FPGA Implementation of Fingerprint Recognition System using Adaptive Threshold Technique

Satish S Bhairannawar1, Anand R2
1,2Department of Electronics and Communication Engineering, DayanandaSagar College of Engineering, Bangalore, India
1satishbhairannawar@gmail.com

Raja K B3 and Venugopal K R4
3Department of Electronics and Communication Engineering, UVCE, Bangalore, India
4Principal, University Visvesvaraya College of Engineering, Bangalore University, Bangalore, India

Abstract—The real time fingerprint biometric system is implemented using FGPA. In this paper, we propose FPGA Implementation of Fingerprint Recognition System using Adaptive Threshold Technique with novel adaptive threshold for each person. The fingerprint images are considered from FVC2004 (DB3_A) and processed to resize fingerprint size to 256x256. The DWT is applied on fingerprint and considered only LL coefficients as features of fingerprint. The Adaptive Threshold value for each person is computed using Deviations between two successive samples of a person, Average Deviation, Standard Deviation and constant. The Adaptive Threshold for test image is computed using Deviations between test images and samples of database, Average Deviation, Standard Deviation and constant. If the Average Threshold of test image is less than Average Threshold of a person then it is considered as match else mismatched. It is observed that the success rate of identifying a person is high in the proposed method compared to existing techniques and also the device utilization in the proposed architecture is less compared to existing architectures.

Keywords— Biometrics, Fingerprint identification, Haar 2D-DWT architecture, Adaptive threshold and Adaptive comparator.

I. INTRODUCTION

The authentication of human beings is very important in the world for the reasons (i) Differentiate criminals and non-criminals to avoid terrorism. (ii) Identify status of a person in terms of annual income like GE, PSE, Business Persons, and Student etc., to avoid black money transactions for the growth of a nation. (iii) The credit card, debit card and currency notes can be eliminated to avoid fraudulent and robbery by identifying a person with proper annual income and (iv) The database of a nation is created to avoid intruders from neighbouring countries. The traditional methods used to identify a person are smart cards, PIN, tokens, passwords etc., which can be lost or stolen and hence not preferred to use. The biometric is an alternate method to traditional methods of identifying persons. The biometric trails can’t be lost or stolen, as these are human body parts and behavior of a person, hence accurate identification can be achieved.

Fingerprint based identification is one of the most important biometric technology, which has drawn a substantial amount of attention recently, since the process of acquiring fingerprint samples are simple and also believed to be unique among individual persons. These essential attributes of fingerprint samples leads to the increased use of automatic fingerprint based identification in both civilian and military applications.

Kavita Tewari and Renu L Kalakoti [1] proposed techniques like Fast Fourier Transform (FFT), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT) for feature extraction. These features consist of mean energy, standard deviation and Shannon entropy. The performance was evaluated on the basis of parameters like Correct Detection Rate (CDR), Correct Rejection Rate (CRR), Total Success Rate (TSR), Miss Rate (MR) and False Positive Rate (FPR). Javier Galbally et al., [2] proposed software-based fake detection method that can be used in multiple biometric systems to detect different types of fraudulent access attempts. The objective of the system is to enhance the security of biometric recognition frameworks, by adding liveness assessment in a fast, user-friendly, and non-intrusive manner, through the use of image quality assessment. The DWT has been extensively used for image processing which uses sub-band coding techniques that employs filtering methods with different cut-off frequencies at different scales. The main advantages of using DWT are time-frequency resolution and multilevel image decomposition. Most of the available DWT architectures [3, 4] are based on high speed linear convolution property of the wavelet filters. Many 2D-DWT architectures have been suggested for efficient hardware implementation. In the subsequent few of them are discussed. The four-processor architecture for 2D-DWT is used for block based implementation which requires large memory [5]. Liao et al., [6] proposed 2D-DWT dual scan architecture, which requires two lines of data samples simultaneously for forward 2D-DWT and also another 2D-DWT architecture, which accomplished decomposition of all stages that result in inefficient hardware utilization and more sophisticated control circuitry. Barua et al., [7] proposed folded based architecture for 2D-DWT by using hybrid level at each stage. In this approach the image is scanned in a raster format by using row processor which decreases the speed of entire structure. The development of VLSI architectures on reprogrammable hardware [8-10] with incorporation of general purpose microprocessor unit for automated fingerprint identification proves to be efficient and economical solution. Mariano Fons et al., [11] proposed FPGA based personal verification system using fingerprints in which they performed an evaluation of system architectures substitute to existing personal computers.

978-1-4799-7678-2/15/$31.00 ©2015 IEEE
Contributions

In this paper, the FPGA implementation of fingerprint recognition system using adaptive threshold is proposed. The 2D-DWT architecture is used to generate LL band coefficients of fingerprint images. The adaptive threshold for each person and test image is calculated and matching is performed to improve performance parameters.

II. PROPOSED HARDWARE ARCHITECTURE

The novel technique of adaptive threshold for each person and test image are computed using average difference, standard deviation and system parameter constant to improve matching technique. The basic block diagram of Top Module of fingerprint identification system is shown in Fig. 1. The Control Unit (CU) controls all components in a particular order to obtain the desired result. The CU works with different states to synchronize all components and also introduces wait states to maintain absolute synchronization between all components. The Control Unit (CU) is also used to turn off individual blocks when not in use resulting in low power optimization of the system.

A. Database Image

The fingerprint database of FVC2004 is considered to test the performance of biometric system. The DB3_A database of FVC2004 [12] has 8 fingerprint samples per person as shown in the Fig. 2. The total numbers of persons in DB3_A are 100 with 8 sample images per person with each fingerprint size of 300x480. The original fingerprint image is resized to 256x256 in pre-processing.

B. Implementation of 2D Haar DWT

The image is divided into 2x2 non-overlapping matrices to calculate LL coefficients. The hardware structure for generating LL-band using 2D Haar transform is shown in Fig. 3. The non-overlapping 2x2 matrix block of an image is considered to compute LL coefficients. The D flip-flops (D ff’s) and Shift Register are connected in series to form shift register of 258 data samples for 256x256 image. The connections from four flip flops which form 2x2 matrices are connected to adder which performs addition of all four pixel values in turn right shifted using shifter block to obtain the required LL coefficients. The clk_div block is used to achieve divide by 2 of clk which in turn connected to D ff to obtain 2x2 non-overlapping matrices.

C. Implementation of Adaptive Threshold

The deviations between two column vectors in the database and deviations between test and database vectors are computed. The maximum and minimum deviations are averaged using adders and shifters. The $\sigma$ and $\lambda$ are multiplied and added with average deviation to obtain $AT$ using multiplier and adder respectively. Similarly $ATT$ of test image with database is also computed. The $AAT$ is compared with $AT$. The values of $AAT$ are compared with $AT$ values in the database. If $AAT$ values are less than $AT$ then the person is matched or else mismatched. The basic block diagram of adaptive threshold implementation is shown in Fig. 4.

Fig. 1. Top Level Description of Hardware Implementation of Fingerprint System

Fig. 2. Eight Sample Images of a Person of FVC2004 (DB3_A) Database

Fig. 3. Hardware Structure for LL band of 2D Haar Transform

Fig. 4. Block Diagram of Adaptive Threshold Implementation
III. MATHEMATICAL MODEL

A. Deviations between two images in the Database

The column vectors of seven fingerprint samples of a person in database are considered and deviations between two column vectors are computed using Average Deviation (AD). The AD between corresponding coefficients of two samples of a person in the database is computed using the following pseudo code.

```
for l = 1: (k - 1)
for i = (l + 1): k
    AD(X_l, X_i) = \frac{\sum_{j=1}^{m}|x(j)_l - x(j)_i|}{m}
end
end
```

Where, I and i are column vector variables of database image samples, k is total number of image samples in database per person, m is total number of LL coefficient features i.e., 16384.

Example

The AD between first column vector \(X_1\) and second column vector \(X_2\) of first person is computed using equation (2).

\[ AD(X_1, X_2) = \frac{\sum_{j=1}^{m}|x(j)_1 - x(j)_2|}{m} \]

1) Adaptive Threshold (AT) of a person in the Database:

The Max(AD) and Min(AD) of first person and compute average of \(\text{Max}(AD)\) and \(\text{Min}(AD)\) using equation (3).

\[ C = \frac{\text{Max}(AD) + \text{Min}(AD)}{2} \]  

The standard deviation \(\sigma\) are calculated using AD’s given by equation (4)

\[ \sigma = [AD(x_1, x_2), AD(x_1, x_3), ... AD(x_1, x_7)] \]

The Adaptive Threshold (AT) for each person in the database is calculated using the parameters \(C, \sigma\) and system parameter (\(\lambda\)) using equation (5).

\[ AT_1 = C + \lambda \cdot \sigma \]

Similarly Adaptive Threshold values \([AT_1, AT_2, ..., AT_p]\) are computed for all persons in the database.

2) Compute Adaptive Threshold of Test image

The AD of test image samples with image in database is computed using equation (6).

```
for T = 1: p
for S = 1: q
    AD_T(X_T, X_S) = \frac{\sum_{j=1}^{m}|x(j)_T - x(j)_S|}{m}
end
end
```

Where, q is total number of image samples in database= \(p \times k\). p is total number of persons. T is the test image sample.

Example

The AD of test image with first image in the data base is computed as using equation (7)

\[ AD_T(X_T, X_1) = \frac{\sum_{j=1}^{m}|x(j)_T - x(j)_1|}{m} \]

Similarly compute AD’s between test image and all image samples in database using equation (8).

\[ AD_T(X_T, X_q) = \frac{\sum_{j=1}^{m}|x(j)_T - x(j)_q|}{m} \]

The Average of AD of each person is computed using equation (9)

\[ A_{AD_T} = \frac{1}{K} \sum_{l=1}^{K}(AD_T(x_T, X_l)) \]

Where, K is number of samples per person.

Similarly the Average of AD of remaining persons are computed with test image using equation (10).

\[ A_{AD_T} = \frac{1}{K} \sum_{p=1}^{K}(AD_T(x_T, X_p)) \]

Note the max and min of \(A_{AD_T} \) and compute \(CT\) using equation (11)

\[ C_T = \frac{\text{Max}(A_{AD_T}) + \text{Min}(A_{AD_T})}{2} \]

The standard deviation \(\sigma\) are calculated using Average AD’s given in equation (12)

\[ \sigma = (A_{AD_T1}, A_{AD_T2}, ..., A_{AD_Tp}) \]

Now, Adaptive threshold of test is given using equation (13).

\[ ATT = C + \lambda \cdot \sigma \]

Where, \(\lambda = 0.5\)

3) Comparison of test and Database images

The computed AAT values of test images are compared with AT values of the database person. If the AAT value is less than AT then the test image is matched with the corresponding person.

IV. PERFORMANCE ANALYSIS

A. Software Simulation and Comparison

The algorithm is implemented using MATLAB. The percentage values of TSR of proposed method is compared
TABLE I. COMPARISON OF PERCENTAGE EER AND TSR VALUES OF PROPOSED METHOD WITH EXISTING METHODS

<table>
<thead>
<tr>
<th>Author</th>
<th>Techniques</th>
<th>%TSR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maya and Sethu [14]</td>
<td>Curvelet-Euclidean</td>
<td>95.02</td>
</tr>
<tr>
<td>Dattatray and Pawan [15]</td>
<td>DWT and PCA</td>
<td>96.3</td>
</tr>
<tr>
<td>M. Mani and Sudhir [16]</td>
<td>OR Logic (DCT)</td>
<td>95</td>
</tr>
<tr>
<td>Jossy P. George et al., [17]</td>
<td>DTCWT</td>
<td>85</td>
</tr>
<tr>
<td>Proposed Method</td>
<td>Adaptive Threshold</td>
<td>96.5</td>
</tr>
</tbody>
</table>

The algorithm uses novel adaptive threshold technique where unique adaptive thresholds are calculated for each person compared to traditional method of having fixed threshold for fingerprint matching. This unique method of calculating thresholds are based on average difference (AD) between image samples C, standard deviation between image samples and constant which improves the tolerance for matching accuracy.

B. Hardware Implementation

The proposed architectures are implemented on FPGA device using Spartan-3 xc3s400-4pq208 commercial version with speed grade -4. The TABLE II shows the hardware requirements with respect to performance for the FPGA implementation. The deviation calculations require 39 slices, 59 flip-flops, 32 4-input LUT's and 1 GCLK and to implement Haar DWT it requires 54 slices, 33 flip-flops, 99 4-input LUT's and 1 GCLK. The Interface Unit, requires 85 slices, 97 flip-flops, 132 4-input LUT'S and 2 GCLKs.

TABLE II. SYNTHESIS REPORTS ON FPGA

<table>
<thead>
<tr>
<th>Logic Utilization</th>
<th>Deviation Calculation</th>
<th>DWT</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. of Slices</td>
<td>39</td>
<td>54</td>
<td>85</td>
</tr>
<tr>
<td>No. of Slice Flip Flops</td>
<td>59</td>
<td>33</td>
<td>97</td>
</tr>
<tr>
<td>No. of 4-input LUTs</td>
<td>32</td>
<td>99</td>
<td>132</td>
</tr>
<tr>
<td>No. of Bounded I/OBs</td>
<td>67</td>
<td>43</td>
<td>32</td>
</tr>
<tr>
<td>No. of GCLKs</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

C. Hardware Comparison between Proposed and Existing Architectures

The estimated CLB LUT’s using FPGA for the proposed algorithm and existing algorithms for entire system (pre-processing-matching) are given in TABLE III. The values of area in terms of LUT’s of proposed method is compared with existing methods presented by Fons et al., [18], Marion Lopez and Enrique Canto [19] and Conti et al., [20]. It is observed that the value of used LUT’s are very less in the case of proposed method compared to existing methods.

TABLE III. AREA COMPARISONS OF PROPOSED METHOD AND EXISTING ARCHITECTURES

<table>
<thead>
<tr>
<th>Author</th>
<th>Techniques</th>
<th>Area (LUT's)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fons et al., [18]</td>
<td>Minutiae Based</td>
<td>21504</td>
</tr>
<tr>
<td>Marion Lopez and Enrique Canto [19]</td>
<td>Minutiae Based</td>
<td>7014</td>
</tr>
<tr>
<td>Conti et al., [20]</td>
<td>Minutiae Based and AES Encryption</td>
<td>37031</td>
</tr>
<tr>
<td>Proposed Method</td>
<td>Adaptive Threshold</td>
<td>263</td>
</tr>
</tbody>
</table>

The adaptive threshold techniques are based on adders and comparators. This reduces the computational complexity of hardware utilization and also it helps in reducing power consumption.

V. CONCLUSION

In this paper, the FPGA implementation of fingerprint recognition system using adaptive threshold is proposed. The LL band coefficients are generated using Haar 2D-DWT. The Adaptive Threshold values for each fingerprint coefficients are assigned using Deviations between two successive samples of a person, Average Deviation, Standard Deviation and constant which is unique. The ATT of test image features are calculated using database features and compared with database AT values for matching. The proposed architecture is compared with existing hardware architectures. It is observed that the proposed technique has less hardware utilization of 263 LUT’s, since it uses adders, multipliers and comparators for adaptive threshold calculation matching. Further it helps in reducing the power which is useful for low power fingerprint recognition system.

References


