information Services DivisionFederal Bureau of Investigation1000 Custer Hollow Road,Clarksburg, WV 26306