H.Anandkumar Singh, R.Gayathri/ International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue 2,Mar-Apr 2012, pp.1129-1133

IMAGE AUTHENTICATION TECHNIQUE USING FSIM ALGORITHM

H.Anandkumar Singh*, R.Gayathri **
*(Department of EEE, Vel Tech Dr.RR& Dr.SR Technical University, Chennai)
** (Research Scholar in Anna University College Of Technology Coimbatore &Head,Department of Electronics and Communication Engineering, Vel Tech Dr.RR& Dr.SR Technical University, Chennai)

ABSTRACT:
Image Authentication technique is useful for user protection from fraud login. Authentication will find the best matching image from a database and return respective image ID with respect to Login ID used in single sign on. In this paper we will discussed feature extraction of fingerprint image using canny edge detection and perwit edge detection. Feature Similarity Indexing of image algorithm is used to generate the matching score between the original image in database and the input test image. The experimental results achieve recognition accuracy using canny and perwit FSIM of 96.77% and 97.16%, respectively, on the publicly available database of Hong Kong Polytechnic University. Totally 50 images of 10 individuals, 4 samples for each palm are randomly selected to train in this research. Then we get every person each palm image as a template (total 10).Experimental evaluation using palmprint image database clearly demonstrates the efficient recognition performance of the proposed algorithm using Perwit FSIM gives best result when compared with the Canny FSIM algorithm.

Keyword: IQA, canny edge, log Gabor.PhaseCongruency, Gradient Magnitude, and FSIM.

I. INTRODUCTION

Biometrics is the field of science which identifies a Person based on the physical, chemical or behavioral Characteristics. The relevance of biometrics in future society has been reinforced by the need for large-scale identity management systems whose functionality relies on the accurate determination of an individual's identity.Examples of these applications include sharing networked computer resources, granting access to nuclear facilities, performing remote financial transactions or boarding a commercial flight. The proliferation of online banking and the deployment of decentralized customer service centers (e.g., credit cards) have further underscored the need for reliable identity management systems that can accommodate a large number of individuals.

The important task in an identity management system is the determination (or verification) of an individual's identity (or claimed identity). Such an action may be necessary for a variety of reasons but here, the essential point is that in most applications, is to prevent impostors from accessing protectedresources. Traditional methods of establishing a person's identity include knowledge based (e.g., passwords) and token-based (e.g., ID cards) mechanisms, but these surrogate representations of identity can easily be lost, shared, manipulated ambiguous, stolen thereby compromising the intended security**.** A fingerprint is an orientation texture pattern of interleaved ridges and valleys. Due to robust feature we selected finger print modality.

II. EDGE DETECTION

Edge detection is an essential element in image processing and many techniques have been proposed. Canny proposed an edge-detection operator from an optimization point of view, and evolved that the first derivative of a Gaussian filter was this optimal operator. The idea was that an optimal edge-detector should be a good detector, with good localization, and should give only one detection for a single edge. It was derived from an information theory point of view, computing the SNR, detection and localization for a given edge, noise and detector .In case of step edges, Canny's optimal operator was similar to Marr's LoG. Canny's proposed for the multi-resolution problem was called *feature synthesis*, and is fine-to-coarse. He included two thresholds in an hysteresis threshold; their value depend on the noise estimation. For instance,[1] proposed a coarse-to-fine method, called *edge focusing*. A strong Gaussian smoothing detects edges, and these edges are tracked.Some edge detection filters were developed with optimality canny [2]. Canny [2] evaluated the detectors by three criteria: good detection, good localization and low spurious response, and he showed that the optimal detector for an isolated step edge should be the first derivative of Gaussian. The optimal canny edge detector for ramp edges was proposed by [3].Canny restricted the detector as a finite impulse response (FIR) filter. [4]Extended it to infinite impulse response (IIR) filter. Besides the shape of the detector, another important problem is to set a proper detection scale. Multiple scales should be employed to describe the variety of the edge structures. Then these multi-scale ascriptions will be synthesized to form an edge map.

Canny [2] used a fine-to-coarse feature synthesis strategy to mingle the multiscale edge information based on a set of predefined rules. Considering that the synthesis of the multiscale edges is intricate and itself an ill-posed problem.

In this paper, we presented a multi feature extraction based on edge detection scheme. [6][7]Applying Log Gabor filter to all the images and multiplied as a product function. Unlike many multiscale edge detectors, where the edge maps were formed at several scales and are synthesized together, our scheme determines edges as the local maxima in the product function after filtering. The filter multiplication enhances image structures and suppresses the noise. An integrated edge map will be formed efficiently, while avoiding the ill-posed edge synthesis process. It will be shown that much improvement is obtained on the localization accuracy and the obtained better detection results.

There are different types of biometric that can be used for authentication are speech, Face, signature, palmprint fingerprint, knuckle and IRIS etc.

Figure 1.Given below shows thebiometric samples.

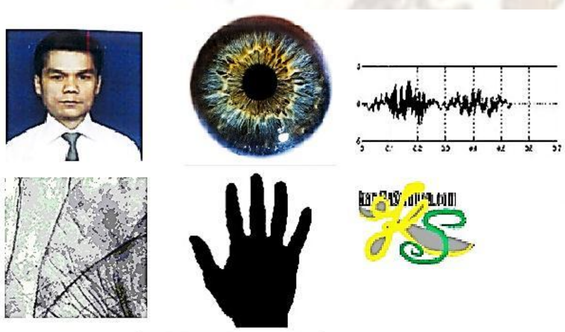


Fig.1 Biometrics samples

There are lots of works done on biometric image authentication. Some of the algorithms used in authentication are:

1. Biometrics for Global Web Authentication: an Open Source Java/J2EE-Based Approach
2. An efficient Iris authentication using chaos theory-based cryptography for e-commerce transactions
3. Biometric Person Authentication Method Using Camera-Based Online Signature Acquisition

III. PROPOSED DESIGN

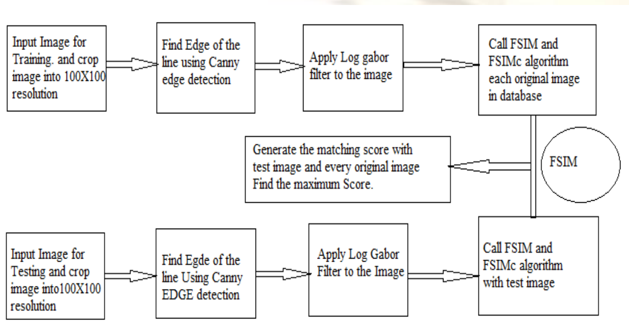


Fig 2: Block Diagram of the Algorithm

1. The image stored in Database undergoes image processing as same as the input test image
2. The line of the palmprint or fingerprint image can be detected using canny edge detection leaving the background.
3. Apply log Gabor filter to remove noise of high frequency.
4. Use FSIM algorithm to find the matching score between the test input image and the original image stored in the database is shown in the figure 2 .

IV. FEATURE SIMILARITY INDEXING

Feature similarity indexing maintains IQA (image quality assurance) based on the fact that human visual system (HVS) understands an image mainly according to its low-level features [6]. The main feature of FSIM is phase congruency which is a dimensionless measure of a local structure. Due to phase congruency the contrast of the image will affect Human visual system but the secondary feature of FSIM which is gradient magnitude control perception of image quality. Phase congruency and Gradient Magnitude play complementary roles in characterizing the image local quality and derive a single quality score.

A. *Phase congruency (PC)*

Rather defining features directly at points with sharp changes in intensity, the Phase Congruency [7] model postulates that features are perceived at points where the Fourier components are maximal in phase.

The 1D signal $g(y)$, has odd symmetric and even symmetric filter scale denoted by $M^o{}_m$ and $M^e{}_m$ which form a quadrature pair.

The signal will form a response vector at position x on scale $m$explained in eqn(1):

$$[E_m(y), O_m(y)] = [h(y)^* P_m^o, h(y)^* P_m^e] \quad (1)$$

The local amplitude on scale n is: t

Let $F(y) = \sum_m E_m(y)$ and
$\text{H}(y) = \sum_m O_m(y)$

Then phase congruency is given by eqn (2)

$$PC(y) = \frac{E(y)}{\epsilon + \sum_m A_m(y)} \quad (2)$$

Where $E(y) = \sqrt{F^2(y) + H^2(y)}$
andε is a small positive constant

We adopt the log-Gabor filters because:

1) One cannot construct Gabor filters of arbitrarily and width and still maintain a reasonably small DC component

in the even-symmetric filter, while log-Gabor filters, by definition, have no DC component; and

2) The transfer function of the log-Gabor filter has an extended tail at the high frequency end, which makes it more capable to encode natural images than ordinary.

The transfer function of a log-Gabor filter in the frequency domain is as follows in eqn(3)

$$G(\omega) = \exp\left(\frac{-(\log\frac{\omega}{\omega_0})^2}{2\sigma_{r1}^2}\right) \quad (3)$$

where ω_0 is the filter's center frequency and σ_r controls the filter's bandwidth.

B. Gradient magnitude (GM)

Image gradient computation is a traditional topic in image processing. Gradient operators can be expressed by convolution masks. Three commonly used gradient operators are the Sobeloperator [8], the Prewitt operator [8] and the Scharr-operator. Their performances will be examined in the section of experimental results.

The partial derivatives $Gx(\mathbf{y})$ and $Gy(\mathbf{y})$ of the image $f(\mathbf{y})$ along horizontal and vertical directions using the three gradient operators are used. The gradient magnitude (GM) of $f(\mathbf{y})$ is then defined as in eqn(4)

$$G = \sqrt{{G_x}^2 + {G_y}^2} \quad (4)$$

C. FSIM Algorithm [6]:

With the extracted PC and GM feature maps, in this section we present a novel Feature Similarity (FSIM) index for IQA. Suppose that we are going to calculate the similarity between images $f1$ (test image) and $f2$ (original image) denote by $PC1$ and $PC2$. The Phase Congruency maps extracted from $f1$ and $f2$, and $G1$ and $G2$ the Gradient Map maps extracted from them. It should be noted that for color images, Phase Congruency and Gradient map features are extracted from their luminance channels. FSIM will be defined and computation based on $PC1$, $PC2$, $G1$ and $G2$. Furthermore, by incorporating the image chrominance information into FSIM, an IQA index for color images or gray scale image, denoted by FSIMC, will be obtained.

1st stage of the FSIM score is between PC_1 and PC_2 Given in eqn(5)

$$FSI_{PC}(y) = \left(\frac{2PC_1(y).PC_2(y)+T_1}{PC_1^2(y)+PC_2^2(y)+T_1}\right) \quad (5)$$

Where T_1 is a positive constant to increase the stability of FS_{PC}. In practice, T_1 can be determined based on the dynamic range of PC values.

2nd Stage of FSIM scoreeqn(6) is between gradient magnitude, GM_1 and GM_2 as

$$FSI_{GM}(y) = \left(\frac{2GM_1(y).GM_2(y)+T_2}{GM_1^2(y)+GM_2^2(y)+T_2}\right) \quad (6)$$

where T_2 is a positive constant depending on the dynamic range of GM values. In our experiments, both T_1 and T_2 will be fixed to all databases so that the proposed FSIM can be conveniently used.

Then, $FS_{PC}(y)$ and $FS_{GM}(y)$ are combined to get the similarity $FS_L(\mathbf{y})$ of $h_1(\mathbf{y})$ and $h_2(\mathbf{y})$. We define $FS_L(\mathbf{y})$ eqn (7) as

$$FSI_L(y) = [FSI_{PC}(y)]^{\alpha}.[FSI_{GM}(y)]^{\beta} \quad (7)$$

where α and β are parameters which are used to adjust the relative importance of Phase Congruency and Gradient Magnitude features. Here we set $\alpha = \beta = 1$ for simplicity. Thus explained in eqn(8)

$$FSI_L(y) = [FSI_{PC}(y)].[FSI_{GM}(y)] \quad (8)$$

V. IMPLEMENTATION

a. Fingerprint Biometric Authentication Via the Internet

One of the major problems with the authentication of users via the internet is the inherent lack of security of traditional authentication techniques, passwords PIN numbers and cookies. With the current development of the biometric fingerprint technology market, the possibility of identifying someone online has been addressed. Our fingerprint biometric authentication system is one of the solutions to come out of recent developments. The fingerprint biometric authentication system allows for a web page to include a validation check using objects embedded in the web page which call on an interface to a fingerprint reader attached to the client computer which returns a coded fingerprint to the server where it is then validated.

b. The Process

The process of fingerprint authentication over the web from the user's point of view is as follows:

1. The client uses his web browser to navigate to a page on the secured server. If they are not logged in they will be redirected to the Login Page. On the login page is an HTML form with fields that prompt for his user ID, and an area for the fingerprint display.

2. Once the client fills in his user ID, and, places his finger on the fingerprint reader. An image of the scanned fingerprint is displayed on the login page.

3. The user submits his login page to the server for biometric authentication of the fingerprint.

4. Once web server (Microsoft Internet Information Server - IIS) receives the login ID and encoded fingerprint data.

5. Internet Information Server passes on the user ID and fingerprint data to a server-side authentication application.

6.In the finger print authentication application fetches the user's fingerprint data, obtained previously during the fingerprint registration process, from a registration database (ODBC compliant data source) and compares it with the supplied fingerprint scan data from the login page.

7. The accept/not accept result, along with user-specific data (such as authorization level) in the event of a successful fingerprint login attempt, is passed back to the ASP script currently running in IIS.

8. Based on the result, the ASP script either redirects the user either to a page reporting the failed login attempt or to a page with the appropriate functionality for the user's authorization level as returned from the database.

9. The finger print feature extraction method and matching by FSIM algorithm is the final process that will take place in the server side to authenticate the biometric image.

VI. EXPERIMENTAL RESULTS AND DISCUSSIONS

Using the above design we train 40 images of 10 different people. Each person has 4 different image stored in database. The test database has 10 different untrained images which undergo the same algorithm as trained image and compare one to one with the original trained image.

Using the FSIM algorithm, we calculate the matching score between the test image and trained image. Depending on the best score, corresponding image from the trained database is selected. Table 1 show the accuracy of canny edge and pewit edge detection technique. Figure 2 explains the feature extraction of Canny and perwit edge detection techniques. Figure 3 explains the log Gabor output of the image which was explained in eqn(3).and figure 4 explains the matching score obtained by the canny and perwit FSIM algorithm respectively.

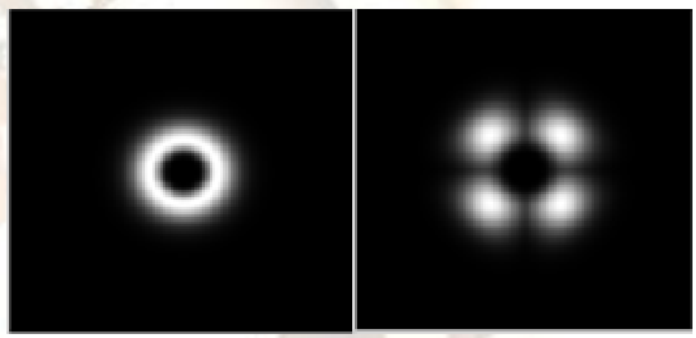
Table1: Accuracy measured.

No. of Train Image	No. of Test image	Recognition Accuracy	
		Canny Score %	Prewitt Score %
40	10	96.77	97.161
Conclusion		Good	Best

Relatedoutput image of the algorithm is as shown below

(i) (ii)

Fig 2. Feature Extraction.(i) Canny edge detection (ii) Perwit edge detection.



(i) (ii)

Fig 3.Log Gabor output
(i)Log-Gabor Filter, (ii) Log Gabor with Low pass-filter

(i) (ii)

Fig 4. Matched image using FSIM
(i)Canny FSIM matching.(ii)Perwit FSIM matching

VIII CONCLUSION:

In this paper, we proposed an Automatic finger print Matching using Feature-Similarity (FSIM) index matching and obtain optimum matching score. The experimental results achieve recognition accuracy using canny and perwitt FSIM of 96.77% and 97.16%, respectively, on the publicly available database of Hong Kong Polytechnic University. Experimental evaluation using palmprint image database clearly demonstrates the efficient recognition performance of the proposed algorithm using Perwit FSIM gives best result when compared with the Canny FSIM algorithm.

REFERENCES:

[1] Bergholm, F., 1987. “Edge focusing”. IEEE Trans. On Pattern Analyis and Machine Intelligence 9, 726–741.

[2] Canny, J., “A Computational Approach To Edge Detection”, IEEE Trans. Pattern Analysis and Machine Intelligence, 8(6):679–698, 1986.DOI: 10.1109/TPAMI.1986.4767851

[3] Petrou, M., Kittler, J., 1991. “Optimal edge detectors for ramp edges”. IEEE Trans. PAMI 13, 483–491.DOI:10.1109/34.134047

[4] Sarkar, S., Boyer, K.L., 1991. “On optimal infinite impulse response edge detection filters”. IEEE Trans.PAMI 13, 1154–1171. DOI:10.1109/34.273709

[5] Paul Bao, Lei Zhang, and Xiaolin Wu, “Canny Edge Detection Enhancement by Scale Multiplication”, IEEE transaction on Pattern analysis and machine intelligence, vol. 27, no. 9, sept 2005

[6] Daugman, J. G. (1988). “Complete discrete 2D Gabor transforms by neural networks for image-analysis and compression”. IEEE Transactions on Acoustics Speech and Signal Processing, 36, 1169–1179.

[7] Kong, W. K., Zhang, D., & Li, W. (2003). “Palmprint feature extraction using 2-D Gabor filters”. Pattern Recognition, 36, 2317–2339.

[8] Loris Nanni *, Alessandra Lumini. “Ensemble of multiple Palmprint representation”, Expert Systems with Applications 36 (2009) 4485–4490

[9] WangmengZuo, FengYue, DavidZhang, “on accurate orientation extraction and appropriate distance measure for low-resolution palmprint recognition”, Pattern Recognition 44 (2011) 964–972

[10] Lin Zhang, David Zhang, FSIM: “A Feature Similarity Index for Image Quality Assessment”, supported by the Hong Kong RGC General Research Fund (PolyU 5330/07E), the Ho Tung Fund (5-ZH25) and and NSFC 90920003

[11] P. Kovesi, “Image features from phase congruency”, Videre: J. Comp. Vis. Res., vol. 1, no. 3, pp. 1-26, 1999.

[12] R. Jain, R. Kasturi, and B.G. Schunck, Machine Vision. McGraw-Hill, Inc, 1995.

[13] R.Gayathri, R. and P. Ramamoorthy, 2012 “Automatic personal identification using feature similarity index matching”. Am. J. Applied Sci., 9: 678-685.DOI: 10.3844/ajassp.2012.678.685

[14] R.Gayathri, R. and P. Ramamoorthy, 2012 “Automatic Palmprint Identification based on High Order Zernike Moment”. Am. J. Applied Sci., 9: 759-765.

Biographical notes

H.Anandkumar Singh received B.E degree in Electronics and Communication Engineering from Visveswarya Technological University Mysore in the year 2005. Currently he is Pursuing M. Tech. degree in Embedded System from Vel Tech Dr.RR& Dr.SR Technical University, Chennai, India. His research interest includes application to image recognition, network security. He has published 2 papers in international Conferences.

R.Gayathri received B.E degree in Electronics and Communication Engineering from Madras UniversityChennai in the year 1999.She received M. Tech. degree in Laser and Electro Optical Engineering from Anna University, College of Engineering Guindy, Chennai India in the year 2001. she is currently pursuing the Ph.D. degree in the department of Electronics and Communication Engineering at Anna University College of Technology, Coimbatore, India. She is currently working as an Assistant Professor and Head in the Department of Electronics and Communication Engineering, Vel Tech Dr.RR& Dr.SR Technical University, Chennai, India. Her research interest includes pattern recognition, computer vision, machine learning, application to image recognition, network security. She has published more than 16 papers in international referred journals, National and International Conferences.