Human Authentication Using Biometric Recognition

Shailendra Kumar Dewangan

Assistant Professor, Department of Electronics & Instrumentation Engineering
Chhatrapati Shivaji Institute of Technology, Durg, Chhattisgarh, India

Abstract - Authentication is the primary requirement for any system by means of privacy & security. Physiological biometrics is based on direct measurements of a part of the human body, such as finger-scan, facial scan, iris-scan, hand-scan, and retina-scan. Behavioral biometrics is based on measurements and data derived from an action and therefore indirectly measure characteristics of the human body, such as voice-scan and signature-scan. The element of time is essential to behavioral biometrics because it may change with time. In this paper the discussion is made on various aspects for designing a biometric recognition system for human authentication and related topics to the particular feature of biometric parameter.

Keywords - Biometric recognition, face, fingerprint, human authentication, iris, signature etc.

1. INTRODUCTION

"Biometrics" in easily explainable terms, is human traits or behaviors which can be measured, and used to differentiate between two or more persons. Biometric broken down literally equates to 'bio' meaning life, and metric meaning a measurable data. Biometrics is the automated use of physiological or behavioral characteristics to determine or verify identity. Automated use means using computers or machines, rather than human beings, to verify or determine physiological or behavioral characteristics. Physiological or behavioral characteristics are distinctive, which provide basic measurement of biometrics [1-2]. Different types of biometric technologies focus on different physical characteristics. Within the biometric community, these different applications are referred to as "modalities". The emerging biometric modalities include: Hand, Face, Fingerprint, Signature, Voice, Iris, Retina, Vein, DNA, Body Odor, Ear Pattern, Keystroke and Lips. General block diagram of a biometric recognition system is shown in Fig. 1. While designing a biometric recognition system distinctiveness is the primary measure of the variations or differences in the biometric pattern among the general population or available database. The highest degree of distinctiveness implies a unique identifier [3-4]. The iris and the retina have higher degrees of distinctiveness than hand or finger geometry. The application helps determine the degree of robustness and distinctiveness required.

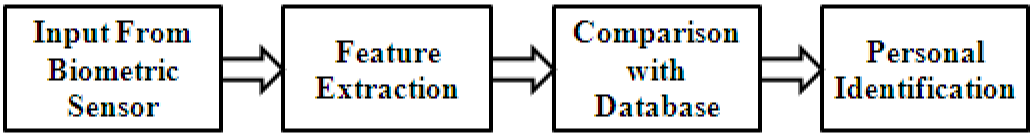

Fig. 1 - Biometric Recognition System

1.1 Signature Recognition - The aim of off-line signature verification is to decide, whether a signature originates from a given signer based on the scanned image of the signature and a few images of the original signatures of the signer [5-10]. This signature recognition process is completed in following steps. First the sample signature is obtained whether from scanned image or directly from the person, then features are extracted from the image of signature, then comparison is made with available database and finally, some kind of classifier is used to decide whether a given signature is an original or a forgery. The typical features to be analyzed from a signature sample may be maximum height, horizontal length, aspect ratio and number of pen ups in the signatures. It measures characteristics of handwritten signatures with respect to shape, speed, pressure, pen angle, sequence, etc. This verifier uses signature or graphic tablets and special pens to identify a person [11-15].

1.2 Face Recognition - The face plays a major role in our social intercourse in conveying identity and emotions. Face recognition is a challenging problem in the field of image analysis and computer vision that has received a great deal of attention over the last few years because of its many applications in various domains such as film processing, human-computer interaction, criminal identification etc. [16-18] A facial recognition system is a computer-driven application for automatically identifying a person from a digital image. It does that by comparing selected facial features in the live image and a facial database. For implementation of face recognition system feature based approach can be followed, which includes first process the input image to identify and extract distinctive facial features (as shown in Fig. 2) such as the eyes, mouth, nose, etc., as well as other marks, and then compute the geometric relationships among those facial points, thus reducing the input facial image to a vector of geometric features [19-21]. The main advantage of feature based method is its robustness to position variations in the input image; however a major disadvantage of these approaches is the difficulty of automatic feature detection.

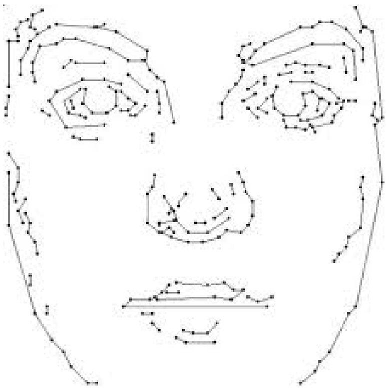

Fig. 2 - Facial Features

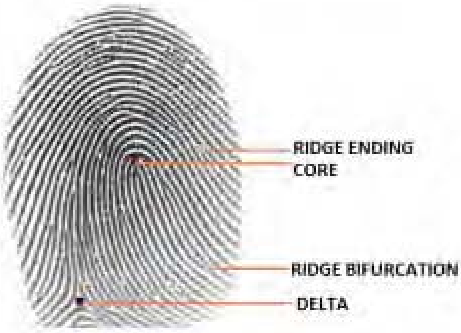

Fig. 3 - Fingerprint Features

1.3 Fingerprint Identification – It is the process of comparing two instances of friction ridge skin impressions from human fingers, to determine whether these impressions could have come from the same individual. The flexibility of friction ridge skin means that no two finger or palm prints are ever exactly alike in every detail; even two impressions recorded immediately after each other from the same hand may be slightly different. The biometric fingerprint sensor takes a digital picture of a fingerprint [22]. The fingerprint scan detects the ridges and valleys of a fingerprint and converts them into ones and zeroes. Complex algorithms analyze this raw biometric scan to identify characteristics of the fingerprint. In a typical image of fingerprint some features (Fig. 3) are required to be analyzed as the performance factors such as arch, delta, loop, ridge, core, lake etc. An arch is a pattern, where the ridges enter from one side of the finger, rise in the center forming an arc, and then exit the other side of the finger. The loop is a pattern, where the ridges enter from one side of a finger, form a curve, and tend to exit from the same side they enter. In the whorl pattern, ridges form circularly around a central point on the finger [23].

The different approaches for fingerprint impression matching can be coarsely classified into following families.

1.3.1 Correlation Based Matching: Two impression images are superimposed and the correlation between corresponding pixels is computed for different alignments (e.g. various displacements and rotations).

1.3.2 Minutiae Based Matching: This is the most popular and widely used technique, being the basis of the fingerprint comparison made by fingerprint examiners. Minutiae are extracted from the two fingerprints and stored as sets of points in the two- dimensional plane. Minutiae-based matching essentially consists of finding the alignment between the template and the input minutiae sets that result in the maximum number of minutiae pairings

1.3.3 Pattern Based (or Image Based) Matching: Pattern based algorithms compare the basic thumb impression patterns (arch, whorl, and loop) between a previously stored template and a candidate fingerprint. This requires that the images be aligned in the same orientation. To do this, the algorithm finds a central point in the impression image and centers on that. In a pattern-based algorithm, the template contains the type, size, and orientation of patterns within the aligned impression image. The candidate impression image is graphically compared with the template to determine the degree to which they match.

1.3.4 Ridge Feature Based Matching: Minutiae extraction is difficult in very low-quality thumb impression images. However, whereas other features of the impression ridge pattern (e.g., local orientation and frequency, ridge shape, texture information) may be extracted more reliably than minutiae, their distinctiveness is generally lower. The approaches belonging to this family compare thumb impression in term of features extracted from the ridge pattern. In principle, correlation and minutiae-based matching could be conceived of as subfamilies of ridge feature-based matching, in as much as the pixel intensity and the minutiae positions are themselves features of the thumb ridge pattern.

1.4 Iris Recognition - Iris recognition is a method of biometric authentication that uses pattern recognition techniques based on high-resolution images of the irises of an individual's eyes. Iris recognition uses camera technology. An iris-recognition algorithm can identify up to 200 identification points including rings, furrows and freckles within the iris. Few of them are shown in Fig. 4. First the system has to localize the inner and outer boundaries of the iris in an image of an eye [24-28]. Further subroutines detect and exclude eyelids, eyelashes, and specular reflections that often occlude parts of the iris.

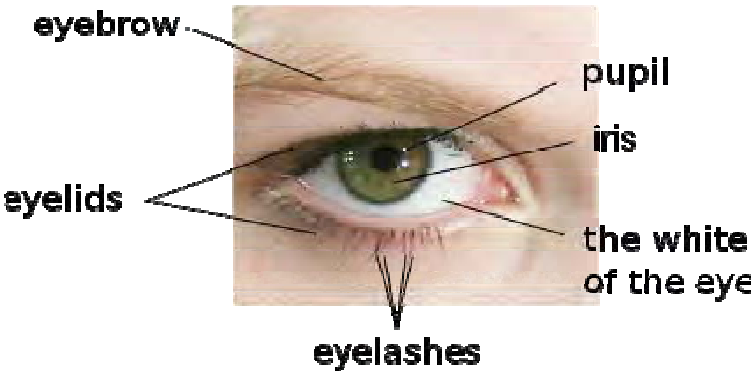

Fig. 4 - Iris Identification Model

For iris identification (one-to-many template matching) or verification (one-to-one template matching), a template created by imaging an iris is compared to stored templates in the iris database. If the Hamming distance is below the decision threshold, a positive identification has effectively been made because of the statistical extreme improbability that two different persons could agree by chance in so many bits, given the high entropy of iris templates.

1.4.1 Advantages of Iris Recognition

- **Uniqueness:** The uniqueness of iris pattern comes from the richness of texture details in iris images, such as freckles, coronas, stripes and furrows. Even twins have totally different iris details. The randomly distributed and irregularly shaped microstructures of iris patterns make the human iris one of the most informative and reliable biometric traits.
- **Stability:** Iris texture is formed during gestation and the main structures of iris are shaped after 8 months. It has also been shown that the iris is essentially stable across one's lifetime.
- **Non-invasiveness:** Since the iris is an internal organ as well as externally visible, iris images can be taken at a distance from the user. Non-invasiveness not only makes the procedure of iris recognition more hygeian than touch needed biometric modalities such as fingerprint recognition, but also enables iris recognition to be applicable to passive or covert personal identification, which is of great importance for public security applications.
- **Scalability:** Images of the iris region can be normalized into rectangle regions of fixed size so that binary feature codes of fixed length can be extracted for extremely fast feature matching based on simple XOR operation. Therefore iris recognition is well suited to large-scale personal identification applications.
- **Security:** Security of biometric systems has been a bottleneck to the wide deployment of biometrics. Compared with most biometric modalities, iris recognition is more secure simply because of the difficulty of live iris forgery.

2. METHODOLOGY

The constant development of computer tools leads to a requirement of a biometric identification system can be made easier by interface between the man and the computer. The process of biometric recognition deals with the problems of reading offline available database. The recognition process can be subdivided into two categories as (i) Online methods & (ii) Offline method. These methods are briefly discussed further;

2.1 Online Recognition : In case of online biometric recognition, there is real time recognition. Online systems have better information for doing recognition since they have timing information and since they avoid the initial search step of locating the features as in the case of their offline counterpart. Online systems obtain the position of the pen as a function of time directly from the interface. Online biometric recognition is known as a challenging problem because of the complexity in different modes.

2.2 Offline Recognition: In case of offline biometric recognition the features are compared in form of documents. Such as the handwritten signature is typically scanned in form of a paper document and made available in the form of a binary or gray scale image to the recognition algorithm. Offline biometric recognition is a more challenging and difficult task as there is no control over the medium and instruments used. The artifacts of the complex interaction between the instrument medium and subsequent operations such as scanning and binarization present additional challenges to the algorithm for the offline recognition methods. Therefore offline biometric recognition is considered as a more challenging task then its online counterpart.

2.3 Experimental Set-up: Various devices are available these days, which can be used for the process of biometric recognition. A digital tablet can be used for taking online or real-time signature samples. Biometric fingerprint identification device is also easily available. A fingerprint scanner is an electronic device used to capture a digital image of the fingerprint pattern. This scan is digitally processed to create a biometric template which is stored and used for matching.

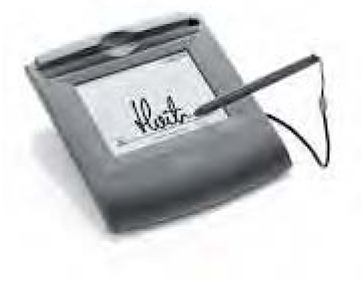

Fig. 5 - Digital Tablet

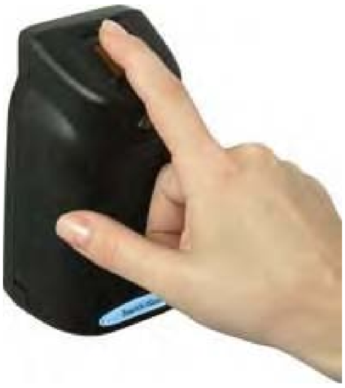

Fig. 6 - Fingerprint Scanner

Face detection is used in biometrics, often as a part of (or together with) a facial recognition system. It is also used in video surveillance, human computer interface and image database management. A face camera is a webcam with 2 Mpx or above which can take a clear crisp photograph of the face. Some recent digital cameras use face detection for autofocus. Also, face detection is useful for selecting regions of interest in photo slideshows that use a pan-and-scale Ken Burns effect. That is, the content of a given part of an image is transformed into features, after which a classifier trained on example faces decides whether that particular region of the image is a face, or not. A face model can contain the appearance, shape, and motion of faces. There are several shapes of faces. Some common ones are oval, rectangle, round, square, heart, and triangle. Motions include, but not limited to, blinking, raised eyebrows, flared nostrils, wrinkled forehead, and opened mouth. The face models will not be able to represent any person making any expression, but the technique does result in an acceptable degree of accuracy. The models are passed over the image to find faces, however this technique works better with face tracking. Once the face is detected, the model is laid over the face and the system is able to track face movements.

Iris cameras (shown in Fig. 7) perform recognition detection of a person's identity by mathematical analysis of the random patterns that are visible within the iris of an eye from some distance. It combines computer vision, pattern recognition, statistical inference and optics. Iris cameras, in general, take a digital photo of the iris pattern and recreating an encrypted digital template of that pattern. That encrypted template cannot be re-engineered or reproduced in any sort of visual image. Iris recognition therefore affords the highest level defense against identity theft, the most rapidly growing crime.

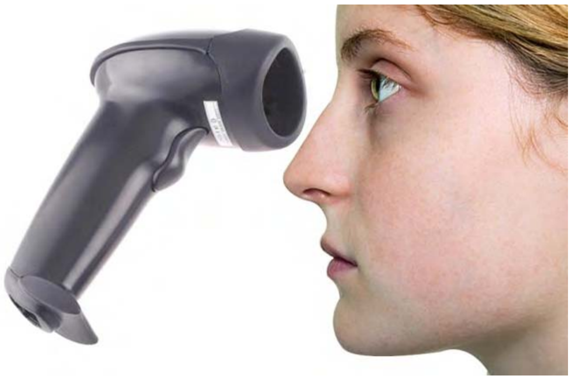

Fig. 7 - Iris Camera

2.4 Performance Parameters: On basis of comparison with existing database and sample images it can be concluded that whether the test sample is available in database or not. Also the genuine and authentic biometric parameter can be decided. For ensuring good performance for the recognition system few parameters are required to be set, are discussed as followings:

2.4.1 False Accept Rate or False Match Rate (FAR or FMR): The false acceptance rate is given by the number of fake samples accepted by the system with respect to the total number of comparisons made. It is the probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs which are incorrectly accepted. In case of similarity scale, if the person is imposter in real, but the matching score is higher than the threshold, and then he is treated as genuine that increases the FAR and hence performance also depends upon the selection of threshold value.

2.4.2 False Reject Rate or False Non-Match Rate (FRR or FNMR): The false rejection rate is the total number of genuine samples rejected by the system with respect to the total number of comparisons made. Both FAR and FRR depend on the threshold variance parameter taken to decide the genuineness of an image. If we choose a high threshold variance then the FRR is reduced, but at the same time the FAR also increases. If we choose a low threshold variance then the FAR is reduced, but at the same time the FRR also increases. The FRR is the measurement of the probability that a biometric system will fail to identify an individual who is properly enrolled. It measures the percent of valid inputs which are incorrectly rejected.

2.4.3 Receiver Operating Characteristic or Relative Operating Characteristic (ROC): The ROC plot is a visual characterization of the trade-off between the FAR and the FRR. In general, the matching algorithm performs a decision based on a threshold which determines how close to a template the input needs to be for it to be considered a match. If the threshold is reduced, there will be less false non-matches but more false accepts. Correspondingly, a higher threshold will reduce the FAR but increase the FRR. This more linear graph illuminates the differences for higher performances (rarer errors).

2.4.4 Equal Error Rate or Crossover Error Rate (EER or CER): The rates at which both accept and reject errors are equal. The value of the EER can be easily obtained from the ROC curve. The EER is a quick way to compare the accuracy of devices with different ROC curves. In general, the device with the lowest EER is most accurate. If the FAR of a system is same as the FRR then the system is said to be in an optimal state. In this condition, the FAR and FRR are also known as ERR.

3. CONCLUSION

Biometrics is a rapidly evolving technology that is being widely used in forensics, security; prevent unauthorized access in bank or ATMs, in cellular phones, smart cards, PCs, in workplaces, and computer networks. There are numerous forms of biometrics now being built into technology platforms. It has been implemented in public for short time. There are lots of applications and solutions in biometrics technology used in security systems, which can improve our lives such as: improved security, it is reduced con and password administrator costs, easy to use and make life more secure and comfortable. But it is not possible to definitely state if a biometric technique are successful run, it is essential to locate factors that’s help to reduce affect system performance. The international biometric group Strike System Strikes are: in Fingerprint Dry/oily finger, in Voice recognition Cold or illness that affects voice, in Facial recognition Lighting conditions, in Iris-scan Too much movement of head or eye, in Hand geometry Bandages, and in Signature-scan Different signing positions. Face recognition technology are more reliable, non-intrusive, inexpensive and extremely accurate. Currently Face recognition technology is the most challenging recognition technologies.

REFERENCES

[1] M. A. Sasse, “Assessing the Biometrics Enterprise: The Present Situation & Future Challenges”, IEE Seminar on the Challenge of Biometrics, London, UK, ISBN 0-8634-1480-X, December 2004.

[2] U. Uludag, S. Pankanti, S. Prabhakar, & A. K. Jain, “Biometric Cryptosystems : Issues and Challenges”, IEEE, Special Issue on Enabling Security Technology for Digital Rights Management, Vol. 92, No. 6, pp. 948–960, 2004.

[3] A. K. Jain, "Biometrics: A Grand Challenge”, International Conference on Pattern Recognition, Cambridge, UK, pp. 935-942, August 2004.

[4] Olufemi Sunday Adeoye, “A Survey of Emerging Biometric Technologies”, International Journal of Computer Applications (0975-8887), Vol. 9, No.10, pp. 01-05, November 2010.

[5] Quen Zong Wu, I. Chang Joe & Suh Yin Lee, “On-Line Signature Verification Using LPC Cepstrum and Neural Networks”, IEEE Trans. on Systems, Man, and Cybernetics, 27 (1), pp. 148-153, 1997.

[6] A. Jain, F. Griess and S. Connell, “On-line signature Verification: Pattern Recognition”, WSEAS Transactions on Mathematics, Issue 9, Vol. 8, 2010.

[7] Bhupendra M. Chaudhari, Abhay B. Nehete, Kantilal P. Rane & Ulhas B. Shinde, “Efficient Feature Extraction Technique for Signature Recognition”, International Journal of Advanced Engineering & Application, pp. 64-70, January 2011.

[8] S. K. Dewangan, P. Gupta, U. K. Sahu & I. Verma, “Realtime Recognition of Handwritten Words using Hidden Markov Model”, International Journal of Technological Synthesis and Analysis, ISSN: 2320-2386, Vol. 1, Issue 1, pp. 07-09, December 2012.

[9] S. K. Dewangan, P. Gupta, U. K. Sahu, I. Verma & R. Sonwane, “Performance Evaluation of Edge Detection Techniques on Photographic Images”, International Journal of Advanced Research in Computer Science, ISSN: 0976-5697, Vol. 3, No. 7, pp. 206-208, November - December 2012.

[10] Bence Kovari, Benedek Toth & Hassan Charaf, “Classification Approaches in Off-Line Handwritten Signature Verification”, WDET Trans. on Mathematics , Issue 9, Vol. 8, p.p. 500-509, September 2009.

[11] S. B. Patil & S. K. Dewangan, “Neural Network based Offline Handwritten Signature Verification System using Hu’s Moment Invariant Analysis”, International Journal of Engineering and Advanced Technology, ISSN: 2249-8958, Vol. 1, Issue 1, pp. 73-79, October 2011.

[12] A. Alizadeh, T. Alizadeh & Z. Daei, “Optimal Threshold Selection for Online Verification of Signature”, Proceedings of the International Multi Conference of Engineers and Computer Scientists, Vol. 1, p.p. 17-21, 2010.

[13] W. Nelson and E. Kishon, “Use of Dynamic Features for Signature Verification”, IEEE International Conference on Systems, Man, and Cybernetics, Charlottesville, Virginia, pp. 201-205, October 1991.

[14] V.A. Baradi & H.B. Kakere, “Offline Signature Recognition System”, International Journal of Computer Applications (0975 - 8887) Vol. 1, No. 27, p.p. 48-56, 2010.

[15] S. K. Dewangan, “Devnagari Handwritten Signature Recognition Using Neural Network”, (ISBN: 978-3-659-26595-2), Lambert Academic Publications (LAP), Germany, 2012.

[16] S. L. Wijaya, M. Savvides & B. V. K. V. Kumar, "Illumination Tolerant Face Verification of Low Bit Rate JPEG2000 Wavelet Images With Advanced Correlation Filters for Handheld Devices", Applied Optics, Vol. 44, pp. 655-665, 2005.

[17] N. Patel & S. K. Dewangan, “An Overview of Face Recognition Schemes”, International Conference of Advance Research and Innovation (ICARI-2015), Institution of Engineers (India), Delhi State Centre, Engineers Bhawan, New Delhi, India, 2015.

[18] E. Acosta, L. Torres, A. Albiol & E. J. Delp, "An Automatic Face Detection & Recognition System for Video Indexing Applications", IEEE International Conference on Acoustics, Speech and Signal Processing, Orlando, Florida, Vol. 4, pp. 3644-3647, 2002.

[19] J. N. K. Liu, M. Wang & B. Feng, "iBotGuard : An Internet-Based Intelligent Robot Security System Using Invariant Face Recognition Against Intruder", IEEE Trans. on Systems Man & Cybernetics, Vol. 35, pp. 97-105, 2005.

[20] B. Moghaddam & M. H. Yang, "Learning Gender with Support Faces", IEEE Trans. on Pattern Analysis & Machine Intelligence, Vol. 24, pp. 707-711, 2002.

[21] A. Colmenarez, B. J. Frey & T. S. Huang, "A Probabilistic Framework for Embedded Face & Facial Expression Recognition", IEEE Conference on Computer Vision and Pattern Recognition, Vol. 1, Ft. Collins, CO, USA, pp. 1592-1597, 1999.

[22] N. Ratha, S. Chen & A. K. Jain, "Adaptive Flow Orientation Based Feature Extraction in Fingerprint Images", Pattern Recognition, Vol. 28, pp. 1657-1672, November 1995.

[23] Sangram Bana & Dr. Davinder Kaur, “Fingerprint Recognition using Image Segmentation“, International Journal of Advanced Engineering Sciences & Technologies, Vol. 5, Issue 1, pp. 12-23, 2011.

[24] P. Thirumurugan & G. Mohanbabu, “Iris Recognition using Wavelet Transformation Techniques”, International Journal of Computer Science and Mobile Computing, Vol. 3, Issue.1, pp. 75-83, January 2014.

[25] Aparna G. Gale & S. S. Salankar, “A Review on Advance Methods of Feature Extraction in Iris Recognition System”, IOSR Journal of Electrical and Electronics Engineering, pp. 65-70, 2014.

[26] Surbhi Garg & Harmeet Kaur, “Survey Paper on Phase Based Iris Recognition”, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, Issue 4, pp. 199-201, April 2014.

[27] M. M. Rahman, R. Hartley & S. Ishikawa, "A Passive & Multimodal Biometric System for Personal Identification", International Conference on Visualization, Imaging & Image Processing. Spain, pp. 89-92, 2005.

[28] J. Daugman, “How Iris Recognition Works”, IEEE Trans. on Circuits and Systems for Video Technology, Vol. 14, No. 1, pp 21-30, January, 2004.

Author’s Profile

Shailendra Kumar Dewangan received M.E. & B.E. in ETC from SSCET Bhilai, Chhattisgarh, India. He is currently working as an Assistant Professor in the Department of Electronics & Instrumentation Engg. at CSIT Durg. His areas of interest include digital signal processing, digital image processing, information security, digital watermarking, advancements in communication technology, etc. Besides he has lifetime membership of Indian Society of Technical Education (ISTE) and Associate membership of Institute of Electronics & Telecommunication Engineers (IETE).