iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** IV **Month of publication:** April 2018

DOI: http://doi.org/10.22214/ijraset.2018.4429

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue IV, April 2018- Available at www.ijraset.com

Secure Transmission of Medical Images Using Elliptic Curve Cryptography with Multimodal Biometric Authentication

Dr. S. Batmavady[1], E. Alamelu[2]
[1]*Dept of Electronics and Communication Engineering*
[2]*(M.Tech) Pondicherry Engineering College, Pondicherry*

Abstract: ***The fastest growing trend in today's digital world is the use of telemedicine by health care professionals incorporating the latest technology to access, aid, decide, diagnose and treat the patients irrespective of the distance barriers. This in particular would help the rural communities where the immediate access to medical facilities are not available. Since, the information transmitted about the patients is to be maintained confidential, images and other data about the patients need to be encrypted to prevent hacking. To ensure the authentication of the user to access the database, password authentication followed by multimodal biometric fusion using finger vein and finger knuckle are incorporated in the proposed work. Further, authentication is strengthened by encrypting the fused image. The medical images are encrypted using Elliptic Curve Cryptographic (ECC) technique. Once the user is authenticated, he is allowed to access the medical image database***
Keywords: Biometric Authentication, Electronic Medical Information (EMI), Elliptic Curve Cryptography (ECC), Multimodal Fusion, Telemedicine

I. INTRODUCTION

Electronic Medical Information (EMI) or patient Health Information (PHI) is the interesting topic in digital medical information storage. Physicians sometimes need to access the information to make the best decision. Hospital management has to protect the confidentiality of medical records to prevent the misuse of data. If patients suspect any such misuse of their information they should contact the physicians or hospital management to prevent any such occurrences in future.

Radiological results such as medical data, ultrasound images and lab test results are increasingly being stored, viewed and transformed from one medical record database to another one, without implementing any security techniques. To increase the level of privacy and confidentiality of patient's information, challenges may arise in storage and transmission of medical information. It is necessary to implement the biometric security for accessing the medical database centre. The traditional security systems such as key, ID cards, token method and passwords are not sufficient enough to ensure tight security [1].

Biometrics is measuring the unique characteristics of a person used for personal identification and verification. Compared to other authentication techniques, biometric identification has significant advantages since the biometric characteristics are unique and cannot be easily modified.

The physical or behavioral traits such as fingerprint, iris, face, voice, signature, gesture, etc. must satisfy the essential properties such as universality, distinctiveness, permanence, collectability, accessibility and acceptability. These are the basic necessities to represent the rightful user to access the medical record database.

Biometric authentication can be divided into unimodal and multimodal biometric authentication systems. Unimodal biometric systems use a single biometric trait of the user for identifying and verifying the individual. Unimodal biometric identification system seems to be attractive, but there are lots of issues and challenges associated with it. It is not easy to implement the unimodal biometric system in large scale system or within a large population. Also, these unimodal systems are quite vulnerable against spoofing attacks.

In order to improve the performance and to overcome the problems associated with unimodal system, multimodal biometric system is employed, which involves simultaneous authentication of two or more biometric traits of the person for identifying the individual. Further, encrypting the biometric traits ensure that unauthenticated users cannot access the database. The authenticated users will have access to the encrypted medical record database.

Section II focuses on various biometric authentication techniques. Section III deals with encryption technique used for encrypting the fused biometric traits of authenticated users. Medical images are also encrypted using ECC. Section IV depicts the block

diagram and the various phases involved in the proposed work. Section V gives the analysis of the results obtained. Section VI ends with conclusion and future work.

II. BIOMETRIC RECOGNITION

Biometric refers to automatic technologies in measuring and examining physiological or behavioural characteristics like fingerprints, iris, voice patterns, facial patterns, and hand measurements [3].

Requirements of those characteristics are:

1) *Universality:* The characteristic should be present in every person.
2) *Distinctiveness:* The characteristic should differentiate any two persons.
3) *Permanence:* The characteristics should be sufficiently invariant over a period of time.
4) *Accessibility:* It should be easy to acquire (Collectability).

The steps involved in the biometric system are data acquisition, pre-processing, matching and decision making [9].

A. Various Methods of Biometric Recognition

A brief introduction to the commonly used biometrics is given below.

1) *Signature based recognition system:* It is a behavioural biometric that change over a period of time and also professional forgers may be able to reproduce signatures that forge the system.
2) *Voice based recognition system***:** The behavioural part of the speech of a person changes over a period of time due to age, ailments etc. Further, speech features are sensitive to disturbances like background noise etc.,
3) *Fingerprint based recognition system:* It is vulnerable to forgery because the fingerprints can be easily duplicated using gelatin gel [4].
4) *Iris based recognition system:* The iris texture carries very distinctive recognition. The acceptability of this biometric trait is limited [5].
5) *Palm print based recognition system:* It needs all the feature of a palm such as hand geometry, ridges, valley features, principal lines and wrinkles are to be combined by using a high-resolution palm print scanner [6].
6) *Face based biometric recognition system:* It has difficulty in recognizing a face from images captured as in the case of twin siblings [7].

B. Finger-Vein Recognition System

Finger vein recognition system is considered to be one of the best authentication technologies [8]. It involves the capturing of inner features of the finger and hence, duplication is difficult. It is a non-invasive technique, with less cost and also aids in easy capturing of the images.

1) *Features of Finger Vein Recognition System:* The finger vein recognition has some advantages over other hand-based biometric authentication techniques [10].

Finger vein capturing systems are compact contactless systems promising high degree of security since, these capture only the internal features of a live person and are difficult to tamper with.

C. Finger knuckle print recognition system

The pattern of texture present in the dorsal surface of finger knuckle region is rich in unique characters and has high capabilities to identify different individuals. Finger knuckle print identification plays a vital role in crime scene. Combination of finger knuckle print with finger vein pattern will make the finger vein pattern more beneficial than the normal finger vein pattern system [12].

D. LBP Based Recognition system

Features are extracted from the fused image based on LBP method. It is an ordered binary set values measured by comparing the centre pixel gray values with its neighbouring pixels. The LBP operator extracts the binary code of size M x N. This method is used to reduce the errors in extracting finger vein patterns.

LBP Code A denotes the LBP feature of fused image in the database and the LBP Code B denotes the LBP feature of input image. Then measure the dissimilarities between two binary patterns, using Hamming Distance (HD) formula,

$$HD = \frac{LBP\ CODE\ A \otimes LBP\ CODE\ B}{CODE\ LENGTH} \quad (1)$$

$\otimes$ is a Boolean function, used to perform exclusive-OR operation between two binary patterns, in equation (1).

III. CRYPTOGRAPHY

A. Purpose of Cryptography

In order to ensure the level of privacy and non-alteration of patient medical data's or images, cryptographic techniques are widely used by the hospital management.

Encryption of medical images involves transformation of medical information including image data, known as plain image into cipher image by using an encryption algorithm. The cipher image will be in unreadable form. It cannot be read by anyone without the knowledge of key. The reverse process of transforming cipher image to original image is based on some key value is known as decryption. Various goals of cryptography are to achieve confidentiality, data integrity, authenticity, non-repudiation and access control.

B. Types of Cryptography

Cryptographic technique protects the medical image data from unauthorized users when it is transferred from one place to another place over the transmission channel. Cryptographic techniques are classified into two main categories

1) Symmetric key cryptography
2) Asymmetric key cryptography

C. Security of Medical Images

For encrypting the sensitive medical images into an unreadable format, it is necessary to implement the image cryptography technique in health care system. Providing security to medical images is purely based on the following aspects:

The data should be protected from the unauthorized access to ensure confidentiality, so that only the authorized persons can access it.

The hospital management should ensure that they send only the exact information, without any modification. This is known as integrity.

D. Elliptic Curve Cryptography

Elliptic curve cryptography was introduced by Koblitz and Miller in 1985. It has some advantages over other public key cryptosystem. It provides same level of security as provided by RSA (Rivest Shamir Adleman) Algorithm [2] with smaller key size, thereby reducing storage and processing time.

Elliptic curve is a plane curve which consists of the points satisfying the equation (2). The general equation of an elliptic curve is given by,

$$y^2 = x^3 + ax + b \tag{2}$$

Where x and y are the points on the elliptic curve and a, b are the coefficients satisfying the following equation (3),

$$4a^3 + 27b^2 \neq 0 (mod\ P) \tag{3}$$

Here p is a modular prime integer. So, an elliptic curve consists of all the points satisfying the elliptic curve equation and along with the point at infinity.

E. Image Encryption Using ECC

The image file is considered as a stream of bits and then constructed into various forms of grids. Intensity value of the pixel is derived from every grid of the image. The intensity values are mapped into the point of elliptic curve. Now this point is encrypted using ECC and sent to the recipient. Receiver uses the decryption algorithm and recovers the points and original image.

ECC algorithm initially converts the source image file into binary values and then map accordingly. By using the binary values from image source file, square grid of size 32 X 32 is constructed and padding is done with 0 if necessary. Then every pixel of the grid with size 32 X 32 is mapped on elliptic curve.

Then the pixels are encrypted using ECC. Hence, an image is first transformed on EC and then encrypted using ECC. The decryption algorithm perfectly recovers the original image.

IV. BLOCK DIAGRAM OF THE PROPOSED WORK

The block diagram of the proposed work is depicted in Fig. 4.1.

A. Outline of various phases involved

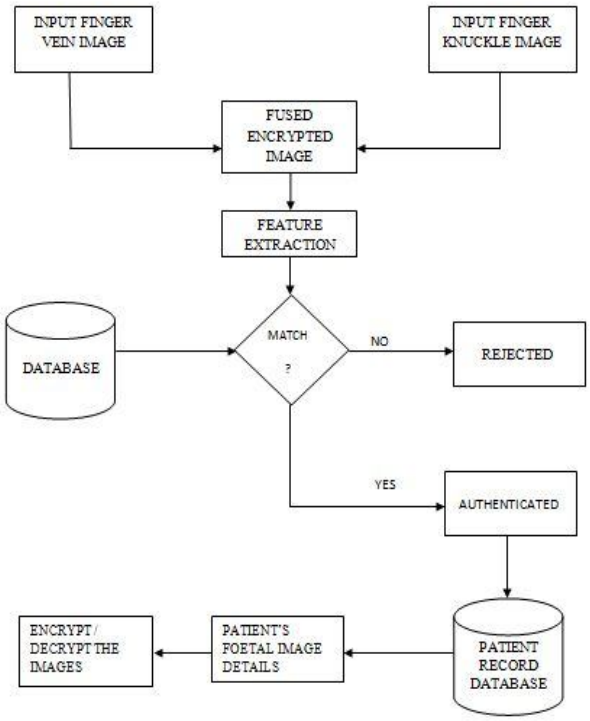


Fig. 4.1 Block diagram of the proposed work

1) *Data collection phase:* The finger vein and finger knuckle features of the doctors and the patients are collected in data collection phase. In the proposed work, the finger vein images are taken from MMCBNU_600 database [11] and the finger knuckle images are from Poly U FKP database.
2) *Fusion phase:* The acquired finger vein and finger knuckle images are fused. Then the fused image is encrypted using the image encryption algorithm. Features are extracted from the fused encrypted image and stored in the database by hospital management.
3) *Encryption phase:* Encrypting the patient's medical images using elliptic curve cryptography followed by storing in medical record database.
4) *Decrypting phase:* Decrypting the encrypted patient's medical images which are stored in the medical record database.
5) *Matching phase:* Comparing the biometric features of fused image with the existing details of images stored in database.

B. Pre-Processing Stages

The pre-processing operation mainly refers to image gray processing, ROI extraction, size normalization and gray normalization.

1) *Image gray processing:* The original colour images are first converted to gray scale image.
2) *ROI extraction:* It deals with the segmentation of the finger vein or knuckle region from the gray-scale image. The rectangular region can be captured based on the height and width of the finger region.
3) *Size Normalization:* There is a need to normalize the ROI region to the same size, because the size of the extracted ROI is different from image to image.
4) *Matching:* Matching is done by measuring the similarities between the extracted LBP feature of image in the database and the LBP feature of input image of a certain individual. The matching score (MS) is calculated as follows,

$$MS = 1 - \frac{LBP\ CODE\ A \otimes LBP\ CODE\ B}{CODE\ LENGTH} \quad (4)$$

$\otimes$ is a Boolean exclusive-OR operator between two binary patterns, in equation (4).

V. RESULTS AND DISCUSSIONS

Due to increasing occurrence of patient's medical record identity theft in most hospitals, it is necessary to implement the biometric recognition system for accessing patient's medical records in hospitals. Multimodal biometric recognition system plays a vital role in enhancing the security for retrieving patient's records and identification of patients in healthcare system [9]. This eliminates manual error and enhances the protection of medical record identity theft:

Finger vein recognition is considered as one of the most confidential biometric trait which is based on the images of human finger vein patterns below the skin's surface. Combination of finger vein and finger knuckle traits will give the best performance and less computational time. Because there is a known relationship between finger vein and finger knuckle biometric traits.

A. When the given input finger vein image and finger knuckle image is matched perfectly with the templates of images in database, then the user gains authentication and allowed to proceed into the system. The output, 'FUSED IMAGE IS MATCHED WITH THE DATABASE' is displayed in the command window.

B. If the given input finger vein image and finger knuckle image is not present in the database, then the user is denied to access the database and the output 'FUSED IMAGE IS NOT MATCHED WITH THE DATABSE' or 'UNKNOWN FINGER' is displayed in the command window.

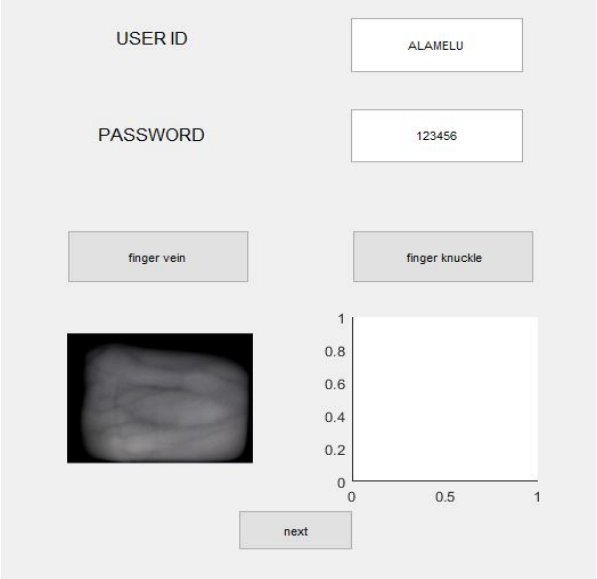


Fig. 5.1 Finger vein input image

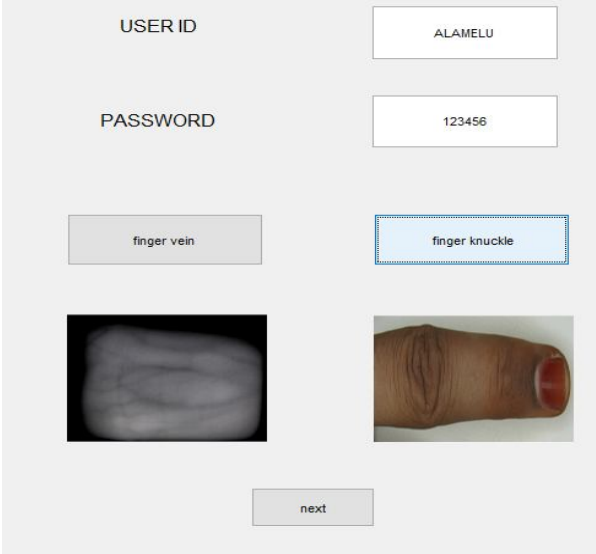


Fig. 5.2 Finger knuckle input image

Password security along with biometric fusion of finger knuckle and finger vein traits are used for valid authentication to access the system. Only when the entered user ID and password is valid, the user can further proceed into the system as shown in Fig. 5.1. The user can proceed into the system by acquiring their finger vein input image. After getting the input of finger vein image, the system will ask for the finger knuckle image of the same person as shown in Fig. 5.2.

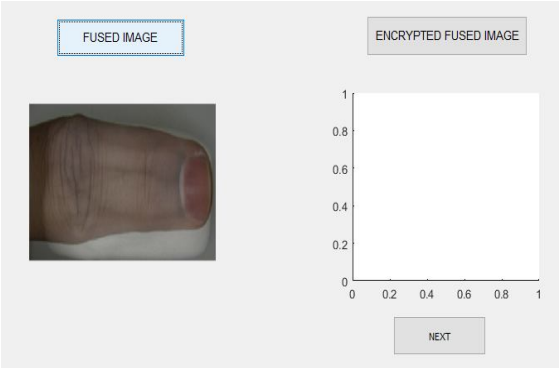


Fig. 5.3 Fused image

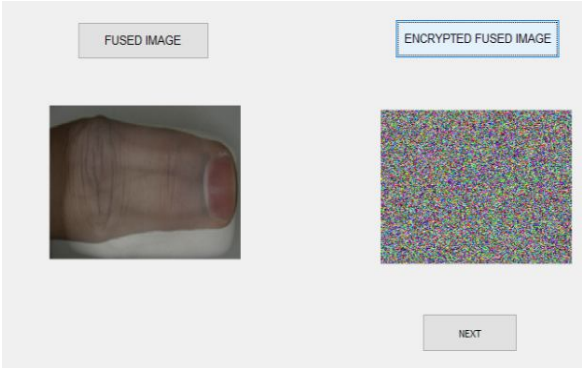


Fig. 5.4 Encrypted Fused image

After acquiring the finger vein and finger knuckle image from the same user, fusion is done between the acquired input images as shown in Fig. 5.3. Then the encryption is done with the fused image to ensure added security and the encrypted fused image is stored in the database as shown in Fig. 5.4.

Fig. 5.5 Fused image is matched

Fig.5.6 Fused image is not matched with database

Then the extracted features from fused encrypted image is compared with the features of existing images in the database

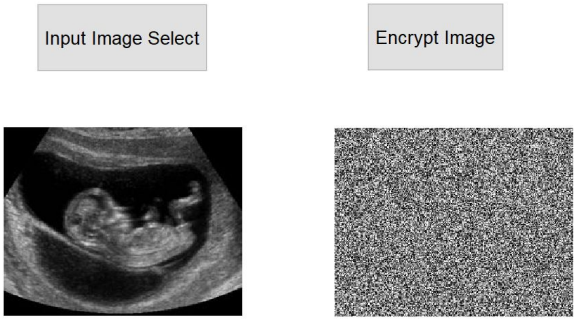


Fig. 5.7 (a) Encrypting medical image

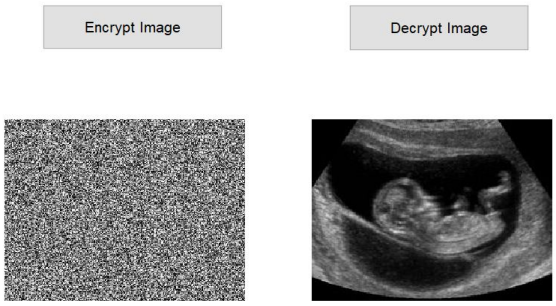


Fig. 5.7 (b) Decrypting medical image

When the matching is perfect, “FUSED IMAGE IS MATCHED WITH DATABASE” is displayed in the command window. The user gains authentication and “ACCESS GRANTED” is displayed in the command window as shown in Fig. 5.5. When the fused image is not perfectly matched with the existing images in the database, “FUSED IMAGE IS NOT MATCHED WITH DATABASE” is displayed in the command window. The user is not given authentication and “ACCESS DENIED” is displayed in the command window as shown in Fig. 5.6.

When the invalid user ID and password is entered, user cannot proceed into the system. An error message of “INVALID USER ID AND PASSWORD PLEASE TRY AGAIN LATER” is displayed in the command window.

When the fused image is matched with the database image, user gains authentication. Then the authorised user is allowed to access the medical record database. Now the authorised user can proceed into the system for encrypting or decrypting the medical images as shown in Fig. 5.7 (a) (b).

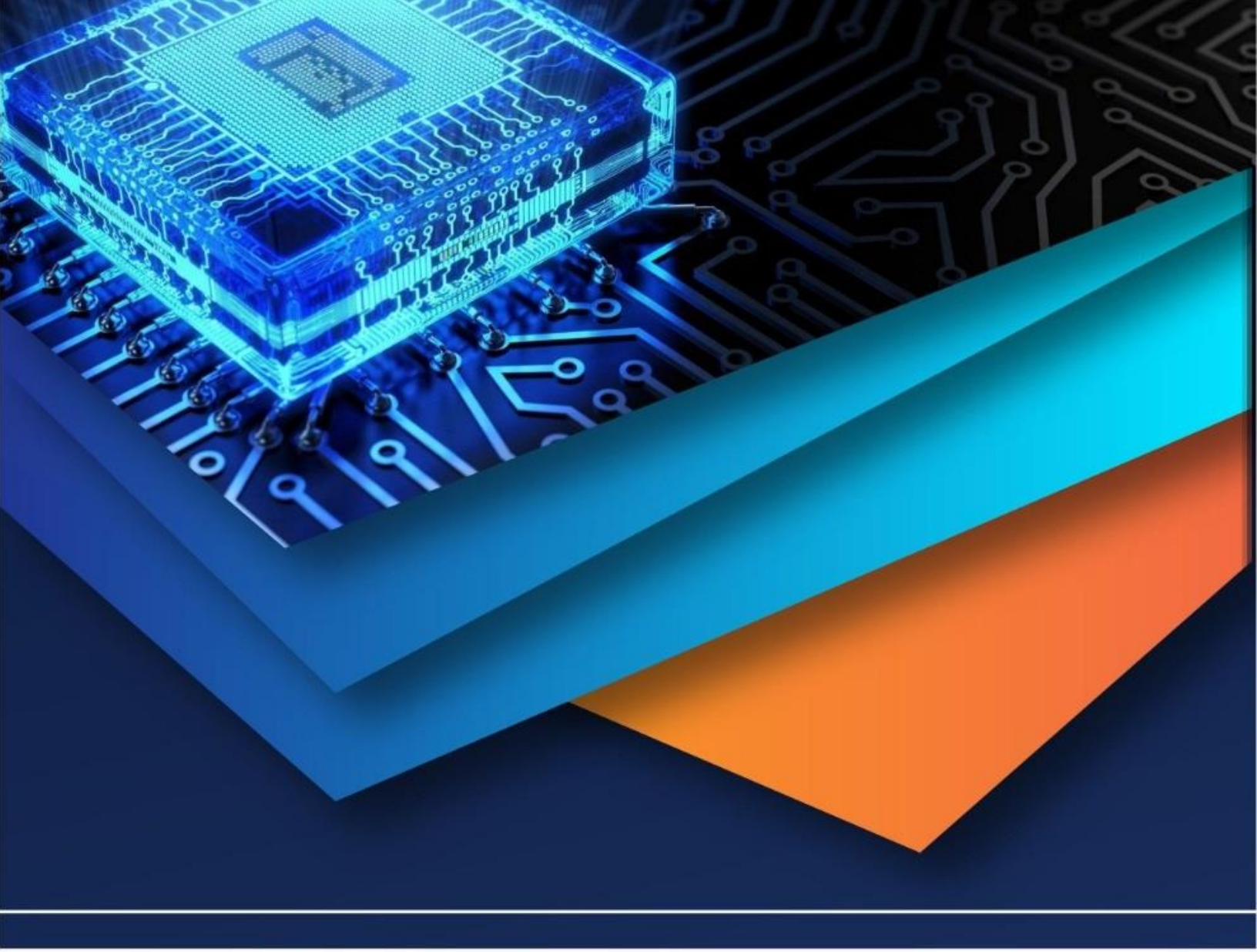
VI. CONCLUSION AND FUTURE SCOPE

The work proposed in this paper ensures confidentiality of medical information for telemedicine applications. Further, authentication phase is tightened with password protection followed by fusion of finger vein and finger knuckle biometric traits. Future work may be focussed on including one more biometric trait for fusion and also incorporating strong encryption algorithms.

REFERENCES

[1] M. Shamim Hossain, Ghulam Muhammad, Sk Md Mizanur Rahman, Wadood Abdul, Abdulhameed Alelaiwi, and Atif Alamri, “Toward End-to-End Biometrics-Based Security for IoT Infrastructure”, IEEE Wireless Communications, pp. 44-51, Oct 2016

[2] Samson Chepuri "An RGB Image Encryption using RSA Algorithm", International Journal of Current Trends in Engineering & Research, vol. 3, pp. 1 – 7, March 2017
[3] Anil K. Jain, Fellow, "An Introduction to Biometric Recognition", IEEE transactions on circuits and systems for video technology, vol. 14, no. 1, pp. 4-20, January 2004
[4] Sun Bei, "A fingerprint identification algorithm based on local minutiae topological property", IEEE First International Conference on Data Science in Cyberspace, vol. 6, pp. 694-697, March 2017
[5] J. Daugman, "Recognizing persons by their Iris patterns", IEEE International Conference on security technology, vol. 16, pp. 5–25, August 2002
[6] Amine Amraoui, Mounir Ait Kerroum, Youssef Fakhri, "Unimodal palm print recognition system based on local features", International Conference on Advanced Technologies for Signal and Image Processing, vol. 11, pp. 1-5, May 2017
[7] Charushila R, Hemprasad Y, "A shearlet transform based illumination invariant 2-D face recognition", International Conference on Electrical, Electronics, and Optimization Techniques, vol. 4, pp. 3407 – 3412, March 2016
[8] Sameer Sharma, Mr Shashi Bhushan, "Improved Human Identification using Finger Vein Images", International Journal of Advanced Research in Computer Science & Technology, vol. 2, pp. 32-34, March 2014
[9] Ajay Kumar and David Zhang, "Improving Biometric Authentication Performance From the User Quality," IEEE Transactions On Instrumentation And Measurement, vol. 59, No. 3, pp.730-735, March 2010
[10] N. Miura, A. Nagasaka , and T. Miyatake, "Feature extraction of finger vein patterns based on repeated line tracking and its application to personal identification", IEEE transactions on Machine Vision and Applications, vol. 15, pp. 194-203, March 2014
[11] Yu Lu, Shan Juan Xie, Sook Yoon, Zhihui Wang and Dong Sun Park, "An Available Database for the Research of Finger Vein Recognition", International Conference on Image and Signal Processing, pp. 410-415, March 2013
[12] Abdellah Guebla, Abdallah Meraoumia, Hakim Bendjenna and Salim Chitroub, "Using of Finger-Knuckle-Print in biometric security systems", International Conference on Information Technologies for Organizations Developement, pp. 23-29, April 2016



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY