BIOMETRICS: ACCESS CONTROL AND AUTHORIZATION BASED ON FINGER-KNUCKLE PRINT IDENTIFICATION

Mr. SHIVARAJ SUBRAY HEGDE
The Oxford College of Engineering
Bangalore, India

Mrs. ARUNA. J
Asst. Professor
The Oxford College of Engineering
Bangalore, India

Mr. ANAND V BHAT
The CEO
BNB Security & Automation Solutions(P).Ltd

***Abstract*—Finger knuckle bending produces a highly unique texture pattern and it can be used as a distinctive biometric identifier. This paper presents an access control and authorization technique based on an emerging biometric identifier, namely finger knuckle-print (FKP), for personal identification.**

The image of the finger knuckle print is captured through reflected light by digital camera. Image captured is first enhanced to one extent and the ROI in the image selected by using the cordinate system. The ROI of the image is then used for the l1- Norm Sparse reconstruction. The reconstructed image is processed through an algorithm to extract the features set of the image. Different Edge detection algorithms are verified for the feature extraction. The feature extracted image is then used to form the finger knuckle print template for biometric authentication. The Correct Recognition Rate (CRR) and Equal Error Rate (EER) for the different fingers are calculated and the graph is plotted.

Keywords— Authentication, FKP, CRR, EER, feature extraction.

I. INTRODUCTION

The problem of providing security entails the protection of thereby ensuring that only authorized users are able to access the contents available inside. Content owners, such as authors and authorized distributors, are losing billions of dollars annually in revenue due to the illegal copying and sharing of digital media. In order to address this growing problem, digital rights management (DRM) systems are being deployed to regulate the duplication and dissemination of digital content. The critical component of a DRM system is user authentication which determines whether a certain individual is indeed authorized to access the content available in a particular digital medium. In a generic cryptographic system, the user authentication method is possession based. That is, the possession of the decrypting key is sufficient to establish the authenticity of the user. Since cryptographic keys are long and random (e.g., 128 bits for the advanced encryption standard (AES), they are difficult to memorize. As a result, these keys are stored somewhere (for example, on a computer or a smart card) and released based on some alternative authentication mechanism (e.g., password). Most passwords are so simple, that they can be easily guessed (especially based on social engineering methods) or broken by simple dictionary attacks. It is not surprising that the most commonly used password is the word "password." Thus, multimedia data protected by a cryptographic algorithm are only as secure as the password (weakest link) used to release the correct decrypting key(s) that can be used for establishing user authenticity. Simple passwords are easy to guess and, thus, compromise security; complex passwords are difficult to remember and, thus, are expensive to maintain. 1) Some users tend to "store" complex passwords at easily accessible locations. Furthermore, most people use the same password across different applications; an impostor upon determining a single password can now access multiple applications. Finally, in a multiuser account scenario, passwords are unable to provide non repudiation (i.e., when a password is divulged to a friend, it is impossible to determine who the actual user is: this may eliminate the feasibility of countermeasures such as holding conniving legitimate users accountable in a court of law).

Many of these limitations associated with the use of passwords can be ameliorated by the incorporation of better methods for user authentication. Biometric authentication or, simply biometrics refers to establishing identity based on the physical and behavioral characteristics (also known as traits or identifiers) of an individual such as face, fingerprint, hand geometry, iris, keystroke, signature, voice, etc.

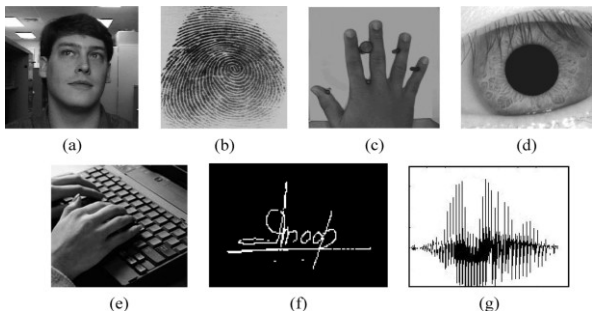

Fig. 1. Examples of biometric characteristics: (a) face, (b) fingerprint, (c) hand geometry, (d) iris, (e) keystroke, (f) signature, and (g) voice.

Biometric systems offer several advantages over traditional authentication schemes. They are inherently more

ISSN: 2278 – 7798

reliable than Password-based authentication as biometric traits cannot be lost or forgotten (passwords can be lost or forgotten); biometric traits are difficult to copy, share, and distribute (passwords can be announced in hacker websites); and they require the person being authenticated to be present at the time and point of authentication (conniving users can deny that they have shared the password). It is difficult to forge biometrics (it requires more time, money, experience, access privileges) and it is unlikely for a user to repudiate having accessed the digital content using biometrics. Thus, a biometrics-based authentication scheme is a powerful alternative to traditional authentication schemes.

II. LITERATURE SURVEY

The finger surface posses unique patterns that have been utilized in the personal identification. Woodard and Flynn (2005) [3] have examined the fine features of finger surface for its use in the biometric system. Authors have presented promising results by using curvature and a shape-based index from finger surface features extracted from finger images. For hand data collection the Minolta 900/910 sensor was used by author. However, the work detailed in [3] does not exploit the texture information that can be simultaneously extracted from the intensity images of hands. Ribaric and Fratric (2005) [4] employed appearance based features from the finger and palm surface images for personal identification. However, the authors in [4] have employed a scanner for imaging which is very slow and, hence, not suitable for online user authentication. S. Malassiotis (2006) combines finger geometry features and color information to authenticate user hands in the cluttered background. The finger shape information is generally believed to be less discriminative and only suitable for small-scale user identification [1]. Michael K.O. Goh and Connie Tee (2009) [5] employed a bimodal palm and knuckle print recognition system using inner surface of palm and finger knuckle. Authors presented a palm print and knuckle print tracking approach to automatically detect and capture these features from low resolution video stream. No constraint is imposed and the subject can place his/her hand naturally on top of the input sensor without touching any device. The palm print and knuckle print features are extracted using Wavelet Gabor Competitive Code and Ridget Transform methods. Several decision level fusion rules are used to consolidate the scores output by the palm print and knuckle print. The work, detailed in [4] and [5] is promising but it relies on crease and wrinkle details on the palm side (inner surface) of the fingers which are quite limited. Ajay Kumar and Ravikanth (2009) [1] investigates a new approach for personal authentication using finger back surface imaging. Author uses texture pattern produced by the finger knuckle bending for identification as it is highly unique and makes the surface a distinctive biometric identifier. Finger geometry features are also extracted from the same image at the same time and integrated to further improve the user identification accuracy of such a system.

Ajay Kumar, Yingbo Zhou (2009) investigate a new approach for efficient and effective personal identification using Knuckle Codes. The enhanced knuckle images are employed to generate Knuckle Codes using Localized Radon Transform that can efficiently characterize random curved lines and creases. The similarity between two Knuckle Codes is computed from the minimum matching distance that can account for the variations resulting from translation and positioning of fingers. Lin Zhang, Lei Zhang and David Zhang (2009) constructed data acquisition device to capture the Finger Knuckle Print images, and then an efficient FKP recognition algorithm is presented to process the acquired data .The local convex direction map of the FKP image is extracted based on which a coordinate system is defined to align the images and a Region of Interest (ROI) is cropped for feature extraction. A competitive coding scheme, which uses 2D Gabor filters to extract the image local orientation information, is employed to extract and represent the FKP features. To match two FKPs, they present a Band-Limited Phase-Only Correlation (BLPOC) based method to register the images and further to evaluate their similarity. An FKP database was established to examine the performance of the proposed system. Rui Zhao (2009) [7] presented an approach in which he uses single knuckle - print image to implement personal identification. Unlike most previous work, there is no need to collect a large amount of images to train the classifier. Michal Choras and R.Kazil (2010) evaluated texture-based knuckle features using IIT Delhi knuckle image database. G S Badrinath, Aditya Nigam and Phalguni Gupta (2011) [2] presented an Efficient Fingerknuckle- print based Recognition System Fusing SIFT (Scale Invariant Feature Transform) and SURF (Speeded up Robust Features) Matching Scores. Corresponding features of the enrolled and the query FKPs are matched using nearest-neighbour-ratio method and then the derived SIFT and SURF matching scores are fused using weighted sum rule. Lin Zhang, Lei Zhang, David Zhang, Hailong Zhu (2011) [8] proposed Ensemble of local and global information for finger–knuckle-print recognition. Shoichiro Aoyama, Koichi Ito and Takafumi Aoki (2011) [9] proposed Finger-Knuckle-Print (FKP) recognition algorithm using Band-Limited Phase-Only Correlation (BLPOC)-based local block matching. The phase information obtained from 2D Discrete Fourier Transform (DFT) of images contains important information of image representation. The phase-based image matching, especially BLPOC-based image matching is successfully applied to image recognition tasks for biometric authentication applications. Shubhangi Neware1, Dr. Kamal Mehta2 and Dr. A.S. Zadgaonkar proposed Finger Knuckle Surface Biometrics (2012) [10]by taking the image of whole finger and applying edge detection technique to that image

III. PROPOSED WORK

Figure below represents work flow diagram for proposed Access control and Authorization based on finger-knuckle print identification.

ISSN: 2278 – 7798

A. *Load Image*

The backside of finger is to be captured using digital camera. The captured image is then loaded initially to the identification system.

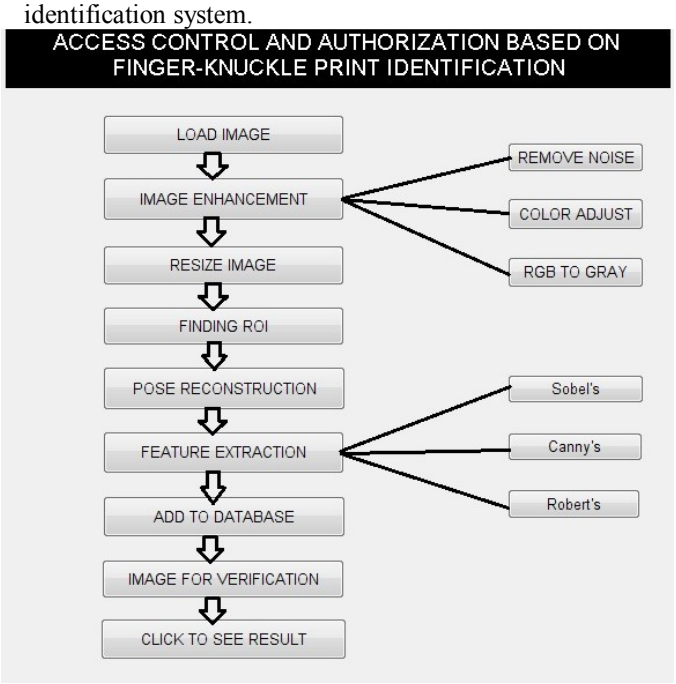

Fig.2 Flow Chart of Proposed Work

B. *Image Enhancement*

The finger surface is highly curved and results in uneven reflection which also generates shadow. The knuckle images therefore have low contrast and uneven illuminations. These undesirable effects are to be reduced using the image enhancement techniques.

Initially the noise in the image is removed by using image noise filter. The image is then used for adjustment of brightness and contrast. Resulting image is then converted in to gray scale image to extract exact features of the finger knuckle image.

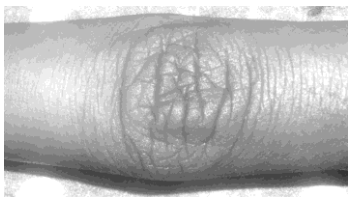

Fig.3 Enhanced FKP image

C. *Image Resize*

The enhanced image will be of large in size, since it is captured through digital camera. The processing of large images will not provide exact result and may take more time. Hence the image is resized according to the requirement.

D. *Finding ROI*

Each of these images requires localization of region of interest for the feature extraction. The region of interest is the region having maximum knuckle creases. It is necessary to construct a local coordinate system for each FKP image. With such a coordinate system, an ROI can be cropped from the original image for reliable feature extraction and matching.

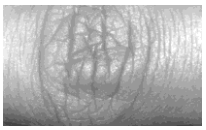

Fig.4 ROI in FKP

E. *Pose Reconstruction*

The verification scheme is simple and fast, and it leads to acceptable accuracy in FKP verification. If the query FKP image is well aligned after ROI extraction, the proposed scheme can work very well. As we discussed in the introduction section, however, there can be certain degree of variations of the finger pose in the data collection process, which lead to deformations in the FKP images and consequently result in false rejections because algorithm is sensitive to image deformations.

The FKP verification accuracy can be improved if we could correct the finger-pose-variation caused deformations of query samples via affine transformation. Unfortunately, it is a particularly difficult problem to estimate the affine transformation parameters for FKP images because very few distinctive key points can be extracted from them. Therefore, this solution is impractical. Here, I propose to reduce the pose variation caused false rejections by enhancing the matching process without pose deformation correction.

Reconstruction With l_1-Norm Sparse Regularization

By approximating Y with $X \cdot w$, one solution to w is the least square solution:

$$\hat{\boldsymbol{w}} = \arg\min_{\boldsymbol{w}} \|\boldsymbol{y} - \boldsymbol{X} \cdot \boldsymbol{w}\|_2^2$$

It is easy to see that

$$\hat{\boldsymbol{w}} = (\boldsymbol{X}^T \boldsymbol{X})^{-1} \boldsymbol{X}^T \boldsymbol{y}$$

Though the least square solution is simple to compute and it ensures the minimal $l2$-norm reconstruction residual of ŷ, it is not the best choice for the verification purpose. The least square solution aims to minimize the reconstruction residual, and the weights $\boldsymbol{w}$ tend to be densely distributed, hence many classes in $\boldsymbol{X}$ will contribute in reconstructing $\boldsymbol{y}$. Finally, some discriminative features in $\boldsymbol{y}$ may be smoothed out in ŷ.

In order to preserve the discriminative features of $\boldsymbol{y}$ in ŷ, some regularization term could be imposed on $\boldsymbol{w}$. Intuitively, we hope that only a small portion of the weights in $\boldsymbol{w}$ are significant so that only several classes are dominantly involved to reconstruct $\boldsymbol{y}$. The $l1$-norm based sparse representation (or sparse coding) is a very good choice to this

ISSN: 2278 – 7798

end. In recent years sparse coding has been successfully used in various image reconstruction and pattern classification applications. It represents a given signal as a sparse linear combination over a dictionary of atoms. By imposing the $l1$-norm constraint on $\boldsymbol{w}$, we have

$$\hat{\boldsymbol{w}} = \arg\min_{\boldsymbol{w}} \|\boldsymbol{y} - \boldsymbol{X} \cdot \boldsymbol{w}\|_2^2 + \lambda \|\boldsymbol{w}\|_1 \qquad (4)$$

where λ is a positive scalar balancing the reconstruction residual and the sparsity of $\boldsymbol{w}$. Eq. (4) can be solved by many convex optimization algorithms such as $l1$-magic, $l1$-*ls* , etc.

The sparse coding in Eq. (4) still has two problems. First, it is known that the commonly used $l1$-minimization solvers such as $l1$-*ls* have an empirical complexity of $O(z^2k^{1.3})$, where z is the dimension of $\boldsymbol{y}$ and k is the number of samples in $\boldsymbol{X}$. In practice, k can be very big so that the sparse coding complexity is high. Second, the atoms in $\boldsymbol{X}$ are the original gallery FKP images, which may contain noise and some trivial structures that can be negative to the representation of $\boldsymbol{y}$.

A random FKP image dictionary D has to be created for the reconstruction of the image. Once the dictionary $\boldsymbol{D}$, which has less number of atoms than $\boldsymbol{X}$, is computed, we use it to code the input FKP image $\boldsymbol{y}$ as follows:

$$\hat{\boldsymbol{w}} = \arg\min_{\boldsymbol{w}} \|\boldsymbol{y} - \boldsymbol{D} \cdot \boldsymbol{w}\|_2^2 + \lambda \|\boldsymbol{w}\|_1$$

Finally, the image is reconstructed as:

$$\hat{\boldsymbol{y}} = \boldsymbol{D} \cdot \hat{\boldsymbol{w}}$$

F. *Feature Extraction*

Knuckle images have strong vertical edges that can be useful for recognition purposes. Proposed transformation calculates ELBP (Edge based local binary pattern) for each pixel in the image. A knuckle print image is transformed into an edge code that is robust to illumination and local non-rigid distortions. Knuckle print image is preprocessed by applying the Canny's edge operator in horizontal direction to obtain vertical edge map which is used to obtain the edge code. ELBP value for every pixel $A_{j;k}$ in the vertical edge map is defined as a 8 bit binary number S whose i^{th} bit is defined as:

$$S_i = \begin{cases} 0 \; if \; Neigh[i] < threshold \\ 1 \; else \end{cases}$$

Where Neigh[i]; i = 1; 2; :::8 are the horizontal gradient of 8 neighboring pixels centered at pixel $A_{j;k}$. The value of threshold is evaluated experimentally. In edge code every pixel is represented by its BLBP value which is an encoding of strong edge pixels in its 8-neighborhood. The key observation point here is that any change caused due to sudden change in the illumination will affect the gray values but BLBP value is not affected much because the strong edge pattern near the pixel remains to be more or less same. This property can be exploited over knuckle print database as it contains lot of illumination variation.

Extracted features will be used for matching edge codes which is being done using tracking. Tracking unidentified objects requires robust, uniquely and visually significant feature points, at-least within a specified neighborhood so as to track them successfully.

Fig.5 Canny's Edge detection of FKP image

Strong derivative points cannot be considered as features because they look like the same along the edge. Corners contain enough information so as to be tracked successfully as they have strong derivatives in two orthogonal directions. The autocorrelation matrix M is used to calculate good features having strong orthogonal derivatives. Matrix M can be defined for any pixel P at i^{th} row and j^{th} column as:

$$M(i,j) = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

such that

$$A = \sum_{-K \le a,b \le K} w(a,b).I_x^2(i+a, j+b)$$

$$B = \sum_{-K \le a,b \le K} w(a,b).I_x(i+a, j+b).I_y(i+a, j+b)$$

$$C = \sum_{-K \le a,b \le K} w(a,b).I_y(i+a, j+b).I_x(i+a, j+b)$$

$$D = \sum_{-K \le a,b \le K} w(a,b).I_y^2(i+a, j+b)$$

Where w (a,b) is the weight given to the neighborhood, $I_x(P)$ and $I_y(P)$ are the partial derivatives sampled within the window defined by w and centered at pixel P. The matrix M defined above can have two eigen vector ∧ 1 and ∧ 2 such that ∧ 1 ≥ ∧ 2 with e1 and e2 as the corresponding eigenvectors. Shi and Tomasi [11] have suggested considering pixels having ∧ 2 ≥T (smaller Eigen vector greater than a threshold) as good corner feature points that are unique, visually significant and can be tracked successfully.

G. *Adding to Database or Creating Database*

For the verification of the users, The FKP database has to be created. The feature extracted image is used for creating database. During the identification process the user FKP image is matched with the database FKP images.

H. *Image Selection for Verification*

In order to authenticate the user, the FKP image of the user has to be loaded first and its feature should be extracted. The feture extracted image is then matched with the database.

- ***Matching***

Let A and B be two knuckle print images that are to be compared. Let a and b be the 2-tuple arrays

ISSN: 2278 – 7798

containing the corner information of knuckle print images A and B respectively. In order to make the decision on matching between A and B, LK Tracking, discussed in Section 2, has been used to determine the average number of features tracked successfully in one knuckle print image against all corner points of another image. Let a(i; j) be a corner point of knuckle print image A. LK Tracking calculates its estimated location in edge code of B, say edge code B(k; l). For every a(i; j) of a, we tell that a pixel a(i; j) is tracked successfully if the euclidean distance between a(i; j) and edge codeB(k; l) is less than or equal to a pre assigned threshold, TH_d and the sum of the absolute difference between every neighboring pixel of a(i; j) and edge code B(k; l), termed as tracking error, is less than or equal to a pre assigned threshold, THe. Thus, we can define Tracked(a(i,j), edgecodeB) for successful / unsuccessful tracking as,

$$Tracked(a(i,j), edgecode_B) = \begin{cases} 1 \textbf{ if } ||a(i,j), b(k,l)|| \leq TH_d \\ \quad \textbf{and } T_{Error} \leq TH_e \\ 0 \textbf{ otherwise} \end{cases}$$

Where, T_{Error} is the tracking error. For every point in a, one can determine whether it can successfully tracks a pixel in edgecodeB. Features Tracked Successfully (fts) for *a* to edgecodeB can be defined by

$$fts(a, edgecode_B) = \sum_{\forall a(i,j) \in a} Tracked(a(i,j), edgecode_B))$$

Thus, the average number of features tracked successfully (FTS) for a to edgecodeB and *b* to edgecodeA is defined by

$$FTS(A,B) = \frac{1}{2} \times [fts(a, edgecode_B) + fts(b, edgecode_A)]$$

I. Click to See Result

The result of the matching is displayed finally at the end of the verification process.

IV. EXPERIMENTAL RESULTS

This section analyses the performance of the proposed system. Performance of the system is measured using correct recognition rate (CRR) in case of identification and equal error rate (EER) for verification. CRR of the system is defined by

CRR =N1/N2

Where, N1 denotes the number of correct (Non-False) top best match of FKP images and N2 is the total number of FKP images in the query set.

At a given threshold, the probability of accepting the impostor, known as false acceptance rate (FAR) and probability of rejecting the genuine user known as false rejection rate (FRR) are obtained. Equal error rate (EER) is the value of FAR for which FAR and FRR are equal.

EER = {FAR | FAR = FRR}

In the proposed system the CRR and EER for the different fingers are calculated and concluded that the left hand finger knuckle print is efficient for the verification process.

Performance Analysis

CRR for Left Index	CRR for Left Middle	CRR for Right Index	CRR for Right Middle
0.9910	0.9926	0.9936	0.9922

Table 1 : Identification Performance

For each finger, Receiver Operating Characteristics *(ROC) curves which plots FAR against FRR is shown in Fig. below.*

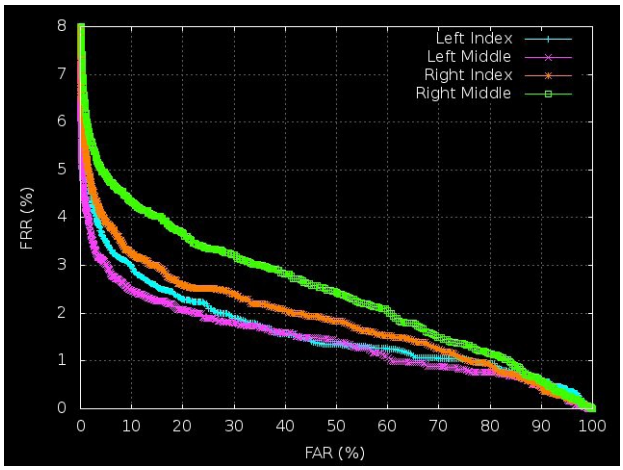

Fig. 6 Finger wise ROC Curves

V. CONCLUSION

This paper presents the secure biometric access control and authentication based on FKP identification. Different edge detection methods are tested with the same FKP image and concluded that the Canny's edge detection will be the efficient edge detection algorithm. The different finger knuckle prints are collected as database and estimated the CRR and EER for collected fingers. The proposed FKP

ISSN: 2278 – 7798

based identification is having several advantages over the other biometric traits like finger print, face recognition, etc. The important advantages are (1) rich in texture features, (2) easily accessible, (3) invariant to emotions and other behavioral aspects such as tiredness, (4) stable features and acceptability in the society.

REFERENCES

[1] Kumar A and Ravikanth C, ―Personal authentication using finger knuckle surface‖ , IEEE Transactions on Information Forensics and Security, 4(1):98 –110, 2009.

[2] Badrinath G S, Nigam A. and Gupta P, ―An Efficient Finger knuckle-print based Recognition System Fusing SIFT and SURF Matching Scores‖ , Information and communication Security, pp374- 387,2011.

[3] Woodard D.L., Flynn P.J., ―Finger surface as a biometric identifier‖ , *CVIU,* vol. 100, pp. 357–384, 2005.

[4] Ribaric S, Fratric I., ―An online biometric authentication system based on eigenfingers and finger-geometry‖ , presented at the 13th Eur. Signal Processing Conf., Antalya, Turkey, Sep 2005.

[5] Michael K.O, Connie T, Andrew B.J., ―Bimodal Palm print and Knuckle print Recognition system‖ , Journal of IT in Asia, Vol 3,2010.

[6] Zhang L, Zhang L, Zhang D, Zhu H, ―Online finger-knuckle-print verification for personal authentication‖ ,Pattern Recognition, 43(7):2560–2571, Elsevier, July 2010.

[7] Zhao R,‖ A Novel Approach of Personal Identification Based on Single Knuckleprint Image‖ , Asia-Pacific Conference on Information Processing18-19 July 2009.

[8] Zhang L, Zhang L, Zhang D, Zhu H,―Ensemble of local and global information for finger-knuckle-print recognition‖ , Pattern Recognition, 44(9):1990 – 1998, 2011.

[9] Shoichiro A, Koichi I, Takafumi A, ―Finger-Knuckle-Print Recognition Using BLPOC-Based Local Block Matching‖ , IEEE, 2011.

[10] Shubhangi Neware, Dr. Kamal Mehta, Dr. A.S. Zadgaonkar, "Finger Knuckle Surface Biometrics" www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 2, Issue 12, December 2012)

[11] Shi, J., Tomasi: Good features to track. In: Computer Vision and Pattern Recognition, 1994. Proceedings CVPR '94., 1994 IEEE Computer Society Conference on. (1994) 593–600

[12] D.L. Woodard, P.J. Flynn, "Finger surface as a biometric identifier",Computer Vision and Image Understanding 100 (3) (2005) 357–384.

[13] D.L. Woodard, P.J. Flynn, "Personal identification utilizing finger surface features", in: Proceedings of CVPR'05,vol. 2, 2005, pp. 1030-1036.

[14] C. Ravikanth, A. Kumar, "Biometric authentication using finger-back surface", in: Proceedings of CVPR'07, 2007, pp. 1-6.

[15] A. Kumar, C. Ravikanth, "Personal authentication using finger knuckle surface", IEEE Trans. Information Forensics and Security 4 (1)(2009)98-1

[16] Zhang L, Zhang L, Zhang D, ―Finger-Knuckle Print: A New Biometric Identifier‖ , Image Processing ICIP, IEEE International Conference, pp1981-84, Nov2009.

[17] Kumar A, Zhou Y, ―Personal Identification using Finger Knuckle Orientation Features‖ , Electronics Letters ,vol. 45, no. 20, September 2009.

[18] Kumar A, Ch Ravikanth, ―Biometric Authentication Using Finger Back Surface‖ , Computer Vision and Pattern Recognition, IEEE Conference, pp1-6, June2007.

[19] Zhang L, Zhang L, Zhang D, ―Finger-Knuckle-Print Verification Based on Band-Limited Phase-Only Correlation‖ , Proceedings of the 13th International Conference on Computer Analysis of Images and Patterns, pp. 141-148,Springer, 2009.

[20] Jain A, Kumar A, ―Biometrics of Next Generation: An Overview‖ , Second Generation Biometrics, Springer, 2010.

[21] Rui Z, Tao L, Shunyan H, Jianying S, ― A Novel Approach of Personal Identification Based on the Fusion of Multi finger Knuckle prints‖ , Advances in information Sciences and Service Sciences(AISS) Volume3, Number10,November 2011.

[22] Kanta Ratha N, Bolle R, ―Automatic Fingerprint Recognition System‖ , Springer, pp17-18.

[23] Gupta P, Rattani A, Mehrotra H, Kaushik A,―Multimodal biometrics system for efficient human Recognition‖ , Biometric Technique for human Identification III, Proceedings of SPIE,Apr.2006.

[24] Kumar A and Zhou Y, ―Human identification using knuckle codes‖ , Proceedings BTAS, Washington, 2009.

[25] Choras M, Kazil R, ―Knuckle Biometrics Based on Texture Features‖ , International Workshop on Emerging Techniques and Challenges for Hand-Based Biometrics (ETCHB), IEEE, 2010.

ISSN: 2278 – 7798