Designing and Implementation of an Efficient Fingerprint Recognition System Using Minutia Feature and KNN Classifier

Mayank Tripathy ^{#1}, Deepak Shrivastava ^{*2}

^{#1}M. Tech Scholar, Dept. of CSE, Disha Institute of Management and Technology, Raipur, India ^{*2}Assistant Professor, Dept. of CSE, Disha Institute of Management and Technology, Raipur, India

Abstract— Biometric feature based person recognition system becomes very important and necessary in this age, due to higher demand of security in corporate culture. A biometric system offers automatic identification of an individual based on a unique feature or characteristic obsessed by the individual. Human fingerprints are rich in details called minutiae, which can be used as identification marks for fingerprint verification. This work deals with the development of a highly robust and efficient biometric person identification system based on fingerprint features. Particularly this work is intended to designing and implementation of an efficient fingerprint recognition system based on minutia feature and KNN classifier. To achieve good minutiae feature extraction from fingerprints, pre-processing in form of image enhancement and binarization is first applied on fingerprints before they are evaluated. Minutia-marking with false minutiae removal methods are also used to remove false minutia. The proposed work utilizes finger print minutia as a feature for finger print identification and for the efficient classification K-Nearest Neighbour (KNN) classifier is utilized. The software platform used for the implementation of the proposed work is MATLAB. A database of total 50 real fingerprint images has been developed to test the effectiveness of the proposed system. For proper evaluation of proposed system performance 25 female and 25 male fingerprint images have been used. After the complete comparative analysis recognition efficiency among proposed system and conventional minutia matching based system, it is found that the fingerprint recognition efficiency of the developed system is very high about 99.9%, while about 70% for conventional minutia matching based system.

Keywords— Biometric system, fingerprint, minutia, feature extraction, feature matching, KNN Classifier.

I. INTRODUCTION

A fingerprint is the feature pattern of one finger (Fig.1). It is believed with strong evidences that each fingerprint is unique. Each person has his own fingerprints with the permanent uniqueness. So fingerprints have being used for identification and forensic investigation for a long time.

A fingerprint is composed of many ridges and furrows. These ridges and furrows present good similarities in each small local window, like parallelism and average width. However, shown by intensive research on fingerprint recognition, fingerprints are not distinguished by their ridges and furrows, but by Minutia, which are some abnormal points on the ridges (Fig.2).



Fig.1. A fingerprint image acquired by an Optical Sensor

Among the variety of minutia types reported in literatures, two are mostly significant and in heavy usage: one is called termination, which is the immediate ending of a ridge; the other is called bifurcation, which is the point on the ridge from which two branches derive.



A. Foundations of Fingerprint Recognition

The fingerprint recognition problem can be grouped into two sub-domains: one is fingerprint verification and the other is fingerprint identification (Fig.3).



Fingerprint verification is to verify the authenticity of one person by his fingerprint. The user provides his fingerprint together with his identity information like his ID number. The fingerprint verification system retrieves the fingerprint template according to the ID number and matches the template with the real-time acquired fingerprint from the user.

Fingerprint identification is to specify one person's identity by his fingerprint(s). Without knowledge of the person's identity, the fingerprint identification system tries to match his fingerprint(s) with those in the whole fingerprint database.

II. PROPOSED METHODOLOGY AND SYSTEM DESIGN

A fingerprint recognition system constitutes of fingerprint acquiring device, minutia extractor and minutia classification. The efficiency of the system basically depends on the feature extraction and its proper classification. For the finger print acquiring part an optical sensor has been utilized and complete database of 50 real images consisting 25 female and 25 males fingerprints have been utilized. The complete proposed methodology of this work is shown in Fig.4 with the help of flow chart representation.



Fig.4 Methodology of the proposed system.

The detailed description for each part of the proposed work is given in following subsections.

A. Fingerprint Image Pre-processing

1) Fingerprint Image Enhancement

Fingerprint Image enhancement process enhances the contrast between ridges and furrows and for connecting the false broken points of ridges due to insufficient amount of ink, are very useful for keep a higher accuracy to fingerprint recognition. Two Methods are adopted in this work: the first one is Histogram Equalization; the next one is Fourier Transform.

Histogram Equalization:

Histogram equalization process expands the pixel value distribution of an image, to increase the perceptional information. The original histogram of a fingerprint image has the bimodal type [Fig.5], the histogram after the histogram equalization occupies all the range from 0 to 255 and the visualization effect is enhanced [Fig.6].



Fig.5 The Original histogram



Fig.6 Histogram plot after the Histogram Equalization

The right side of the following Figure [Fig.7] is the output after the histogram equalization.



Fig.7 Histogram Enhancement, Original Image (Left), Enhanced image (Right)

Fingerprint Enhancement by Fourier Transform

The image is divided into small processing blocks (32 by 32 pixels) and performs the Fourier transform according to:

$$F(u,v) = \sum_{\substack{x=0\\ x=0}}^{M-1} \int_{y=0}^{y=1} f(x,y) \times \exp\left\{-j2\pi \times \left(\frac{ux}{M} + \frac{vy}{N}\right)\right\} \qquad \dots (1)$$

For u = 0, 1, 2... 31 and v = 0, 1, 2... 31.

In order to enhance a specific block by its dominant frequencies, we multiply the FFT of the block by its magnitude a set of times. Where the magnitude of the original FFT = abs (F(u, v) = |F(u, v)|.Get the enhanced block according to

$$g(x, y) = F^{-1} \left\{ F(u, v) \times \left| F(u, v) \right|^{k} \right\} \qquad ...(2)$$

Where $F^{-1}(F(u, v))$ is done by:

$$f(x, y) = \frac{1}{MN} \sum_{x=0}^{M-1} \sum_{y=0}^{M-1} F(u, y) \times \exp\left\{j2\pi \times \left(\frac{ux}{M} + \frac{vy}{N}\right)\right\} \dots (3)$$

For x = 0, 1, 2... 31 and y = 0, 1, 2... 31.

Where k in formula (2) is an experimentally determined constant, which we choose k=0.45 to calculate. While having a higher "k" improves the appearance of the ridges, filling up small holes in ridges, having too high a "k" can result in false joining of ridges. Thus a termination might become a bifurcation. Fig.8 presents the image after FFT enhancement.



Fig.8 Fingerprint enhancement by FFT Enhanced image (left), Original image (right)

The enhanced image after FFT has the improvements to connect some falsely broken points on ridges and to remove some spurious connections between ridges.

Fingerprint Image Binarization

Fingerprint Image Binarization is the mapping 8-bit Gray fingerprint image to a 1-bit image with 0-value for ridges and 1-value for furrows. After the operation, ridges in the fingerprint are highlighted with black color while furrows are white



Fig.9 the Fingerprint image after adaptive binarization Binarized image (left), Enhanced gray image (right).

2) Fingerprint Image Segmentation

To extract the Region of Interest (ROI), a two-step method is used. The first step is block direction estimation and direction variety check [1], while the second is extraction of ROI using Morphological processing.

Block direction estimation

Proposed block direction estimation process comprises two simple steps:

- i. Estimate the block direction for each 16×16 block of the fingerprint image by calculating gradient values along x-direction (gx) and y-direction (gy) for each pixel of the block. Two Sobel filters are used to perform this task.
- ii. After direction estimation of each block, those blocks without significant information on ridges and furrows are discarded based on the following formulas:

 $E = \{2\Sigma\Sigma(g_{X}*g_{y}) + \Sigma\Sigma(g_{X}^{2}-g_{y}^{2})\}/W*W*\Sigma\Sigma~(g_{X}^{2}+g_{y}^{2})$ For each block, if its certainty level E is below a threshold, then the block is regarded as a background block. The direction map is shown in the following diagram. It is assumed there is only one fingerprint in each image.



Fig.10 Direction map. Binarized fingerprint (left), Direction map (right).

ROI extraction by Morphological operations

Two Morphological operations called 'OPEN' and 'CLOSE' are adopted. The 'OPEN' operation can expand images and remove peaks introduced by background noise [Fig.11]. The 'CLOSE' operation can shrink images and eliminate small cavities [Fig.12].





Fig.12 After CLOSE operation



Fig.13 After OPEN operation

Fig.14 ROI + Bound

Fig.14 shows the interested fingerprint image area and it's bound. The bound is the subtraction of the closed area from the opened area.

3) Minutia Feature Extraction

Fingerprint Ridge Thinning

Ridge thinning process has been used to eliminate the redundant pixels of ridges till the ridges are just one pixel wide. In each scan of the full fingerprint image, the algorithm marks down redundant pixels in each small image window (3x3) and finally removes all those marked pixels after several scans. The thinned ridge map is then filtered by other three Morphological operations to remove some H breaks, isolated points and spikes.

Minutia Marking

After the fingerprint ridge thinning, marking minutia points is relatively easy. In general, for each 3x3 window, if the central pixel is 1 and has exactly 3 one-value neighbors, then the central pixel is a ridge branch [Fig.15]. If the central pixel is 1 and has only 1 one-value neighbor, then the central pixel is a ridge ending [Fig.16].



Fig.17 Triple counting branch

Fig.17 illustrates a special case that a genuine branch is triple counted. Suppose both the uppermost pixel with value 1 and the rightmost pixel with value 1 have another neighbor outside the 3x3 window, so the two pixels will be marked as branches too. But actually only one branch is located in the small region. So a check routine requiring that none of the neighbors of a branch are branches is added.

Also the average inter-ridge width D is estimated at this stage. The average inter-ridge width refers to the average distance between two neighboring ridges. The way to approximate the D value is simple. Scan a row of the thinned ridge image and sum up all pixels in the row whose value is one. Then divide the row length with the above summation to get an inter-ridge width, finally all the interridge widths are averaged to get the D.

False Minutia Removal

False minutia will significantly affect the accuracy of matching if they are simply regarded as genuine minutia. So some mechanisms of removing false minutia are essential to keep the fingerprint verification system effective. Seven types of false minutia are specified in following diagrams:



Fig.18 False Minutia Structures

Fig.18 False Minutia Structures. m1 is a spike piercing into a valley. In the m2 case a spike falsely connects two ridges. m3 has two near bifurcations located in the same ridge. The two ridge broken points in the m4 case have nearly the same orientation and a short distance. m5 is alike the m4 case with the exception that one part of the broken ridge is so short that another termination is generated. m6 extends the m4 case but with the extra property that a third ridge is found in the middle of the two parts of the broken ridge. m7 has only one short ridge found in the threshold window. [4] Only handles the case m1, m4,m5 and m6. [9] And [2] have not false minutia removal by simply assuming the image quality is fairly good. [12] Has not a systematic healing method to remove those spurious minutia's although it lists all types of false minutia shown in Fig. 18 except the m3 case. The procedures in removing false minutia are:

- ➢ If the distance between one bifurcation and one termination is less than D and the two minutia's are in the same ridge (m1 case). Remove both of them. Where D is the average inter-ridge width representing the average distance between two parallel neighboring ridges.
- ➢ If the distance between two bifurcations is less than D and they are in the same ridge, remove the two bifurcations. (m2, m3 cases).
- ➢ If two terminations are within a distance D and their directions are coincident with a small angle variation. And they suffice the condition that no any other termination is located between the two terminations. Then the two terminations are regarded as false minutia derived from a broken ridge and are removed. (Case m4, m5, m6).
- ➢ If two terminations are located in a short ridge with length less than D, remove the two terminations (m7).

The proposed procedures in removing false minutia for this work have two advantages. One is that the ridge ID is used to distinguish minutia and the seven types of false minutia are strictly defined comparing with those loosely defined by other methods. The second advantage is that the order of removal procedures is well considered to reduce the computation complexity.

Unify terminations and bifurcations

Since various data acquisition conditions such as impression pressure can easily change one type of minutia into the other, most researchers adopt the unification representation for both termination and bifurcation. So each minutia is completely characterized by the following parameters at last: 1) x-coordinate, 2) y-coordinate, and 3) orientation.

The orientation calculation for a bifurcation needs to be specially considered. Here this work proposes a novel representation to break a bifurcation into three terminations. The three new terminations are the three neighbor pixels of the bifurcation and each of the three ridges connected to the bifurcation before is now associated with a termination respectively [Fig.19].



Fig.19 A bifurcation to three terminations Three neighbors become terminations (Left) Each termination has their own orientation (Right)

Track a ridge segment who's starting point is the termination and length is D. Sum up all x-coordinates of points in the ridge segment. Divide above summation with D to get sx. Then get sy using the same way. Get the direction from: atan((sy-ty)/(sx-tx)).

Structure of Minutia Feature

The minutia feature is a unique key to represent an individual uniquely during fingerprint based person recognition. Conventional minutia matching algorithm needs some complex structure of minutia feature along with supportive information, for providing robustness to increase the recognition rate. This leads to the demand of high storage space requirement for database storage and also increases the recognition time consumption. The minutia feature utilized by all the conventional minutia matching algorithms needs to store minutia information along with the complete path. Table-I shows five rows out of 374 rows of minutia feature extracted from first fingerprint image of our database for conventional minutia matching techniques.

TABLE I Example of Minutia feature used by conventional techniques

inple of Minutia feature asea by conventional teening						
S. No.	Minutia Path		Real Minutia			
1	1.93E+02	1.87E+02	-2.11E+00			
2	2.09E+02	1.94E+02	-2.44E+00			
3	7.50E+01	2.30E+01	-6.88E-01			
4	1.17E+02	1.26E+02	-2.28E+00			
5	2.37E+02	4.90E+01	-1.95E+00			

This proposed work proposes an efficient minutia classification scheme by using KNN classifier. Since the classification ability of the proposed KNN classifier is very high and robust, this work only uses obtained real minutia values to represent particular individuals fingerprint. Hence the minutia feature used for the same fingerprint image for this work is given in table-II.

 TABLE II

 Example of Minutia feature used by proposed technique

	S. No.	Real Minutia	
ſ	1	-2.11E+00	
	2	-2.44E+00	
ſ	3	-6.88E-01	
ſ	4	-2.28E+00	
	5	-1.95E+00	

Therefore by removing the path consideration the feature handling and database storage requirement reduces to 70%.

4) Minutia Classification using KNN Classifier

This is the most important and critical stage for any recognition system.

In pattern recognition, the K-Nearest Neighbors algorithm (KNN) is a non-parametric method used for classification and regression. In both cases, the input consists of the K closest training examples in the feature space. The output depends on whether KNN is used for classification or regression:

In KNN classification, the output is a class membership. An object is classified by a majority vote of its neighbors, with the object being assigned to the class most common among its K nearest neighbors (K is a positive integer, typically small). If K = 1, then the object is simply assigned to the class of that single nearest neighbor.

In KNN regression, the output is the property value for the object. This value is the average of the values of its k nearest neighbors.

A graphical user interface is also developed for the proposed system to make the project work user friendly. The snapshot of the developed GUI is shown below.



Fig.20 the snapshot of the developed GUI.

III. EXPERIMENTATION RESULTS

A. Experimentation Results

A database of total 50 real fingerprint images has been developed to test the effectiveness of the proposed system. For proper evaluation of proposed system performance 25 female and 25 male fingerprint images have been used.

This work tests all the images without any fine tuning for the developed database. The experiments show developed program can differentiate imposturous minutia pairs from genuine minutia pairs in a certain confidence level. Here table-III shows the tabulated results for correct and incorrect fingerprint recognition of all the 50 images for both the conventional minutia matching and proposed KNN based technique.

	TABLE III		
Tabulated results for correct	and incorrect fi	ingerprint recognition	of all 50
images			

		Minutia Matching		Proposed KNN	
		Technique		Based Technique	
S. No.	Fingerprint Image Name	Recognition Status	Correct Recognition	Recognition Status	Correct Recognition
1	1.bmp	Yes	Recognized	Yes	Recognized
2	2.bmp	Yes	Not Recognized	Yes	Recognized
3	3.bmp	Yes	Not Recognized	Yes	Recognized
4	4.bmp	Yes	Not Recognized	Yes	Recognized
5	5.bmp	Yes	Not Recognized	Yes	Recognized
6	6.bmp	Yes	Not Recognized	Yes	Recognized
7	7.bmp	Yes	Not Recognized	Yes	Recognized
8	8.bmp	Yes	Not Recognized	Yes	Recognized
9	9.bmp	Yes	Not Recognized	Yes	Recognized
10	10.bmp	Yes	Recognized	Yes	Recognized
11	11.bmp	Yes	Recognized	Yes	Recognized
12	12.bmp	Yes	Recognized	Yes	Recognized
13	13.bmp	Yes	Recognized	Yes	Recognized
14	14.bmp	Yes	Recognized	Yes	Recognized
15	15.bmp	Yes	Recognized	Yes	Recognized
16	16.bmp	Yes	Recognized	Yes	Recognized
17	17.bmp	Yes	Recognized	Yes	Recognized
18	18.bmp	Yes	Recognized	Yes	Recognized
19	19.bmp	Yes	Recognized	Yes	Recognized
20	20.bmp	Yes	Recognized	Yes	Recognized
21	21.bmp	Yes	Recognized	Yes	Recognized
22	22.bmp	Yes	Recognized	Yes	Recognized
23	23.bmp	Yes	Recognized	Yes	Recognized
24	24.bmp	Yes	Recognized	Yes	Recognized
25	25.bmp	Yes	Recognized	Yes	Recognized
26	26.bmp	Yes	Recognized	Yes	Recognized
27	27.bmp	Yes	Recognized	Yes	Recognized
28	28.bmp	Yes	Recognized	Yes	Recognized
29	29.bmp	Yes	Recognized	Yes	Recognized
30	30.bmp	Yes	Recognized	Yes	Recognized
31	31.bmp	Yes	Recognized	Yes	Recognized
32	32.bmp	Yes	Recognized	Yes	Recognized
33	33.bmp	Yes	Recognized	Yes	Recognized
34	34.bmp	Yes	Recognized	Yes	Recognized
35	35.bmp	Yes	Recognized	Yes	Recognized
36	36.bmp	Yes	Recognized	Yes	Recognized
37	37.bmp	Yes	Recognized	Yes	Recognized
38	38.bmp	Yes	Recognized	Yes	Recognized
39	39.bmp	Yes	Recognized	Yes	Recognized
40	40.bmp	Yes	Recognized	Yes	Recognized
41	41.bmp	Yes	Recognized	Yes	Recognized
42	42.bmp	Yes	Recognized	Yes	Recognized
43	43.bmp	Yes	Recognized	Yes	Recognized
44	44.bmp	Yes	Not Recognized	Yes	Recognized
45	45.bmp	Yes	Not Recognized	Yes	Recognized
46	46.bmp	Yes	Not Recognized	Yes	Recognized
47	47.bmp	Yes	Not Recognized	Yes	Recognized
48	48.bmp	Yes	Not Recognized	Yes	Recognized
49	49.bmp	Yes	Not Recognized	Yes	Recognized
50	50.bmp	Yes	Not Recognized	Yes	Recognized



Fig.21 Recognition Result

Now Fig. 21 shows the plot of fingerprint recognition for conventional minutia matching and developed KNN based fingerprint recognition system. From Fig. 21 it is clearly observable that the recognition efficiency of the developed technique is very high 99.9%, while for conventional minutia matching technique it is about 70%.

IV. CONCLUSIONS

This paper put forward a highly robust and efficient biometric person identification system based on fingerprint features. Particularly this work was intended to design and implement an efficient fingerprint recognition system based on minutia feature and KNN classifier. The proposed work utilized finger print minutia as a feature for finger print identification and for the efficient classification K-Nearest Neighbor (KNN) classifier is utilized.

To achieve good minutiae feature extraction from raw fingerprints, pre-processing techniques have been also used. Additionally minutia marking with false minutiae removal process is used to remove false minutia. The software platform used for the implementation of the proposed work is MATLAB 2012(b). A database of total 50 real fingerprint images has been developed to test the effectiveness of the proposed system. For proper evaluation of proposed system performance 25 female and 25 male fingerprint images have been used. After the complete comparative analysis of recognition efficiency among proposed system and conventional minutia matching based system, it is found that the fingerprint recognition efficiency of the developed system is very high about 99.9%, while coming out about 70% for conventional minutia matching based system.

Moreover a new framework of the minutia feature utilization has been also developed, resulting the advantage over the conventional one that, the database storage and feature space requirement is 70% reduced as compare to conventional minutia matching technique.

REFERENCES

- Lin Hong. "Automatic Personal Identification Using Fingerprints", Ph.D. Thesis, 1998.
- [2] D.Maio and D. Maltoni. Direct gray-scale minutiae detection in fingerprints. IEEE Trans. Pattern Anal. And Machine Intell., 19(1):27-40, 1997.
- [3] Jain, A.K., Hong, L., and Bolle, R.(1997), "On-Line Fingerprint Verification," IEEE Trans. On Pattern Anal and Machine Intell, 19(4), pp. 302-314.
- [4] N. Ratha, S. Chen and A.K. Jain, "Adaptive Flow Orientation Based Feature Extraction in Fingerprint Images", Pattern Recognition, Vol. 28, pp. 1657-1672, November 1995.

- [5] Alessandro Farina, Zsolt M.Kovacs-Vajna, Alberto leone, Fingerprint minutiae extraction from skeletonized binary images, Pattern Recognition, Vol.32, No.4, pp877-889, 1999.
- [6] Lee, C.J., and Wang, S.D.: Fingerprint feature extration using Gabor filters, Electron. Lett., 1999, 35, (4), pp.288-290.
- [7] M. Tico, P.Kuosmanen and J.Saarinen. Wavelet domain features for fingerprint recognition, Electroni. Lett., 2001, 37, (1), pp.21-22.
- [8] L. Hong, Y. Wan and A.K. Jain, "Fingerprint Image Enhancement: Algorithms and Performance Evaluation", IEEE Transactions on PAMI, Vol. 20, No. 8, pp.777-789, August 1998.
- [9] Image Systems Engineering Program, Stanford University. Student project By Thomas Yeo, Wee Peng Tay, Ying Yu Tai.
- [10] L.C. Jain, U.Halici, I. Hayashi, S.B. Lee and S.Tsutsui. Intelligent biometric techniques in fingerprint and face recognition. 1999, the CRC Press.
- [11] M. J. Donahue and S. I. Rokhlin, "On the Use of Level Curves in Image Analysis," Image Understanding, VOL. 57, pp 652 - 655, 1992.
- [12] Jin Fei Lim; Chin, R.K.Y., "Enhancing Fingerprint Recognition Using Minutiae-Based and Image-Based Matching Techniques," Artificial Intelligence, Modelling and Simulation (AIMS), 2013 1st International Conference on, vol., no., pp.261, 266, 3-5 Dec. 2013.
- [13] Sudheesh, K.V.; Patil, C.M., "An approach of cryptographic for estimating the impact of fingerprint for biometric," Pattern Recognition, Informatics and Medical Engineering (PRIME), 2012 International Conference on, vol., no., pp.167,171, 21-23 March 2012.
- [14] Patil, A.R.; Zaveri, M.A., "A Novel Approach for Fingerprint Matching Using Minutiae," Mathematical/Analytical Modelling and Computer Simulation (AMS), 2010 Fourth Asia International Conference on, vol., no., pp.317,322, 26-28 May 2010.
- [15] Ito, K.; Morita, A.; Aoki, T.; Higuchi, T.; Nakajima, H.; Kobayashi, K., "A fingerprint recognition algorithm using phase-based image matching for low-quality fingerprints," Image Processing, 2005. ICIP 2005. IEEE International Conference on , vol.2, no., pp.II,33-6, 11-14 Sept. 2005.
- [16] Malathi, S.; Meena, C., "An efficient method for partial fingerprint recognition based on local binary pattern," Communication Control and Computing Technologies (ICCCCT), 2010 IEEE International Conference on , vol., no., pp.569,572, 7-9 Oct, 2010.
- Conference on , vol., no., pp.569,572, 7-9 Oct. 2010.
 [17] Liming Zhang; Yilong Yin, "Fingerprint Matching Based on Ternary Vector," Pattern Recognition, 2009. CCPR 2009. Chinese Conference on, vol., no., pp.1,5, 4-6 Nov. 2009.
- [18] Wen Wen; Zhi Qi; Zhi Li; Junhao Zhang; Yu Gong; Peng Cao, "A Robust and Efficient Minutia-Based Fingerprint Matching

Algorithm," Pattern Recognition (ACPR), 2013 2nd IAPR Asian Conference on , vol., no., pp.201,205, 5-8 Nov. 2013. Zin Mar Win; Sein, M.M., "Fingerprint recognition system for low

- [19] Zin Mar Win; Sein, M.M., "Fingerprint recognition system for low quality images," SICE Annual Conference (SICE), 2011 Proceedings of, vol., no., pp.1133, 1137, 13-18 Sept. 2011.
- [20] Kaur, R.; Sandhu, P.S.; Kamra, A., "A novel method for fingerprint feature extraction," Networking and Information Technology (ICNIT), 2010 International Conference on , vol., no., pp.1,5, 11-12 June 2010.



Mr. MAYANK TRIPATHY is studying M.TECH (IV SEM) in information Security in Disha Institute of Management and Technology, Raipur Chhattisgarh India. He has completed B.E. (Information technology) in session 2011-12 from K.I.T. Collage Raigarh (C.G.) university of Chhattisgarh swami Vivekananda technical university Bhilai (Chhattisgarh). His research interests are in Information and Network Security, genetic algorithm, Cryptography, artificial intelligence, Digital Signal Processing and Image Processing.



Mr. Deepak Shrivastava received his M. Tech. in Information Security, Branch of Computer Science and Engineering degree from Disha Institute of Management and Technology, Raipur, Chhattisgarh, India, affiliated to Chhattisgarh Swami Vivekananda Technical University, Bhilai, Chhattisgarh, India in 2014 and Master in Computer Applications (MCA) degree from Indira Gandhi National Open University in 2008. He is Assistant Professor, Department of Computer Science and Engineering in Disha Institute of Management and Technology, Raipur, Chhattisgarh, India. His research interests are in Information and Security, Cloud Network Computing. Cryptography, Artificial Intelligence, Digital Signal Processing and Image Processing.