IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-8, Aug 2018 E-ISSN: 2347-2693

Data Encryption Standard Algorithm in Multimodal Biometric Image

Sharmila S.More[1*], Bhawna Narain[2], B.T. Jadhav[3]

[1,2]MATS School of Information Technology, MATS University, Raipur, India
[3]Dahiwadi College Dahiwadi, Maharashtra, India

[*]*Corresponding Author: sharmilamore22@gmaill.com, Tel.: 9765370563*

Available online at www.ijcseonline.org

Accepted: 16/Aug/2018, Published: 31/Aug/2018

***Abstract*—** In every field of technology there are major issues of security. Biometric images are used as input and then the features like edge, texture are extracted. This is done by applying feature extraction algorithms and data encryption standard cryptographic algorithm on Fingerprints, Iris, face and palm simultaneously. In this paper we have explained the information about multimodal biometrics, DES algorithm, and role of DES in multimodal. We have discussed the implementation of DES algorithm by using MATLAB on parameters of captured images according to age and gender. Parameters such as key size, input size, time taken, simulation, memory requirement, CPU usage. Matching algorithm, time delay, FAR, FRR is also a major issue in multimodal biometrics.

***Keywords*—** Cryptographic algorithm; Biometric traits; FAR, FRR; Data Encryption Standard; Cipher Text.

I. INTRODUCTION

Biometrics or biometric authentication is the process used in computer science for identifying the authorized user by using their characteristics. It is also used to identify individuals in groups. Identifying the people by using their physiological and behavioral characteristics is the emerging trend in the modern era (Sharmila Shinde ***et al.***., 2014). There is lots of technical difference between every biometric type is as follows (Sharmila More ,B.Jadhav, 2017):

- To identify the person using hand recognition system we measure shape of the hand.
- In Iris recognition system we analyzing features of colored ring of the eye.
- In Retinal recognition system, analyzing blood vessels in the eye of person.
- In Vascular recognition system we analyze the vein patterns of person.
- Genetic markup is measured in DNA recognition system.
- Vocal behavior is measured in Speaker or voice recognition system.
- The time spacing of typed words is measured in Keystroke recognition system.
- Shape of the eyes, eyebrows, nose, lips etc measured in Facial recognition system.

Multimodal biometrics:

Multimodal biometrics is based on combination of more than one type of biometric modalities or qualities. Advantages of a multi-modal biometric system are higher accuracy, security, universality and cost-effective etc.The goal of multimodal biometrics is used to reduce the biometric parametric errors I.e. False Accept Rate (FAR), False Reject Rate (FRR) and Failure to Enroll Rate (FTE).

In Multimodal Biometric System Fusion can be done by four levels and these are Sensor Level, Feature Level, Matching Score Level and Decision Level. In sensor Level biometric characteristics are coming from sensor level. Feature Level fusion on signal coming from different biometric channels is first proposed and features vectors are extracted separating. In Matching Score Level combining the feature, we process them separately and individual matching score is found. And lastly at decision Level-each modality is first pre-classified independently. The final classification is based on the fusion of the output of the different modalities. Multibiomtric system may be Multi algorithmic, Multi-instance, Multi-sensorial.We use this image by era (Sharmila More, B.Narain ***et al.***., 2017).

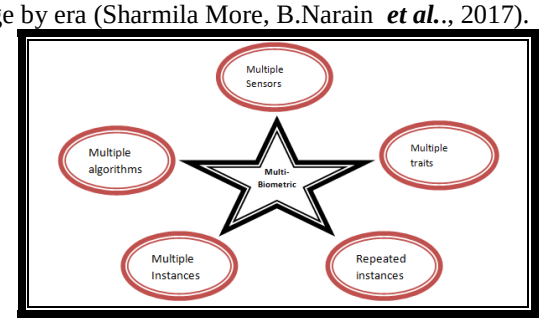

Figure1. Classification of multimodal biometric system

DES

Data Encryption Standard is a symmetric key algorithm who encrypts the electronic data. The DES has 64 bits block size but this algorithm actually uses 56 bits for encryption process and 8 bits are used for parity checking. The algorithm gives 16 rounds of completing its task. The number of counts of rounds used in feistel cipher depends upon required security from the system. If process uses more number of rounds then it provides more security, but one drawback is that the system becomes slow.These algorithm is already developed and also applying encryption on image (Sanjay Kumar ***et al.***., 2014)

The Algorithm has following features:

-The DES algorithm have a high security level related to a small key and same key used for encryption and decryption

-The DES algorithm can be easily understood

-It is not depend on the algorithm's confidentiality

-It is flexible and reasonable.

-It can be well-organized and exportable.

Encryption and decryption process of DES algorithm uses the same structure, but key used in reverse order and because of that we use one hardware and software for both direction of processing. The combination of substitutions and permutations is called as product cipher.

II. ROLE OF MULTIMODAL BIOMETRICS IN DES

Cryptography is becoming an increasingly important feature of computer security (B.Kiran Bala ***et al.***., 2014).Proposed method gives the security to the whole system by using fingerprint, face, Palm and face features as a key in a cryptosystem. In the proposed model we use multimodal biometric features. Biometric template protection is one of the important issues in deploying a practical biometric system. To tackle this problem, many algorithms have been reported in recent years, most of them being applicable to using fingerprint, face, Palm and face biometric. Since the contents and representation of every template is different than other .The template protection algorithm of one biometric trait cannot be directly applied to other. Moreover, we believe that no single template protection method is capable of satisfying the diversity, revocability, security and performance requirements (B.Kiran Bala ***et al.***., 2014). Data fusion is the process of integrating multiple data sources to produce more consistent, accurate, and useful information than that provided by any individual data source

III. DES ALGORITHM FOR IMAGE PROCESSING

The algorithm consist combinations, permutations and substitution between the images to be encrypted and the key is applied on both the encryption & decryption process. The DES has 64 bits block size but this algorithm actually uses 56 bits for encryption process and 8 bits are used for parity checking. The algorithm gives 16 rounds of completing its task.

We denote K1 ---- K16 = Keys applying on each round simultaneously

We divide data in two parts i.e. Left Side and Right side

Li= Left side and Ri= Right Side

DES Algorithm:

These algorithm is already developed we apply this on multimodal biometric images.[

The algorithm works in following ways

Step 1: Input Data in 64 bit plaintext.

Step 2: Using Initial permutation of blocks.

Step 3: In encryption stage we divide the blocks into two parts: left and right Li and Ri.

Step 4: Using formula in each round-

Li = Ri-1

Ri = Li-1 XOR F (Ri-1, Ki)

Step 5: Permutation and substitution steps repeated 16 times.

Step 6: Then in decryption process the left and right parts is inverse and we give Final permutation.

Step 7: 64-bit Cipher Text Data.

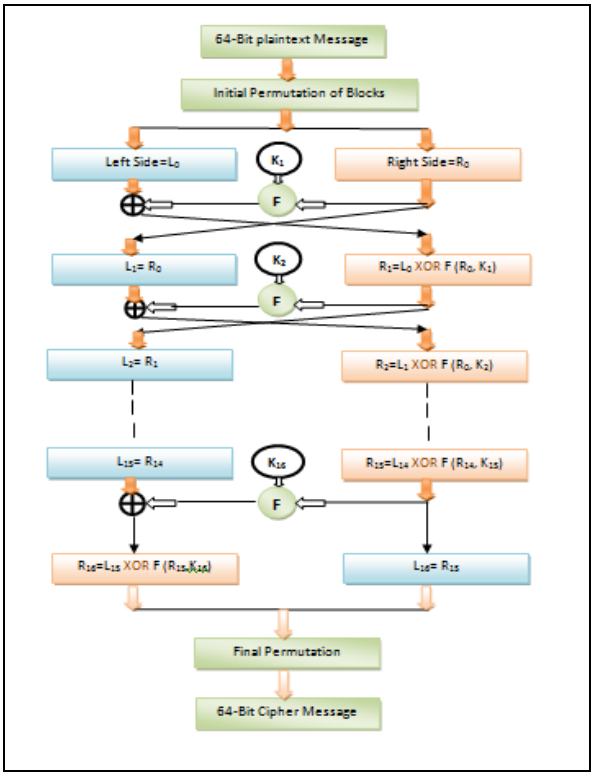

Figure 2. Working of DES algorithm

The above figure 2 explain the working of DES algorithm and figure 3. Define how DES key will be generated.

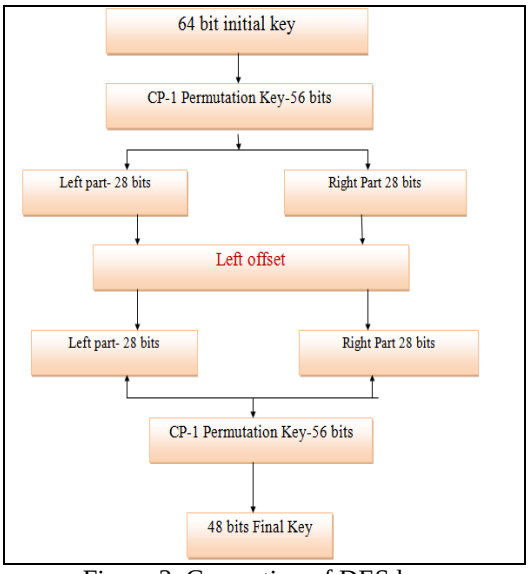

Figure 3. Generation of DES keys

IV. IMPLEMENTATIONS OF DES USING MULTIMODAL BIOMETRIC IMAGES

1. We will create the Image Data set according to Age and Gender. In that we will group age and gender as
   a. Age: 10-20, 21-30, 31-40, 41-50, 51-60 & 61-70.etc
   b. Gender: F- Female & M-Male
2. We are applying algorithm on 5 data sample images.
3. Then we compare training set with Test Data set and find out personal identification.
4. Sample Data set Encrypted Data set of Fingerprint:

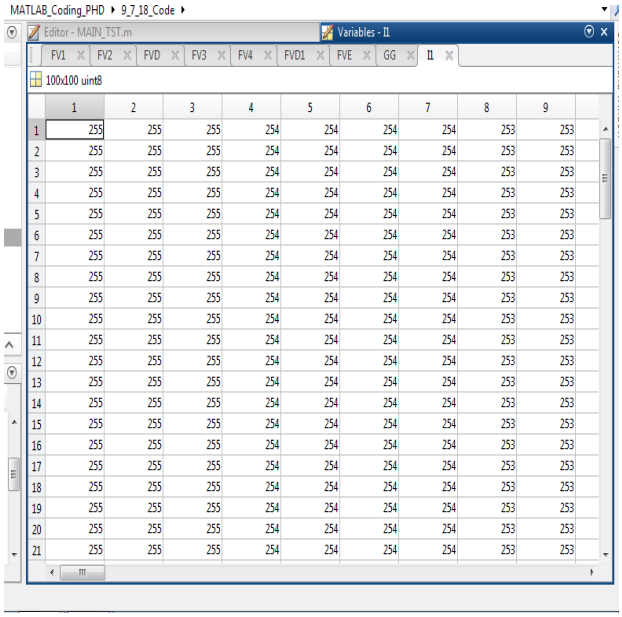

Figure 4. Encrypted Data set of Iris Decrypted Dataset

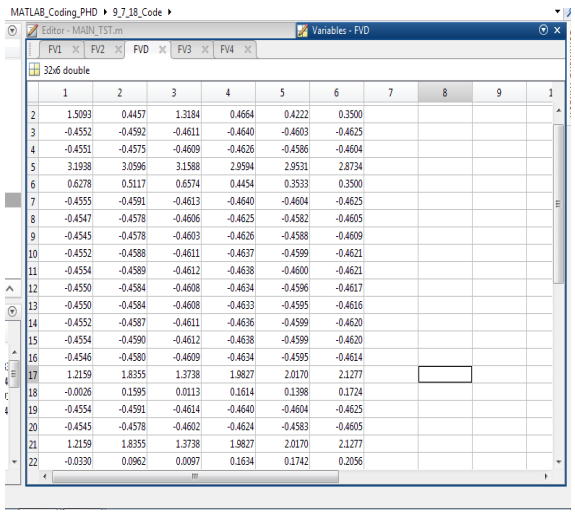

Figure 4. Decrypted Data set of Iris

Encrypted data set of palmprint:

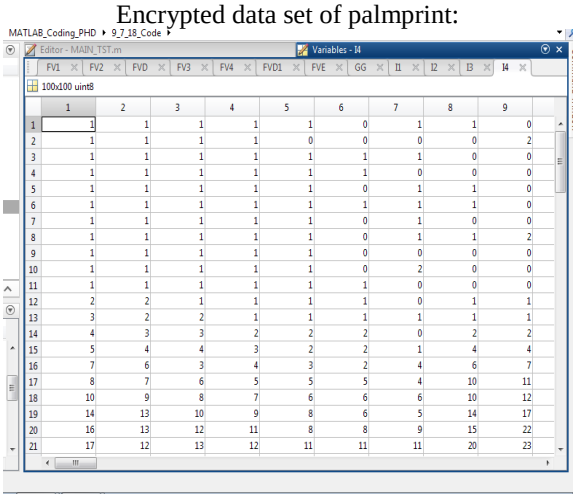

Figure 5. Encrypted data set of palmprint

Female Data Set

Age Group	Personal Identity No	Fingerprint	Iris	Face	Palm
10-20	P101	1 0 1 1 1 1 1 1 . . N	1 0 1 1 1 1 1 1 . . N	1 0 1 1 1 1 1 1 . . N	1 0 1 1 1 1 1 1 . . N
21-30	P102				
31-40	P103				
. . 61-70	. . .	. . .	. . .	. . .	. . .

Table-1: Female Data Set

Male Data Set

Age Group	Personal Identity No	Fingerprint	Iris	Face	Palm
10-20	P101	1 0 1 1 1 1 1 1 . . N	1 0 1 1 1 1 1 1 . . N	1 0 1 1 1 1 1 1 . . N	1 0 1 1 1 1 1 1 . . N
21-30	P102				
31-40	P103				
. . 61-70	. . .	. . .	. . .	. . .	. . .

Table-2: Male Data Set

Expected Outcomes- Find the perfect match and display ID number of that person.

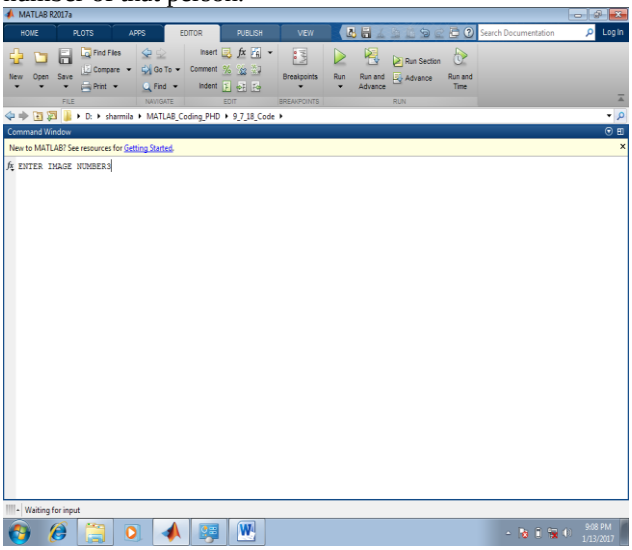

Figure 6. Expected outcome In real time implementation of DES algorithm we refere (B.Rajesh ***et al.***., 2008)

V. METHODOLOGY

Proposed Architecture: The multi modal biometric system designed consists of six modules as in figure 1.

- Fingerprint analysis module.
- Iris analysis module.
- Palm print analysis module.
- Face analysis module
- Conversion and Fusion.
- DES Encryption/Decryption module.

Generation of secure biometric keys with the help of multi-modal biometrics such as iris, fingerprint, face and palm print is done as shown in figure 1

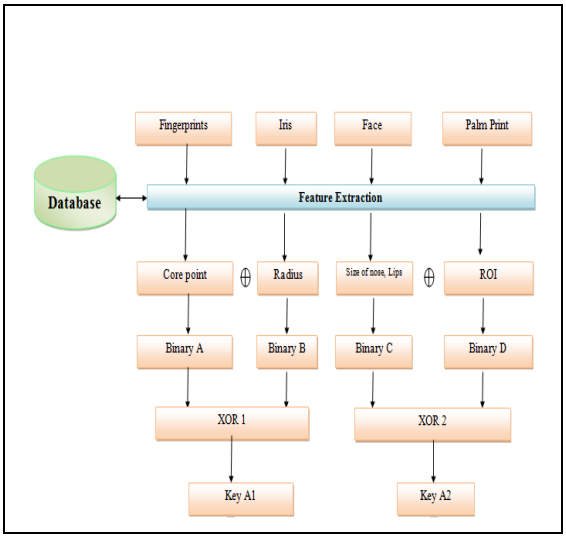

Figure7: Generation of Secure biometric keys

Module Implementation:

The minutiae points are extracted from fingerprint image, texture features from iris image , ROI score from palm print and shape of the eyes, eyebrows, nose, lips etc measured in facial recognition system which are are generated by biometric system. The features are now converted into respective decimals. The decimals are converted into binaries and all the four binary follows XOR operation to generate combined cryptographic key. The key is later compressed to Hexadecimal value which can act as encryption key. The encryption key is now used for DES encryption and decryption process. Again encryption and decryption is followed based on the two ciphers generated

Module 1: Biometrics Sensing

This module helps to recognize the biometric information of the users via sensors, camera.

- Images are generated which are further passed to module two for evaluation.
- The Module helps to collect the information of human biometrics
- The information to be collected are- Fingerprint, Palm print, Iris and Face.

Module 2: Pre-processing -Feature Extraction Description (Teena Joseph ***et al.***., 2016,)

- It helps to extracts the features from human biometrics in order to generate biometric key
- The features are extracted in form of decimals which are then used to convert binary value
- Different techniques are followed for each biometric
- At first the image is enhanced, followed by thinning, segmentation.

Module 3: Normalization and Fusion Description
(Teena Joseph ***et al.***., 2016,)

- This module helps to normalize the data or information gathered in form of features to the type which can be used to create or generate key.
- The features are then fused by following the XOR operation of the biometric values obtained.

Module 4: Generation of Keys Description

- The above module and the current one are integrated to generate binary biometric ciphers key
- The two binary keys generated are then considered as input to next module of encryption.

Module 5: DES Encryption and Decryption Description

- The module follows the process of encryption and decryption by using DES encryption process.
- The binary keys generated from the above module are passed as inputs to generate encrypted ciphers.

VI. RESULTS AND DISCUSSION

Analysis of about 5 different samples is followed and detailed evaluation can be seen from the table All the features are extracted and normalized in form of binary values which later follows the proposed algorithm. All the values are pass as input to the proposed technique which provides better security due to 4 levels of multimodal biometrics. This paper combines the scores based on fusion of Iris, Fingerprint, face and Palm print data to generate biometric cryptographic keys.

The analysis is done and it provides information about the performance and calculates approximately measures of the combined biometric techniques. The Iris, Fingerprint, face and Palm print data are collected from about 5 individuals and used for evaluation. Scores for each biometric trait are generated respectively. The calculation of analysis parameters such as key size, input size, time taken, simulation, memory requirement, CPU usage are estimated and also FAR, FRR .

The biometrics features for Iris, Fingerprint, face and Palm print are collected separately according to age and gender. Then, scores are obtained followed by the fusion technique discussed. The table provides the comparative analysis of parameters such as key size, input size, time taken, simulation, memory requirement, CPU usage and respective results are observed.

Graphical representation of multimodal images:-

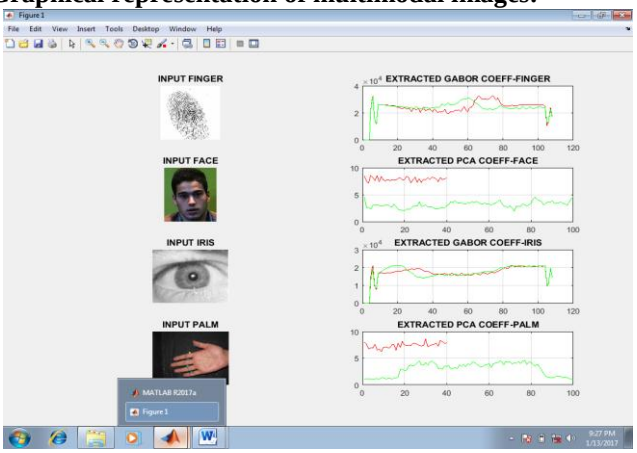

Figure 8. Graphical representation of multimodal images

VII. CONCLUSION

In these paper we had already discussed the security issues of multimodal biometrics of existing system, has been overcome in the proposed system and give more security in the biometrics .Existing cryptographic DES algorithm applying on the multimodal biometrics and checking the performance which is medium and then compare to the proposed system methodology as well as algorithm by the experimental results and tabulations justify the results. In future trying to implement on large dataset and for different cryptographic algorithm RSA, AES, Blowfish, M-RSA and proposed Hybrid algorithm ,that algorithm can be implement and matching algorithm time taken should be minimize and try to avoid the false acceptance rate and false rejection rate in the system. And comparing the parameters analysis of these algorithms with proposed hybrid algorithm.

REFERENCES

[1]. Abhishek Sharma, Narendra Kumar ,"Encryption of Text Using Fingerprints as Input to Various Algorithms", International Journal of Science and Research (IJSR), Volume 3 Issue 4, April 2014, ISSN (Online): 2319-7064, pp. 418-421.
[2]. Bk. Bala and Jl. Joanna, "Multi Modal Biometrics using Cryptographic Algorithm," Eur. J. Acad. Essays, vol. 1, no. 1, pp. 6–10, 2014.
[3]. B.Rajesh , G.S.Rath, "Real Time Implementation Of DES Algorithm By Using Tms3206713 DSK " National Institute Of TechnologyRourkela 2008.
[4]. Burrows M. and D. Wheeler, "A block-sorting lossless data compression algorithm," Algorithm, Data Compression, no. 124, p. 18, 1994.
[5]. C. M. Bishop, Pattern Recognition and Machine Learning, vol. 4, no. 4. 2006.
[6]. Ieee, "IEEE Standard Specifications for Public-Key Cryptography," IEEE Std 1363-2000. p. i, 2000.
[7]. D. G. Lowe, "Object recognition from local scale-invariant features," in Proceedings of the Seventh IEEE International Conference on Computer Vision, 1999, pp. 1150–1157 vol.2.

[8]. Lumini and L. Nanni, "Overview of the combination of biometric matchers," Information Fusion, vol. 33. pp. 71–85, 2017.
[9]. S. S. More, B. Narain, and B. T. Jadahv, "A Comparative Analysis of Unimodal and Multimodal Biometric Systems," in International Conference (ITESM-2017) On Innovative Trends in Engineering Science and Management, 2017, vol. 8, no. 5.
[10]. S. S. More. and B. T. Jadhav, "Comparative Study of Biometric Devices," Int. J. Innov. Res. Comput. Commun. Eng., vol. 5, no. 2, pp. 1302–1309, 2017.
[11]. S. S and S. Mathew, "Multimodal Biometric Authentication : Secured Encryption of IRIS Using Fingerprint ID," Int. J. Cryptogr. Inf. Secur., vol. 6, no. 3/4, pp. 39–46, 2016.
[12]. Sanjay Kumar , Sandeep Srivastava ," Image Encryption using Simplified Data Encryption Standard (S-DES) ", International Journal of Computer Applications (0975 – 8887) Volume 104 – No.2, October 2014.
[13]. S. S. More and B. T. Jadahv, "FUZZY LOGIC ALGORITHMS FOR EXTRACTING BIOMETRIC DATA," in National Conference on Modern Approach for Green Electronics & Computing 29th and 30th September 2014 (MAGEC 2014) ISBN : 978-81-928732-2-0, 2014, pp. 200–204.
[14]. S. S. More and B. T. Jadahv, "An Overview on Technologies Used in Biometric System," Int. J. Innov. Res. Comput. Commun. Eng., vol. 4, no. 2, pp. 365–373, 2016.
[15]. S. S. More, "Biometrics: Overview and potential use for E-Governance Services," Int. J. Adv. Res. Comput. Sci. Softw. Eng., vol. 4, no. 6, pp. 1145–1151, 2014.
[16]. Sharmila Shinde, J. Shinde, Kharade M and Kadam D. "Biometrics: Overview and potential use for E- Governance Services," Int. J. Adv. Res. Comput. Sci. Softw. Eng., vol. 4, no. 6, pp. 1145–1151, 2014.
[17]. Odinaka, P. H. Lai, A. D. Kaplan, J. A. O'Sullivan, E. J. Sirevaag, and J. W. Rohrbaugh, "ECG biometric recognition: A comparative analysis," IEEE Trans. Inf. Forensics Secur., vol. 7, no. 6, pp. 1812–1824, 2012.
[18]. R. Patil and M. a. Zaveri, "A Novel Approach for Fingerprint Matching Using Minutiae," Math. Model. Comput. Simul. (AMS), 2010 Fourth Asia Int. Conf., 2010.
[19]. Rupam Kumar Sharma , Generation of Biometric Key for Use in DES, https://arxiv.org/ftp/arxiv/papers/1302/1302.6424.pdf ,Bosco College Of Engineering and Technology, Assam India.
[20]. Teena Joseph, Latha Parthiban, "Multimodal biometric based authentication for ensuring data security in Cloud Computing ", Journal of Chemical and Pharmaceutical Sciences, Volume 9 Issue 4 , 2016, ISSN: 0974-2115.
[21]. Wayman J., Biometric Systems: Technology, Design and Performance Evaluation. 2005.
[22]. William E. B, C. Barker, "Data Encryption Algorithm," Recomm. Triple Data Encryption Algorithm Block Cipher, no. January, 2012.

Authors Profile

Ms Sharmila S. More

Ms Sharmila S. More is Research Scholar of Ph.D(Computer Science) in MATS School of Information Technology, MATS University, Raipur and Assistant Professor in Department of Animation Science , Y.C.I.S. Satara. I have published 8 research papers during 2013-18 in National & international conference and international journals. I awarded as Best Teacher award in 2015 at the YCIS Satara. My Citation Index is -14.

Dr. Bhavana Narain

Dr. Bhavana Narain as Associate Professor in MSIT Department pf MATS University, Raipur , CG. Ph.D(Computer Application), M.Phill(Computer Science). Her work experience is 15 years .Her area of interest is computer networks(adhoc, mesh) and Digital image processing. She has published 41 papers in national and international journals and conferences. Two books are aslo published, she has worked as Co-pi in two minor projects. She has been working as state student coordinator of Computer Socitey of India and awardd as Best Teacher and Researcher by National organization.

Dr. B.T.Jadhav

Director of Rayat Institute of Research and Development Satara, Maharashtra. He is a recognized Research Guide for Computer Science and Electronics at Shivaji university Kolhapur. He has published 163 research papers during 2004- in national and international journal and conferences. Ph.D. completed students are- 4 and Guiding for- 6 students. He is also worked as Ph.D. referee for Pune Kolhapur Solapur and Bombay University.

