ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 2, February 2014

Secure Transmission of Medical Images through Biometric Identification

R.SARANYA[1], Dr.R.MEENAKUMARI[2]

Assistant Professor, Department of ECE, KPR Institute of Engineering and Technology, Coimbatore, India[1]

Professor, Department of EEE, Kongu Engineering College, Perundurai, Erode, India[2]

Abstract: In the fastest digital world, people have much less time to consult a doctor in person for their health monitoring. It is easier for them to communicate in digital mode by using internet, web services, video or tele-conferencing, etc. But the communication between a patient and doctor must be confidential; While Internet is a wide open source, there may be some brutal attacks like hacking of information which are sent through e-mails. To make the communication or transmission of information in a secured manner, the user needs a Security algorithm for information which he/she wants to send over internet. That information may be text, image, audio or video. This article suggests an image authentication algorithm for providing security to medical images along with end user's security ensured by using biometric identification. Cryptography based image authentication method is implemented and facial features are used as biometrics parameters.

Keywords: Biometric Identification, Correlation coefficient, DCT, ELM, Face recognition, FAR, FRR, Image authentication.

1. INTRODUCTION

In the fast evolution of digital data exchange, security of any information becomes vital in data storage and transmission. Due to the increasing use of images in various fields, it is essential to protect the image data confidentially from unauthorized access. Medical imaging is one of the popular application areas of image processing field. To ensure confidentiality of medical images that are sent over wireless channel, many security techniques like cryptography, watermarking, steganography, etc., are available.

1.1 Cryptography

Cryptography is the study of hiding information using secret keys and sent via wireless channel. Information may be text, number, image, audio or video. Various types of cryptography include 1) Public key cryptography (RSA, McEliece) or asymmetric key cryptography that uses two keys - public and private keys, 2) Secret key cryptography (DES, AES) uses one key that is shared by both sender and receiver. If this key is disclosed, communications are compromised and insecure and 3) Hash functions uses single key and used for encryption.

Image encryption and decryption has applications in various fields including internet communication, multimedia systems, medical imaging, tele-medicine and military communication.

Discrete Cosine Transform based private key cryptosystem involves transformation of input image and cipher image into frequency domain and sent over internet. Decryption of original data from the cipher is easily applicable for the receiver.These techniques provide security to images from hackers over the channel but there is no security at the end user's side. Hence anybody can send or receive those images.

1.2 Biometrics

Biometrics refers to automatic systems that use measurable, physical or physiological characteristics or behavioral traits to recognize the identity, otherwise to verify or authenticate the claimed identity of an individual. Biometric identification is an actively growing area of research and is widely used in application fields like E-commerce, E-banking, E-passports, E-licenses and security applications like Border Security control, Crime prevention / detection and Forensics, Attendance recording , payment systems and Access control. It includes fingerprint, iris, face, voice, palm symmetry, hand geometry and so on. Biometric identification has significant advantages over other authentication techniques because biometrics characteristics are not easily modifiable and are unique.

Fingerprint recognition has been widely used because it is cost affordable and best utilized in small-scale verification systems. This recognition method finds applications in mobile phones, computers, Employees identification scheme, etc. But this method encounters problems like some fingerprints are unsuitable for use due to cuts or other defects. Also artificial finger straps are readily available in the market makes the recognition process difficult or identifying the wrong individual. To overcome the difficulties in fingerprint recognition, some other methods are suggested.

Iris recognition has evolved in recent years which eliminate the problem in fingerprint mechanism. The accuracy and speed of iris systems allows this technique implementing in a large scale system. The iris of each person is distinctive and even identical twins have different patterns. Since it is extremely difficult to alter the texture of the iris through surgery, it would be difficult for someone to provide wrong identifications. Also it is relatively easy for the system to detect when an artificial iris specially made by contact lens, is being used to gain identification. But iris recognition also encounters some difficulties in the verification applications. To overcome such difficulties in iris recognition techniques, Face

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 2, February 2014

recognition comes into existence in the modern world of artificial intelligent systems.

1.2.1. Face Recognition

Face recognition field has achieved a significant growth over the past few years. It is the popular area of research for more than 3 decades in computer vision and the most successful applications of image analysis. Several companies offer face recognition software that can produce high-accuracy results with a large database. Recent research involves developing techniques that accounts for changes in lighting, expression, and aging, for a given person. Also, researches under this field include dealing with glasses, facial hair, and makeup.

Two predominant approaches in face recognition system are geometric feature- based and appearance-based. The geometric feature based approach uses the properties of facial features such as location of eyes, nose, mouth, chin and their relations for face recognition descriptors. The appearance-based face recognition approach operates directly on image based representation. The whole face region is the raw input to a recognition system and the facial features are processed as templates.

Face recognition is commonly used in two ways, Face identification and Face verification [8]. Identification refers to the ability of a computer system to uniquely distinguish an individual from a larger set of individual biometric records on file. The presented biometric data would simply compared with all other entries in the database for a match, and upon a successful match the associated identity data would be released from the database. This is often called as a one-to-many match, and is used by police to identify criminals on watch lists, as well as by governments to identify qualified recipients for benefit-entitlement programs and registration systems such as voting, driver's license and other applications. Biometric verification or authentication involves a one-to-one search whereby a live biometric sample presented by a person is compared to a stored sample in a database previously given by that individual, and the match is confirmed. The eligibility of the person for the service or benefit has already been previously established. The matching of the live biometric to the sample is necessary to authenticate the individual as an eligible user. There need not be any search or matching to a central database, although a central database can still be used, provided that some other identification data is used.

1.3 Extreme Learning Machine

ELM is one of the virtual neural networks, provides less training time and high accuracy. It is a sequential learning algorithm where the training observations are sequentially used as single data block or data with varying or fixed length in the learning algorithm. At any time, only the new observations are seen and learned. The training data are discarded as soon as the learning procedure for that particular data is completed as in [4]. ELM requires less number training data to train a network. For a face recognition system, it just needs 4 parameters from a single face image to be taken.

In this article Section 2 provides an overview of existing methods, its merits and demerits. Section 3 deals with the proposed method of image security algorithm. Section 4 gives the results and discussions which are done using MATLAB tool. Section 5 deals with conclusion of the article.

2. LITERATURE SURVEY

Atefe Assadi and Alireza Behrad [1] proposed a method for Face recognition using Texture and depth information. This method provided a 3D approach for recognizing faces under pose variation and different illumination conditions. Scale-invariant feature transform (SIFT) descriptors are used to extract the facial feature points and compared with the database. They also calculated the matching points using SIFT feature vector. Input face image with maximum matching points is recognized as known face. This method provided 88.96% recognition rate.

Deo Brat Ojha et al [2] proposed an authenticated transmission of medical images over a noisy channel using codebase cryptography. For secure transmission, McEliece key cryptography was used for encryption. Then Sequitter compression was used for efficient use of bandwidth of the channel. Decryption was done at the receiver's side to get the image. This method was used to provide a fast encryption and decryption algorithm. But the keys sizes were larger in size, would make it as complex method.

Guang-Bin Huang et al [8] developed an online sequential learning algorithm for single hidden layer feed forward networks (SLFNs) with additive or radial basis function (RBF) hidden nodes. Here the training time got reduced results in high accuracy. This algorithm could be effectively used with small database and data could be included when needed. Input weights and biases were randomly generated and based on this the output weights were analytically determined. Other sequential learning algorithms needed many control parameters to be tuned but OS-ELM needed only the number of hidden nodes to be specified.

Ismail Amr Ismail et al [4] proposed a digital image encryption algorithm based on chaotic maps. In the encryption phase, the pixels were encrypted using an iterative cipher module based feedback and data-dependent inputs mechanism for mixing the current encryption parameters with previously encrypted information. To make the cipher more robust against any attack, the secret key was modified after encryption of each pixel of the plain image. If the secret key was modified, it was difficult to decrypt the original image as sent.

Ramesha K et al [10] proposed a Feature Extraction based Face Recognition, Gender and Age Classification (FEBFRGAC) algorithm. In this paper, recognition process was performed based on the geometric features based on the symmetry of human faces and the variation of gray levels, the positions of eyes, nose and mouth were extracted and located by applying the Canny edge operator. The gender was classified based on posteriori class probability and age was classified based on the shape and texture information using Artificial Neural Network. This algorithm provided face matching ratio is 100%, gender classification is 95%, and age classification is 90%.

Shermina J [11.a] proposed a face recognition system based on Multi linear principal component analysis

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 2, February 2014

(MPCA) and Locality preservation projection (LPP). In this paper, after face image preprocessing, dimensionality reduction is performed using MPCA. Features were extracted using LPP which provided nearest neighbor search in the low dimensional space. Recognition was performed by using L2 similarity distance measure, computed between the database image and the query image. High recognition rate was achieved by combining both the MPCA and LPP.

Shermina J [12.b] proposed a Face recognition system based on Discrete Cosine Transform (DCT) and PCA. In this research paper, low frequency DCT components are used to normalize the illuminated image. 64 illumination conditions are taken into account. This paper provided with accuracy of 94.2% and concluded that combination of DCT with any other recognition methods provided significant illumination invariant recognition accuracy.

Thamizharasi A [13] proposed a survey paper of Analysis on Face recognition by combining multi scale techniques and Homomorphic filter using Fuzzy k nearest neighbor classifier. In this paper, DCT and Discrete wavelet transform (DWT) were the two multi scale techniques used. Homomorphic filters were used for normalization of illumination. K means clustering algorithm was applied to group the pixels in the preprocessed image based on gray-scale threshold values. Fuzzy k nearest neighbor classifier was used to classify image in the test database by calculating the Euclidean distance matrix within the train database. DCT yielded 89.5% recognition rate while DWT yielded 90% rate with Homomorphic filter, K means clustering and Fuzzy k nearest neighbor classifier. The system became more complex because of more no. of techniques and also computation time would be more.

Zeghid M et al [15] proposed a modified AES based algorithm for image encryption. In this paper, Advanced Encryption Standard is used which would be a private key cryptosystem. AES was added with a key stream generator for improving the performance of efficiency. A better encryption result in terms of security against statistical analysis attacks was provided by W7 model key stream generator.

3. PROPOSED METHODOLOGY

This paper proposed a combined method of image authentication using biometric identification. Feature extraction based face recognition using ELM network is used for end user's security. The face recognition process will be used for end user security in many other authentication systems. Medical images are confidentially transmitted via wireless channel with higher level of security using various types of encryption/decryption algorithms. These algorithms avoid hacking of medical images while transmission across internet. But there is no security at the end user or receiver's side and thus anyone can receive the encrypted message. If the cryptographic algorithm will be private means the intruder can easily decrypts the message and gets the medical image. Hence it is necessary to provide authentication while transferring via internet. Face recognition algorithm is included at the end users side. Once the user gains the authority, he/she can transfer the images in a secured manner. The flowchart describes the proposed face recognition model will be shown in the figure1.

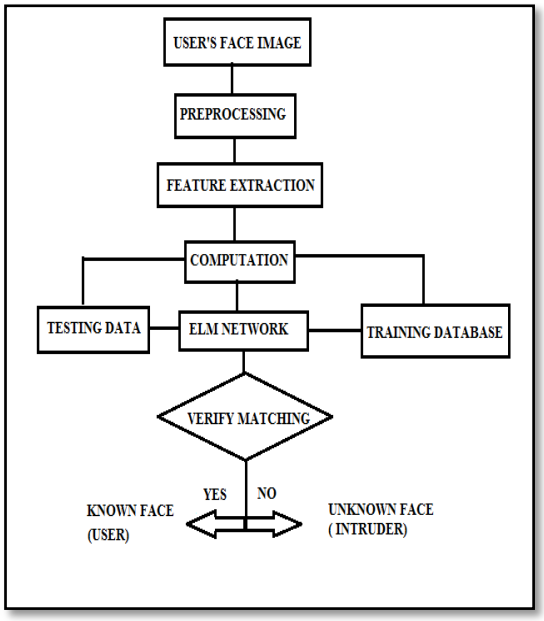
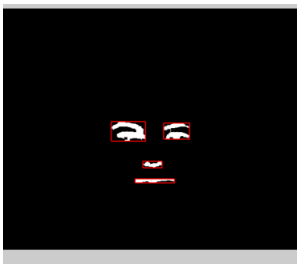


Fig.1 Face recognition model

3.1 Face Recognition Methodology

Initially an RGB color image of the user is captured using a web camera or high resolution video camera. The size of the face image is 640x480.The input face image is transformed into binary face image for retaining the important features. Background changes, illuminations are adjusted and concentrating on the face region alone. This process referred as Pre-processing for improving the quality of the image shown in the figure 2(a).

(a)



(b)

Fig.2 (a) RGB image of user1 and (b) Detected Regions with bounding boxes

*m-Male and f-female

Feature extraction is performed after pre-processing the input face image. The regions of two eyes, nostrils and mouth are located in the binary face image. Then the

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 2, February 2014

regions are represented within the bounding boxes and filled the disconnected pixels are shown in the figure 2(b). From the extracted regions, the following distances are measured in the face image. The distances are calculated by calculating centroid values of each bounding boxes.

Inter-Ocular Distance - The distance between the right eye and the left eye pixels.

Eye to Nose Distance - The distance between the midpoints of the line joining the eyes and the nose tip pixels.

Eye to Mouth Distance - The distance between the midpoint of the line joining the eyes and the center point of the mouth.

Nose to Mouth Distance - The distance between the nose tip and the center point of the mouth.

The above said distances are calculated from the face image and the ratios are calculated. These computed ratios are referred as features of the face image which are taken into account for recognition. The ratios are mentioned as follows,

1. **EENR** is Eye to Eye and to Nose Ratio and is the ratio between the Inter-ocular distance and the Eye to Nose distance.
2. **EEMR** is Eye to Eye and to Mouth Ratio and is the ratio between the Inter-ocular distance and the Eye to mouth distance.
3. **EENMR** is Eye to Eye and Nose to Mouth Ratio and is the ratio between the Inter-ocular distance and Nose to mouth distance.
4. **ENEMR** is Eye to Nose and Eye to Mouth Ratio and is the ratio between the Eye to Nose distance and Eye to mouth distance.

Similarly these ratios are computed for legitimate users and created as database. The table 1 shows the extracted features of the sample database images used in the recognition process.

The computed features from the face image are given as inputs to an extreme learning machine network. Number of hidden layer neurons alone is entered manually or it will be the sum of input neurons and output neurons. Input weights and biases are assigned randomly and from that output weights are calculated. The features are trained within the network for the given database. The query image is verified for matching purpose. If matching exists, the result shown as *KNOWN FACE* otherwise the result will be *UNKNOWN FACE*. Thus user verification is performed once the extracted features are matched with the database otherwise user cannot access the authority to use the resources. Figure 3 shows the simple architecture of ELM network.

TABLE.1 DATABASE FOR DIFFERENT FACE IMAGES

Face image	EENR	EEMR	EENMR	ENEMR
06-1m	1.1895	0.6548	1.4571	0.5505
11-1m	1.1602	0.8944	3.9055	0.7709
14-1f	1.4506	0.8730	2.1926	0.6018
15-1f	1.3810	0.9320	2.8666	0.6748
20-1m	2.8710	1.7429	4.4360	0.6070
21-1m	1.1133	0.6869	1.7936	0.6170
25-1m	1.4453	0.7610	1.6074	0.5265
28-1m	1.2863	0.8328	2.3626	0.6474
29-1m	1.3404	0.8107	2.0809	0.6048

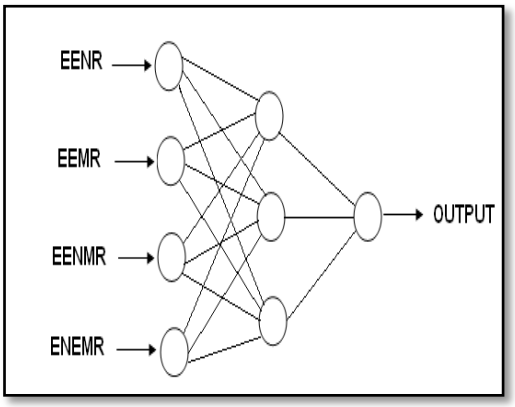


Fig.3 A simple ELM network

In this proposed method, 35 face images of different users are used for recognition purpose. Out of these 35 images, 9 images are taken as training data and remaining 26 images are taken for testing data. The accuracy or performance metrics of the biometric identification depends on two parameters, FAR and FRR.

False Acception Rate or False Match Rate (FAR or FMR) 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. False Reject Rate or False Non-Match Rate (FRR or FNMR) is the probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs which are incorrectly rejected.

3.2. Image Authentication method

After the user gains the authority to access the medical images, he/she may encrypt the medical image using key image. Encryption process is performed by using transform based private key cryptosystem. The medical image is first converted into frequency domain using Discrete Cosine Transform (DCT). Then recognized face image is also converted into frequency domain and used as key image. Cipher image is created by embedding the medical image with key image. This cipher image is sent over the internet through e-mail. At the receiver's side, similar method of face recognition is performed for verification. For decryption of cipher image, DCT key image is used to recover the original image by using inverse transformation. Thus the image security is achieved with biometric verification technique. Figure 4 shows the image authentication methodology.

3.2.1 DCT

DCT divides an image into non overlapping blocks, and apply a 2D DCT on each block to get its equivalent frequency coefficients. It is widely used in multimedia

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 2, February 2014

and imaging applications. It is the fundamental for JPEG Image Compression. It reduces the correlation between images hence used for hiding purposes. DCT can concentrate more energy in the low frequency bands than the DFT. It is cost effectiveness. Some of the application areas are JPEG Encoders, MPEG-1 & MPEG-2, Image & Pattern Recognition, Biomedical signals like EEG & ECG and Speech information compression. The implementation of 2D DCT and IDCT is given below,

$$F(u,v) = \frac{2}{N} C(u)C(v) \sum_{y=0}^{N-1} \sum_{x=0}^{N-1} f(x,y) \cos[\frac{(2x+1)u\pi}{2N}] \cos[\frac{(2y+1)v\pi}{2N}]$$

$$f(x,y) = \frac{2}{N} \sum_{y=0}^{N-1} \sum_{x=0}^{N-1} C(u)C(v)F(u,v) \cos[\frac{(2x+1)u\pi}{2N}] \cos[\frac{(2y+1)v\pi}{2N}]$$

$$where\ \mathrm{C(u)},\ \mathrm{C(v)} = \sqrt{\frac{1}{N}} \qquad u, v = 0$$

$$= \sqrt{\frac{2}{N}} \qquad 1 < \mathrm{u, v} < \mathrm{N} - 1$$

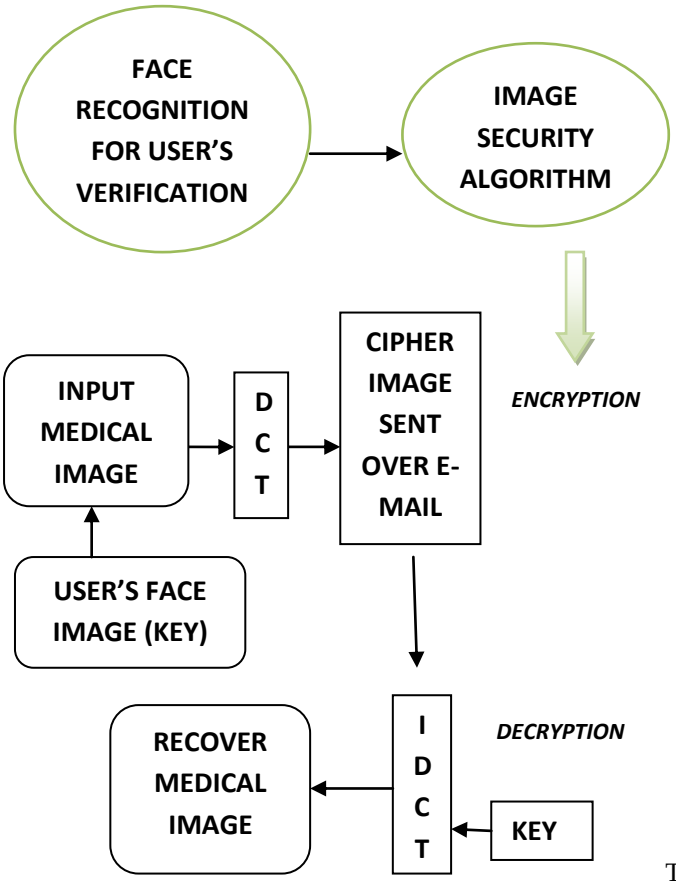
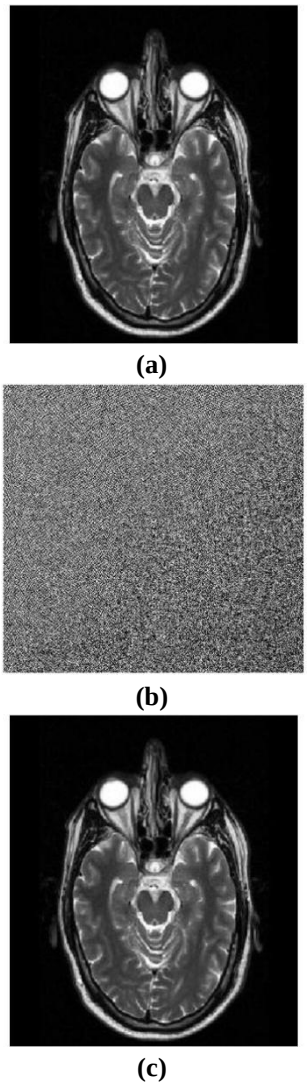


Fig.4. Image authentication model

4. RESULTS AND DISCUSSIONS

At the sender side, user verification is performed using Face recognition method then image encryption is performed using DCT based private key cryptosystem. The encrypted image is being sent over the internet through e-mail. At the receiver side, user verification is again performed using similar method of Face recognition. The received encrypted image is decrypted using the private key to regain the original medical image. Thus the medical image security is achieved through biometric identification. The parameter used to find the similarity between the input image and cipher image is Correlation coefficient. It is a measure of the strength of the linear relationship between two variables that is defined in terms of the (sample) covariance of the variables divided by their (sample) standard deviations. Based on the proposed image encryption algorithm, it yields correlation coefficient of *-5.0226e-005*.



(a) **(b)** **(c)**

Fig.5(a) Input medical image, (b) Encrypted image and (c) Decrypted image

5. CONCLUSION

The proposed face recognition method yields the best authentication system. This method is simple and efficient. It deals with pixel information rather than texture information hence the accuracy will be more. The use of ELM network for training and testing the database provides fast and accurate authentication system. The measured FAR is 3.85% and FRR is 0% hence the proposed face recognition system yields a better biometric identification system using ELM network. The proposed face recognition technique is implemented in secure

transmission of medical images at the end user's side. DCT based image authentication algorithm is widely used since it provides key based on biometric identification. It also provides better security to images.

REFERENCES

[1] Atefe Assadi and Alireza Behrad "A new method for human face recognition using texture and depth information", *IEEE transactions on Neural Network Applications in Electrical Engineering (NEUREL)*, pp. 201-205, 2010.

[2] Deo Brat Ojha, Ajay Sharma, Abhishek Dwivedi, Nitin Pandey, Amit Kumar, "An Authenticated Transmission of Medical Image with Codebase Cryptosystem over Noisy Channel", *International Journal on Advanced Networking and Applications* ,vol. 02, Issue: 05, pp. 841-845,2011.

[3] Deo Brat Ojha et al, "An Authenticated two-tier security on transmission of medical image using codebase cryptosystem over teeming channel", *International Journal of Computer applications*, vol.12-no.9, pp. 22-26,2011.

[4] Ismail Amr Ismail, Mohammed Amin, and Hossam Diab, "A Digital Image Encryption algorithm based A composition of Two Chaotic Logistic Maps", *International Journal of Network Security, Vol.11, No.1, pp.1-10*, 2010.

[5] Lala Krikor et al, "Image Encryption Using DCT and Stream Cipher", *European Journal of Scientific Research,* vol.32, No.1, pp-47-57, 2009.

[6] Mintu Philip and Asha Das, "Survey: Image Encryption using Chaotic Cryptography Schemes", *IJCA Special Issue on "Computational Science - New Dimensions & Perspectives" NCCSE*, 2011.

[7] Mohammad Ali Bani Younes and Aman Jantan, "Image encryption using Block based transformation Algorithm", *IAENG International Journal of Computer Science*, 2008.

[8] Nan-Ying Liang, Guang-Bin Huang, P.Saratchandran, and N. Sundararajan , "A fast and accurate online sequential learning algorithm for feed forward networks", *IEEE transactions on neural networks*, vol. 17, No. 6,2006.

[9] Panduranga H.T and Naveen Kumar S.K, "Hybrid approach for Image encryption using SCAN patterns and carrier images", *(IJCSE) International Journal on Computer Science and Engineering*,Vol. 02, No. 02, pp: 297-300,2010.

[10] Ramesha K et al, **"**Feature Extraction based Face Recognition, Gender and Age Classification"**,** *International Journal on Computer Science and Engineering (IJCSE)*, vol. 02, no.01S, pp.14-23, 2010.

[11.a]Shermina J, "Face recognition system using multilinear principal component analysis and locality preservation projection", *IEEE GCC conference and exhibition, Dubai, United Arab Emirates*, 2011.

[11.b]Shermina J , "Illumination invariant face recognition system based on Discrete Cosine Transform and Principal Component Analysis", *International Conference on Emerging Trends in Electrical and Computer Technology (ICETECT)*, pp. 826-830, 2011.

[12] Thamizharasi A, "Performance Analysis on Face recognition by combining multi scale techniques and Homomorphic filter using Fuzzy k nearest neighbor classifier", *IEEE International Conference on Communication Control and Computing Technologies (ICCCCT)*,pp. 643-650,2010.

[13] M.Turk and Pentland, "Face recognition using Eigen faces", IEEE International conference on Computer vision and pattern recognition, 1991.

[14] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki, "A Modified AES Based Algorithm for Image Encryption", International Journal of Computer Science and Engineering Vol.1, No. 1.

[15] Zixiang Xiong, Kannan Ramchandran, Michael T. Orchard, and Ya-Qin Zhang, "A Comparative Study of DCT- and Wavelet-Based Image Coding" , *IEEE transactions on circuits and systems for video technology*, vol. 9, No.1,1999.

[16] Face images databases from www.cs.cmu.edu/~cil/v-images/html and www.face-reg.org/databases/html. and Medical images from brain images: mr-tip.com, radiologyinfo.ca and breastimaging.cancer.gov