Generic Biometric Footprint Recognition Framework for Personal Security

Kapil Kumar Nagwanshi[1], Sipi Dubey[2] and Toran Verma[3]

[1,2,3] **Deptt. of CSE, Rungta College of Engineering and Technology,
Bhilai, CG 490024, India**

Abstract

The present paper introduces a matcher framework for footprint based biometric system. Extensive literature survey concerning traditional techniques for access control and latest biometrics technique observed and proved the significance of a footprint based recognition system. The problem has been identified based on the gap. The standard algorithm for enrolment authentication and identification has proposed in the methodology section. The paper defines a generic framework for footprint biometric system. Pre-processing phase normalized the images for further processing. For feature extraction fuzzy logic and neural network, the technique has anticipated in feature set generation Phase. The matching and decision module tries to meet almost all trade-offs between biometric systems. The error rate is also being expected to reduce to level ±1 %.

Keywords: *Gait, Matcher, Footprint, Fuzzy Logic, Neural Networks, Centre of pressure (COP).*

1. Introduction

According to Ref. [1], biometrics authentication denotes the identification of humans by their physiognomies or traits. The signal processing domain employed footprint biometrics as a system of access control and identification of individuals. Biometric is referring to the employment of the mathematical model and statistical analysis to biological sciences [2]. A biometric trait commonly stored as feature vectors or templates recognizes users. These unique features make a person identifiable using a diversified set of biometric traits such as eyes, fingerprints, gait, ear, palm prints, speech, retina, and footprints. The unimodal technique uses only one biometric trait such as a footprint for personal identification. While multimodal personal identification system uses more than one sensor such as one for signature and other for retinal image capturing, might be used in this process (if a single source does not provide sufficient recognition rate) [3, 4, 1]. The term *identification*, *recognition*, and *verification* have been adopted from literature presented by Ref. [5] and Ref. [3]. They represent recognition as the integration of (i) the one-to-one relationship with a requested template defines verification and, (ii) identification is a procedure of one-to-many comparisons to find a match in the template dataset if it exists. According to Ref. [6, 7] the complete biometric system is struggling for (refer Fig. 1) *universality*, *uniqueness*, *permanence*, *measurability* or *collectability*, *performance*, *acceptability*, and *circumvention*. None of the biometric systems from physiological to behavioral or from unimodal to multimodal can satisfy all the trade-offs [8].

2. Traditional Techniques for Access Control

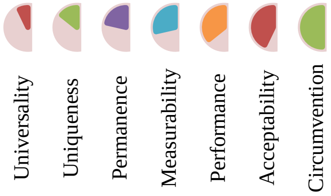

Fig. 1 - Trade-offs between biometric systems

The access control based biometric systems is divided into (i) knowledge-based methods such as textual passwords, or personal identification number and (ii) the internet community has widely used the token-based approach, for example driving license, passport number and so forth. It is effortless for an impostor to copy one's signature based on the password, PIN, driving license and so fort under theaccess control leads to the necessity of a unique identification method to cope up with such vulnerability of knowledge-based and token-based access control system. Biometric patterns are unique and reliable to individuals in authenticating identity than the conventional token and knowledge-based profiles. Nonetheless, the assortment of biometric traits improves privacy concerns about the use of this evidence [9][10].

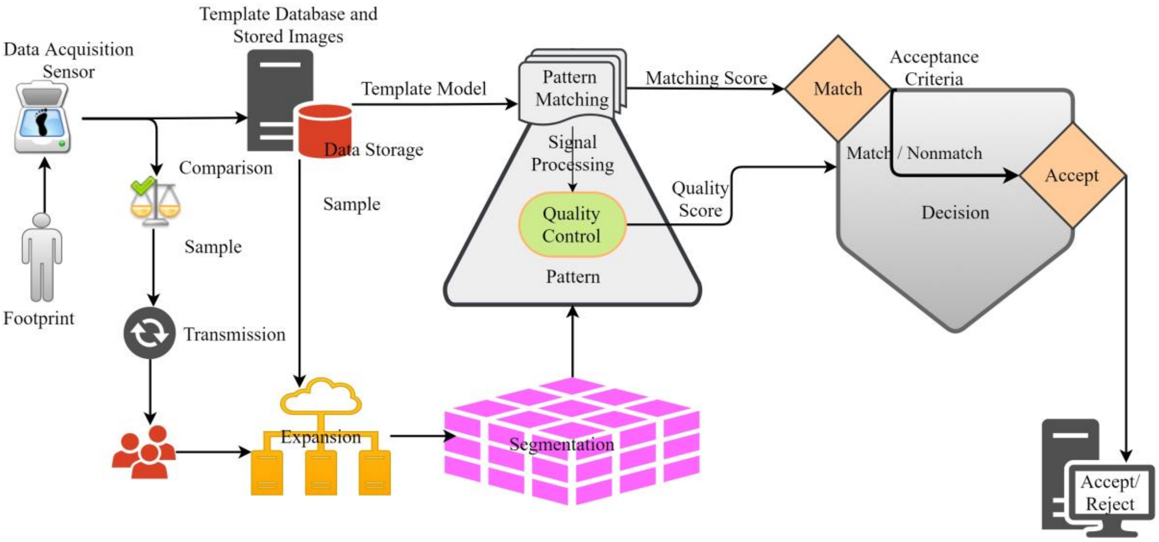

Fig. 2 Generic framework for footprint biometric system

2. Biometrics

The archaeological artifacts illustrate a way of authenticating person with the help of fingerprint carvings since 8000 BC [3]. Clay seals commonly used in 200 BC among officials during the Han Dynasty in China [11]. Laws of Yung-Hwui specified the use of fingerprints to sign divorce matters in 600 AD. "The Story of the River Bank" written by Shi-Naingan, describes the use of fingerprints for a solving a murder mystery in 1160 AD. Grew [12], studied and explained the science of ridges, furrows, and pores of hands and feet of a human for identification. Malpighi [13] introduced to the irregular ridges and patterns of human fingerprints and footprints. Purkinje [14] creates a system in the fingerprint classification (still in use) includes nine fingerprint pattern, two loops, one arch, one tent, and five types of the whorl. India has the first country officially adopted and recorded fingerprint for person identification. International Association for Identification was formed in 1916 to share biometric-based innovations. Locard [15] recognized the first rules for the minimum number of ridges that must be in accord before a fingerprint match might be declared. The first Automated Fingerprint Identification system is commonly known as AFIS became operational in 1984 [11, 4].

4. Problem Identification

Robbins [16] has examined the uniqueness of human footprint (and foot) morphology significantly and provided comprehensive information on several physical aspects of the people who made them was retrieved. The shape, or form, of an individual's foot, can identify uniquely come as no surprise to the anthropologists. Many automated biometrics-features have originated after 1977 such as fingerprint, eye-based biometric, face and facial expressions, ear and thermal ear images, voice and speech synthesis, gait, foot, shoe, foot boundary, palm prints, palm veins and so forth for identification and verification of on individual [17]. Footprint based system use pressure mat sensor or scanning sensor for the human footprint to recognize a person. It is a widespread practice in Japan to identify an infant by its footprints, hence they took the footprint traditionally by inkpad or now by scanning [18].

A human being has a tremendous legal capacity in Austria and some other countries such that one cannot ignore the role of biometric in society. India also uses the biometric fingerprint based passports to overcome from identity theft. Travelling by air is also very common; hence terrorists can take advantage of such a vulnerable system present in railway, or bus stations or any such crowd places to harm the properties of the country. To ensure the security of such stated places, we must have a profligate system which is capable of identifying the people rapidly. Despite the accomplishment of monetary transactions, the overpass of international borders and many more inhabitant solicitations, they are liable for personal identification, which might be unavoidable. An old token-based method such as non-biometric passport, credit cards, and so forth and knowledge-based ID like the PIN, passwords (are vulnerable to track using brute force attack) does not intrinsically imply the legal capacities. One may not be competent to at a guess, the person involved in the transaction is genuine or imposter; on the other side, the designated system is struggling with the non-repudiation problems of information and personal security. [19, 20]. Biometry facilitates personal identification in several ways [3, 21] not less than: (i) *Permanence* is the preservance of biometric pattern life-long and not need to remember like passwords; (ii) *Singularity* is the uniquness of biometric traits of each person; and (iii) *Efficiency* and user convenience because of last two reasons.

No biometric system fulfils all the features of biometric trade-offs. Present work inspects footprint biometrics as a novel developing substitute of access control in public domain includes airports, temples, religion places, research laboratories, public health domains, spas or thermal bath centres, and resembles its performance to the other biometric fields [22, 11]. Since it is expected to imply footprints in future for a highest security application domain including highest recognition rate without the need for additional hardware like airports, and banking, and so forth.

2. Materials and Method

The first method which is based on a simple calculation of Euclidean distance [17] in which Person identification has been made among ten men using normalized static footprint captured in stand-up posture. Recognition rate is 85% which is in turn not adequate for concrete uses. Subsequently, Jung et al. [23, 24] developed a method based on Hidden Markov Model captured footprints from five subjects for the position- based quantization of COP(Centre of Pressure) in ref. [25] using the shoe-type pressure sensor. Acquired data is highly correlated as it has collected in a day's span and the RR obtained is therefore, 100%. Fortunately, this is great to have such an outstanding recognition rate, but one cannot ignore very less subject has taken into account. Quantized COP trajectory, and HMM’s for two footprints combined with Levenberg-Marquart learning method gives a rate of recognition at 64% and is not equally distributed and not high enough. Comprehensive Evaluation Model comes into existence with 92% recognition rate for establishing to recognize toe shape by NNFL. Neural network and fuzzy logic have been exploited in this method by Jang [26]. The major problem with this approach is the comprehensive vector is based on a single factor. Therefore, it becomes a tedious process for significant data.

Several approaches evaluated during last decade includes: (i) Self-organizing map [27] for automation of process, (ii) ART2 [28] for optimization of footprint recognition, (iii) trace transform technique for parallel line [29], (iv) UbiFloor2 [30] using neural network and PCA [25] with a large extent of optimization, and (v) wavelet transform [31, 32] based footprint recognition.

Designing biometric systems is a challenging task leads to decide which comparison mode for verification and identification needs to use for an efficient outcome. The second challenge is to incorporate the exploitation of operational mode viz. automatic or semiautomatic. The third challenging task is to select the number of modalities by the need of the application and hardware for sensing these patterns [31, 32]. Designing footprint-based biometric systems require different formulation due to target is the foot. Wayman [33] has described a way of target application formulation method which helps to justify the selection of precise features include: "(i) cooperative vs. non-cooperative, (ii) overt vs. covert, (iii) habituated vs. non-habituated, (iii) attended vs. non-attended, (iii) standard vs. non-standard, (iv) public vs. private, and (v) open vs. closed". A footprint-based identification system may apply in the covert mode for secrecy of application in airports it can use as the non-habituated and overt mode [6, 34, 21, 35] . Wild [4, 5] had identified target application domains on the basis of (i) avoiding the low throughput by adopting promising environment, i.e., subjects walking barefoot; (ii) inhibiting unhygienic recording stipulations; (iii) uses larger sensor size for capturing footprint; and (iv) privacy concerns based on users interest.

From the previous discussion, it is apparent that we have to implement an efficient algorithm for footprint recognition. Based on a compilation of the available literature the generic system suitable for footprint biometric system has divided into five subsystems as shown in Fig. 2. The system constitutes of (i) data collection subsystem which records the footprint image via a sensor; (ii) acquired data is transmitted through transmission module to the data storage and signal processing module; (iii) images and template of the user is stored in data storage module; (iv) signal processing module performs feature extraction pattern matching operations; and (v) identification or verification by using the match scores performed in decision systems module.

Present approach proposes three algorithms each of which is for enrollment, authentication, and identification respectively. These algorithms are described below as Algorithm 1 for Enrollment; Algorithm 2 is developed for Authentication and finally Algorithm 3 for Identification. These algorithmic framework further guides to create new approaches based on soft-computing and GPU computing based technique [10]. In the obtained algorithms combination of techniques has been applied separately for image segmentation subsequently image restoration has also to be exploited for good result [36].

Algorithm 1: Enrolment

```
1. Acquire the footprint from acquisition subsystem.
2. Based on acquired data prepare template.
3. Store obtained template into the database.
```

Algorithm 2: Authentication

```
1. Acquire the footprint image from acquisition subsystem.
2. Based on acquired data prepare template.
3. Check template.
    a. if (match(stored, obtained)==true)
            then write match→(Accept)
    b. else
            write non match→(Reject)
```

Algorithm 3: Identification

```
1. Acquire the data from acquisition subsystem.
2. Based on acquired data prepare template.
3. Check template.
    a. if (match(stored, obtained)==true)
            then write match→(Accept)
    b. else
            write non match→(Reject)
4. Identify according to matching score.
```

5.1 Structure of Image Acquisition Phase

A core property of sensor determines matching performance of a biometric system. What should be captured is the fundamental question. To capture 2D image of the human foot print there are two possible choices: (a) volar or planter scans referring to the soleprint and (b) dorsal scans are pointing to images of the upper part of the foot. Many biometric systems provide personal verification based on foot images, which rely on diverse views of the foot and various kinds of sensors. Another critical entity is to distinguish between a natural and fabricated footprint image by a sensor (genuine vs.impostor attack). Choice of the sensor for a system which is susceptible to regular imposter attacks supports aliveness detection [5, 21]. This is difficult to deceive thermal sensors than the optical sensors sometimes even an ink print is sufficient. Security abilities, such as possible encryption for decentralized data acquisition and compression influence the selection of a dedicated sensor [3]. Another important consideration is foot size based on which sensor size has also been determined, and it is depicted in Fig. 3 which shows the distribution of foot size geometry and corresponding foot length. In this work, no specialized biometric sensor has been utilized. Simple flatbed scanner is used while considering cost effectiveness and ease of use. This sensor is denoted by $\varphi(X,Y)$, where $X \: and \: Y$ is the dimension of sensor. The acquired image is thus a function of sensory image as provided in eq.(1):

$$\alpha(x,y) = f(\varphi(X,Y),\rho) \tag{1}$$

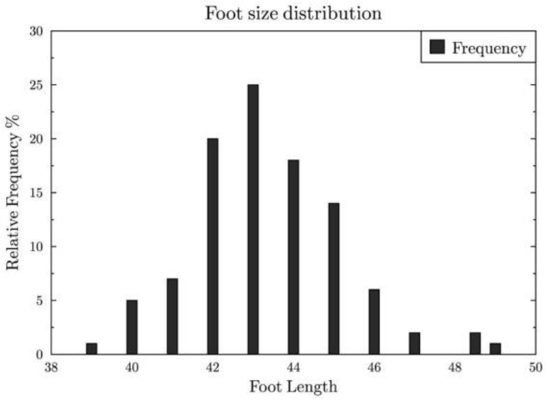

Fig. 3 Foot size distribution

where $\alpha(x,y)$ is an acquired image through sensor $\varphi(X,Y)$ passes through a function $f(.)$ with a threshold ρ.

5.2 Pre-processing Phase

The preprocessing is a very critical phase. The ability to normalize different rotations of footprint is at the core of the pre-processing and this process can increase recognition accuracy enormously. The acquired footprint $\alpha(x,y)$ then cropped into $\alpha_L(x,y)$ for left foot and $\alpha_R(x,y)$ for right foot. The obtained images subsequently rotated to a customary angle so that the footprint becomes normalized, this has been given in eq. (2) and eq. (3) with a rotation of $\theta \: and \: \emptyset \: degree$ for left and right foot respectively.

$$L(x,y) = \omega(\alpha_L(x,y),\theta) \tag{2}$$

$$R(x,y) = \omega(\alpha_R(x,y),\emptyset) \tag{3}$$

5.3 Feature Set Generation Phase

From the normalized image of the left and right foot, feature set has been extracted. Some of the identified feature-set are defined as follow: (i) Silhouette: = {contour distance to foot centroid, length and enclosed area of silhouette polygon}; (ii) Shape :={ 15 local foot widths and positions}; (iii) Toe-length: ={5×3 length of the nearest, intermediate and farthest points, 5×2 average finger widths, 5 toe lengths and 4 inter-toe angles}; (v) Soleprint: = {variance of 288 overlapping blocks in edge-detected image (similar to [37])}; (vi) Eigen-feet: ={ projection of sub-sampled footprint onto feature space spanned by 20 most significant principal components}; and (vii) Minutiae: = { on collected footprint data as using NIST mindtct minutiae extractor on ball-print region under big toe [2] }. For large scale identification out of m subjects, the approximation $FAR(m) \cong m.FAR$ holds [20, 9], Let S be a biometric sample within the universe of discourse X, a feature extractor is a function $E : X \rightarrow F$ which maps each sample S to its feature vector representation $x \in F$ within the feature space F. Where $E_1, E_2, \ldots, E_i, ..$ denote different feature extractors such as lightning, Gaussian curvatures etc.

5.4 Matching and Decision module

Present approach examined three different matchers vis-à-vis False Acceptance Rate (FAR) and False Rejection Rate (FRR) for the identification task. Let r and n be the two feature vectors where $r \in F, and\ n \in F\ .OR.\ n \notin F$. A matcher is a function $\zeta: F \times F \rightarrow \mathbb{R}$ returning a similarity score $\zeta(r, n)$. Different matchers can be denoted by $S_1, S_2, \ldots S_3 \in S$. the complete module of decision and verification has been demarcated by definition 1,2,3, and 4 as follows:

According to [5], the biometric system might be run on either of the two approaches, i.e. (i) identification and (ii) verification.

Definition 1: One-to-one comparison of the acquired biometric sample to the associated referred identity template in the database using threshold η is defined as verification

Definition 2: For a Given biometric sample $S \in X$ (Ref. subsection 5.3) and a claimed identity $i \in \{1, \ldots, m\}$, a verification system is a function $V : X \times M \rightarrow \{1,0\}$ determining in eq. (4) whether the claim is true or false it will return 1 for genuine and 0 for imposter based on threshold value η defines a verification system.

$$V := \begin{cases} 1 & if\ \zeta(E(S), i_i) \geq \eta\ \mid genuine \\ 0 & otherwise \mid imposter \end{cases} \quad (4)$$

Definition 3: Acquired biometric data sample K which is none of any stored sample S is related in one to many with all template data i_i until a suitable match found defines identification.

Definition 4: For a given biometric sample $S \in X$ identification system is a function I which is defined by $I: X \rightarrow M \cup \{reject\}$ determining the identity $m_i, i \in \{1, \ldots, m\}$ can be determined by eq. (5),

$$I(S) := \begin{cases} m_i,\ \ if\ i\ = \arg_j \max\{\zeta(E(M), i_j)\} \land \zeta(E(M), i_i) \geq \eta; \\ \\ reject, & otherwise \end{cases} \quad (5)$$

constitutes the identification system

6 Result and Discussion

The references discussed shows to meet all the tradeoffs in any biometric system is almost impractical. Fuzzy logic and the neural network have been exploited for recognition with anticipated promising recognition rate. Seven feature sets and four definitions for the system defines footprint biometric. From the complete set of debate footprint based biometric proves its significance in a variety of application where access control is required. This system is expected to have a minimum error (based on developed hypothesis [10]) and faster recognition rate.

Conclusion

The present paper introduced an approach for footprint recognition leads to the design of the generic footprint biometric framework. Other biometric features have also taken into account for support of the enrolment, authentication, and identification algorithms. Because the footprint-based research and its employment are still in developing stage and in coming years, it would be expected the full-featured biometric footprint system in operational form. As the challenges in security demands more on the biometric trait, footprint proves its emphasis on real-time application.

Acknowledgments

The authors would also like to thank Dr. S. P. Dubey from Rungta College of Engineering and Technology, Bhilai, India, who provided insight and expertise that greatly assisted the research, although they may not agree with all the interpretations/conclusions from this paper. The authors are also immensely grateful to our management Dr. Sourabh Rungta and Mr. Sonal Rungta for their kind support..

References

[1] A. A. Ross and A. K. Jain., " Information fusion in biometrics," *Pattern Recognition Letters,* vol. 24, pp. 2115-2125, 2003.

[2] Online, "NSTC," 14 September 2006. [Online]. Available: http://www.biometrics.gov/Documents/Glossary.pdf..

[3] D. Maltoni, D. Maio, A. K. Jain and S. Prabhakar, Handbook of Fingerprint Recognition, New York USA: Springer, 2003.

[4] P. Wild, "Single-sensor hand and footprint-based multimodal biometric recognition," Naturwissenschaftlichen Fakultät der Universität Salzburg, Salzburg,, January 2008.

[5] R. M. Bolle, J. H. Connell, S. Pankanti, N. K. Ratha and A. W. Senior., Guide to Biometrics, Springer, New York, NY, USA, 2004.

[6] A. K. Jain, S. Pankanti, S. Prabhakar, L. Hong, A. Ross and J. L. Wayman, "Biometrics: A Grand Challenge," in *17th International Conference on Pattern Recognition (ICPR),* Cambridge, UK, 2004.

[7] A. Jain, R. Bolle and S. Pankanti, Biometrics: Personal Identification in Networked Society, Kluwer Academic Publications, 1999.

[8] K. K. Nagwanshi and S. Dubey, "Statistical Feature Analysis of Human Footprint for Personal Identification Using BigML and IBM Watson Analytics," *Arab J Sci Eng,* pp. 1-10, 2017.

[9] A. K. Jain, L. Hong and S. Pankanti, "Biometric Identification," *Communications of the ACM,* vol. 43, no. 2, pp. 91-98, 2000.

[10] K. K. Nagwanshi and S. Dubey, "Biometric Authentication using Human Footprint," *International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868,* vol. 3, no. 7, pp. 1-6, Aug 2012.

[11] A. Farelo and A. Wrzeczycki, "A history of fingerprints," INTERPOL, Lyon, France, Apr 2009.

[12] N. Grew, "The Description and Use of the Pores in the Skin of the Hands and Feet," *Phil. Trans. R. Soc.,* vol. 14, pp. 566-567, Jan 1684.

[13] M. Malpighi, De externo tactus organo anatomica observatio, etc, Naples Austria: Longus, 1665.

[14] J. E. Purkynje, "Commentatio de examine physiologico organi wisus (Habilitatio inauguralis)," Dr. W. Junk, Vratislaviae, 1823.

[15] E. Locard, Treaty of Forensic Science-T. I and II Footprints and traces in the criminal investigation. T. III and IV Proofs of Identity, Vols. I-VII, Lyon, 1931.

[16] L. M. Robbins, "The Individuality of Human Footprints," in *39th Annual Meeting of the American Academy of Forensic Sciences*, St. Louis,, 1978.

[17] K. Nakajima, Y. Mizukami, K. Tanaka and T. Tamura, "Footprint-Based Personal Recognition," *IEEE TRANSACTIONS ON BIOMEDICAL ENGINEERING,* vol. 47, no. 11, Nov 2000.

[18] J. Fernadez, "The Classification of footprints of new born children (64)3," Int.Crim.Police Rev., 1953.

[19] K. K. Nagwanshi, M. Kumar and S. Dubey, "Development of Fuzzified Emotional Mobile (FEM)," in *IEEE International Multi-Conference on Automation, Computing, Communication, Control and Compressed Sensing (iMac4s), 2013 : ISBN:978-1-4673-5089-1*, Kottayam, Kerala, India, 22-13 March 2013.

[20] I. N. Bankman, Handbook of medical imaging: Processing and Analysis, Elsevier, 2008.

[21] A. Uhl and P. Wild, "Footprint-based biometric verification," *Journal of Electronic Imaging,* vol. 17, no. 1, pp. 1-12, 2008.

[22] P. H. Hennings-Yeomans, B. V. K. V. Kumar and M. Savvides, "Palmprint Classification Using Multiple Advanced Correlation Filters and Palm-Specific Segmentation," *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY,* vol. 2, no. 3, pp. 613-622, Sep 2007.

[23] J.-W. Jung, Z. Bien, S.-W. Lee and T. Sato, "Dynamic-Footprint based Person Identification using Mat-type Pressure Sensor," in *25th Annual lntemational Conference of the IEEE EMBS*, Cancun, Mexico, September 17-21,2003.

[24] J.-W. Jung, T. Sato and Z. Bien, "Uconstrained person recognition method using dynamic footprint," in *Intl. Conf. on Fuzzy Information Processing 2003-Vol-II*, 2003.

[25] V. Kumar and M.Ramakrishnan, "Footprint Recognition with COP Using Principle Component Analysis (PCA)," *Journal of Computational Information Systems,* vol. 8, no. 12, pp. 4939-4950, 2012.

[26] J.-S. R. Jang, "ANFIS: Adaptive-network-based fuzzy inference system," *IEEE Transactions on Systems, Man and Cybernetics,* vol. 23, pp. 665-685, 1993.

[27] T. Kohonen, Self-Organizing Maps, 3e, Springer Series in Information Sciences, 2001.

[28] B. Shin, E. Cha, Y. Woo and R. Klette, "Segmentation of Scanned Insect Footprints Using ART2 for Threshold Selection," *LNCS , Springer-Verlag,* vol. 4872, pp. 311-320, 2007.

[29] A. Kadyrov and M. Petrou, "The Trace Transform and Its Applications," *IEEE Transactions on Pattern Analysis and Machine Intelligence,* vol. 23, no. 8, pp. 811-828, 2007.

[30] J. Yun, G. Abowd, W. Woo and J. Ryu, "Biometric User Identification with Dynamic Footprint," in *Second International Conference onBio-Inspired Computing: Theories and Applications, 2007. BIC-TA 2007,* Zhengzhou, 2007.

[31] W. Li, D. Zhang and Z. Xu, "Palmprint Identification By Fourier transform," *Intl.Journal of Pattern Recognition and Artifical Intelligence,* vol. 16, no. 4, pp. 417-432, 2002.

[32] V. D. A. Kumar and M. Ramakrishnan, "Footprint Recognition using Modified Sequential Haar Energy Transform (MSHET)," *International Journal of Computer Science Issues, ISSN (Online): 1694-0784,* vol. 7, no. 3, pp. 47-50, May 2010.

[33] J. L. Wayman, "Technical testing and evaluation of biometric identification devices," *In Biometrics: Personal Identification in a Networked Society,* p. 345–368, 1999.

[34] V. Kumar and M. Ramakrishnan, "Employment of footprint

recognition system," *Indian Journal of Computer Science and Engineering,* vol. 3, no. 6, pp. 774-778, Jan 2013.

[35] V. A. Kumar and D. M. Ramakrishnan, "Legacy of Footprints Recognition- A Review," *International Journal of Computer Applications (0975 – 8887),* vol. 35, no. 11, pp. 9-16, December 2011.

[36] R. C. Gonzalez and R. E. Woods, Digital Image Processing, 3rd Edition, New Delhi: Pearson, 2008.

[37] A. Kumar and D. Zhang, "Personal Recognition Using Hand Shape and Texture," *IEEE TRANSACTIONS ON IMAGE PROCESSING,* vol. 15, no. 8, pp. 2454-2461, AUG 2006.

Kapil Kumar Nagwanshi received the M.Tech. Degree in computer science and engineering from C.S.V. Technical University, Bhilai, India in 2008,is currently pursuing Ph.D from C.S.V. Technical University, Bhilai. His research area includes biometrics, GPU computing, neural networks, fuzzy logic and predictive analytics. He has published more than 25 research papers in referred journals and conferences.

Sipi Dubey is a PhD from Pt. Ravishakar Shukla University Raipur, is currently working as Professor at Rungta College of Engineering \& Technology Bhilai.Her research area includes Image Processing, Signal Processing, Face Recognition, and Biometrics. She has published more than He has published more than 40 research papers in referred journals and conferences

Toran Verma received the M.Tech.~degree in computer science and engineering from C.S.V. Technical University, Bhilai, India in 20011, is currently pursuing Ph.D from C.S.V. Technical University, Bhilai. His research area includes biometrics, machine learning, neural networks, fuzzy logic and predictive analytics. He has published more than 25 research papers in referred journals and conferences.