Two Stage Security Scheme to Retrieve Secured Data from Database Using E²D²M² Technique In Patient Monitoring

Sukumar T.[1*] and Santha K.R.[2]
1. Department of Information Technology, Sri Venkateswara College of Engineering, Anna University, Sriperumbudur, Tamil Nadu, 602105, INDIA
2. Department of Electrical and Electronics Engineering, Sri Venkateswara College of Engineering, Anna University, Sriperumbudur, Tamil Nadu, 602 105, INDIA
*sukumart@svce.ac.in, santha@svce.ac.in

Abstract

Now a days maintaininig a patient database is a challenging task. Patient monitoring system can be established by ensuring confidentiality of patient details in accordance to fingerprint recognition and authentication. In this paper, a method of retrieving the secured data from database using $E^2D^2M^2$ method is introduced. The $E^2D^2M^2$ method is implemented with the techniques of encryption, embedding, decryption, data unmasking, authentication key, and fingerprint matching. The process has two sides namely client side and server side. In the client side, the enhanced sample fingerprint image is encrypted through encryption technique and the authentication key is super imposed on a cover image. Then the encrypted image is superimposed on a cover image. The superimposed output is then sent to the server side. In the server side, the embedded and encrypted images are separated. Authentication key is extracted from embedded cover images. Fingerprint image is decrypted from encrypted image. After these processes, the minutiae of the fingerprint is extracted and compared with fingerprint database. Similarly, the authentication key is compared with the authentication key database. Secured data is retrieved from the database based on the matched results.

Keywords: Encryption, fingerprint recognition, image matching, authentication, message authentication.

Introduction

Patient monitoring system is a growing and essential field in order to maintain integrity and confidentiality of patient details. Maintaining and establishing patient database in a secure way is a challenging task. Information security is an emerging field in engineering in order to secure important data. Different techniques are followed to provide security for the data which can be retrieved from the database through a password or biometric characteristics. Fingerprint based information security is always an attractive biometric feature owing to its uniqueness. The fingerprint is unique even for twins. This special characteristic of fingerprint has enthused the researcher to pursue research in the field of information security and provide protection to the data. Fingerprint matching is classified into correlation based matching, minutiae-based matching, and feature based matching [1]. Baoxi Yuan [2] proposed a novel fingerprint retrieval approach based on minutiae triplet. The number of matched minutiae polygons can be derived by matching the information of minutiae triplets, and, a one-bit flag is attached to each index to enhance the matching precision. These two techniques significantly increase the accuracy and efficacy of fingerprint retrieval in large databases. Arun Ross [3] proposed a compact fixed-length representation of a fingerprint image. It is worth mentioning that the performance of the proposed technique is inferior to that of a minutiae-based fingerprint matching. An effective weighting technique is required to correlate with the template.

Chen Kaizhi [4] proposed a method of extracting a rotation-translation-invariant texture feature from the minutiae neighborhood to help matching fingerprint minutiae. The texture feature has an important role in accelerating the matching speed and improving the matching accuracy when it is integrated into fingerprint matching. Mangala R. Belkhede [5] proposed an effective matching algorithm to provide security for online transaction but, this matching algorithm is only limited to single server authentication.

Arun Ross [6] proposed a hybrid technique that performs better than a purely minutiae-based matching scheme. This technique combines minutiae information with the ridge feature map. Garg. R [7] proposed a key point descriptor which provides robustness to rotation and translation of fingerprints. This process computes the matching scores by implicitly aligning with the unencrypted information on the access control device. But, this method did not address the fingerprint matching with respect to time.

Hang Yin [8], proposed a simple and effective method based on the vector orthogonal theory. The main advantage of this approach is its simplification. Compared to the traditional methods, computational expensiveness and complexity are considerably reduced. This approach does not detect the delta points precisely in some conditions. Hence, improvement is required in accuracy. Zhifan Gaol [9], proposed an efficient method of extracting neighboring minutiae by introducing a novel algorithm for fingerprint matching which is invariant to the rotation and translation of a finger print. This technique focused on analyzing the relationship of minutiae and not on capturing more information about fingerprints. Optimization of the performance of this method was not achieved for better performance because a considerable amount of time was lost

owing to the comparison of differences between two feature sets. Secondly,this method did not measure the non-linear transformation which occurred due to the changes in the structures.

Peng Li [10], proposed an alignment-free fingerprint cryptosystem based on the fuzzy vault scheme which was developed using the minutia local structure, which are invariant to the transformation in fingerprint capturing. This method avoided the alignment procedure and not only improved the performance but also secured the fuzzy vault scheme at the same time. Despite the larger template storage expense, the proposed alignment-free fingerprint cryptosystem outperforms the minutiae-based fingerprint cryptosystems in terms of accuracy and security. A drawback of the proposed fingerprint cryptosystem is that the minutia descriptor vault accounts for 86% of the total storage.

Feng Liu [11], proposed a method, which had a high computational complexity, to measure the differences between pores which is based on the residuals obtained by tangent distance and sparse representation technique, thereby, making this method more robust to noise and local distortions in fingerprints when compared to the existing DP and SRDP method. Chouaib Moujahdi [12], proposed a new approach for fingerprint template protection. The information provided by the minutiae is used to construct a new representation based on special spiral curves which are used for the recognition task instead of the traditional minutiae-based representation. Their approach meets revocability, diversity and security, which are required for template protection. The performance of fingerprint shell is not very sensitive to translation/rotation of fingerprint impressions. If the majority of minutiae is missed or several spurious minutiae are added or cropped, the constructed curves will change drastically.

Yadigar Imamverdiyev [13], proposed a highly performing Biometric cryptosystem based on discretized fingerprint texture descriptors. These descriptors are binarized using a biometric discretization method and are used in the fuzzy commitment scheme (FCS). In the future,LDPC codes may be used to process large blocks of fingerprint biometric cryptosystems using large-sized minutiae based binary representations. Gaurav Bhatnagar [14], proposed a chaotic encryption framework based on fractional wavelet packet transform (FrWPT) for securing palm print data. Various analyses such as key sensitivity, key space analysis, edge distortion analysis, randomness analysis, statistical analysis and numerical analysis helped in the achievement of high security.

Miao Qi [15], proposed a novel multimodal biometric image hiding approach based on correlation analysis, which is used to protect the security and integrity of transmitting multimodal biometric images for network-based identification. It provided good imperceptibility and also resisted common attacks and assured great effectiveness but, this method was not robust though it was effective.Mohd Shahrimie [16], proposed a new approach of multimodal finger biometrics based on the fusion of finger vein and finger geometry. The proposed Band Limited Phase Only Correlation (BLPOC) method was utilized to measure the similarity of finger vein images. Compared to the existing methods, BLPOC is resilient to noise, occlusions, and rescaling factors, thus enhancing the performance of finger vein recognition. Haiyong Chen [17] proposed a new algorithm to transform fingerprint features into encrypted forms. This improved the accuracy and speed of fingerprint recognition process. Zhenxing Qian [18], proposed a novel scheme of reversible data hiding (RDH) in encrypted images using distributed source coding (DSC). This method outperforms other existing methods.

The existing works focused only on fingerprint matching in a secure way to access the database to retrieve data.But, the proposed work, has achieved a high level of security to retrieve data from database. The algorithm also withstood various biometric attacks.

Proposed Work

Abbreviation
AUT Key – Authentication Key
$E^2D^2M^2$ – Encryption, Embedding, Decryption, Data Unmasking, Authentication key and Fingerprint Matching
The proposed work contains two stages, namely client side and server side as shown in fig. 1.
The following tasks have been done on client side.

1. In the client side, the fingerprint image is encrypted through encryption algorithm.
2. Authentication key is superimposed on a cover image through data masking process.
3. The modified image and encrypted image are superimposed.
4. The superimposed image is transmitted to the server side.

The following steps have been done on server side.

1. The encrypted image and cover image are separated from each other through the extraction process.
2. The original image is obtained from encrypted image through decryption process.
3. The Authentication key is extracted from the cover image.
4. Authentication key is matched with the authentication key database
5. Enhancement of fingerprint.
6. Minutiae extraction
7. Fingerprint matching with fingerprint database
8. Checking matched results
9. Retrieval of secured data

The algorithms A, B, C and G have been referred from the previous work of the same author and reproduced in this paper [19].

Client Side:
Let image be I and size is n x m x k
Where n is the number of rows, m is the number of columns and k is the number of bits to represent it.
Let the upper boundary of an array value is val_{upper}

A. Key Generation Algorithm

Step 1: Compute array upper boundary new value using equation 1

$$val_{upper} = \sum_{x=1}^{2}\left[\prod_{i=1}^{2} val_{upper_i^{(i)}}\right]_x \quad (1)$$

Step 2: update array values with respect to index base on the following condition

$$Array(index) = \begin{cases} 1, val_{upper} < 0 \\ 0, otherwise \geq 0 \end{cases} \quad (2)$$

Step 3: compute the key vector with respect to index using the following equation

$$key(index1) = \left[\sum Array(index1 x index2)^{(index2-1)}\right]^2 \quad (3)$$

Where index1 and index 2 vary from 1 to row size

B. Encryption Algorithm

Step 1: compute the index value

$$index(i) = index(i) - 1$$

Where i vary from 1 to m

$$index(i) = n.index(i)$$

$$new\_index(i) = \sum_{j=1}^{n} j + index(i)$$

Step 2: compute a key value based on an index

$$key(index(i)) = new\_index(i)$$

Step 3: Encrypt image using above key

$$EI(r_n, c_m) = I(r_n, c_m) \oplus key(index(i)) \quad (4)$$

Where n varies from 1 to n,
m varies from 1 to m and i varies from 1 to 3

C. Embedding Algorithm

The embedding algorithm hides authentication key on a cover image using the following steps.

Let the maximum characters can be encoded in an image are $c_{max.}$ The message values are converted into binary values for the process. Let the message contain m characters $c_0, c_1, c_2, ...c_m$. Let the picture height and length be I_h and I_l respectively.

Step 1: Compute the picture height and length using the following equation.

$$I_h = I_h - \sum_{i=1}^{3} i \text{ and } I_l = I_l - \sum_{j=1}^{2} j$$

Step 2: Compute the suitable hiding points on an image based on the following conditions

$$if\ k < I_l\ then\ k_i = I_l \% k_i\ and$$
$$k_i = k_i + 1$$
$$else$$
$$k_i = k_i \% I_l + 1$$
$$if\ k_j < I_h\ then\ k_j = I_h \% k_j + 1$$
$$else$$
$$k_j = k_j \% I_h + 1$$

Let Array be $A(I_l, I_h)$ and initial value is equal to one

$$k_i = \sum_{j=1}^{m} k_j + I_h / 2$$

$$k_j = \sum_{i=1}^{m} k_i + I_l / 2$$

$$c_j > \left(\max_c \Big/ key_{lgth}\right) + 2$$

$$if\ A(I_l, I_h) = 1\ then\ c_j = c_j + 1$$

Find the non zero values in an array and update index

$$If\ Array\ A(I_l, I_h) \neq 0\ then\ index = A(I_l, I_h) \quad (5)$$

D. An algorithm for superimposing encrypted image on the cover image

Let encrypted image be E (x, y) and cover image be C (m, n)

Step1: Perform logical bitwise with each pixel presents in an image.
Let Z be a total number of pixels in an image.
Z = x*y
Let p_1, p_2, p_3……. Ps are pixels in an image E (x, y)
Let each pixel containing b_1, b_2…. b_8

$$p_k = \prod_{i=1, j=1}^{i=8, j=8} b_i o_{j-2}; o_j = 1, if\ j > 2 \quad (6)$$

Where k varies from 1 to z

Step 2: Perform the following operations on the cover image
Z = x* y
Let q_1, q_2, q_3……. Quiz are pixels in an image C (m, n)
Let each pixel containing b_1, b_2…. b_8

$$q_t = \frac{b_i}{2^{|k|}}\ i = 1\ to\ 8 \quad (7)$$

k finds suitable locations on the image. In our experiment k varied from 1 to 4. Optimal value is 4. Where t varies from 1 to z

Step 3: Select the suitable place on the pixels from above resultant output

$$q_t = \prod_{t=1}^{z} q_t (x^3 + x^2) \quad (8)$$

In our experiment x varied from 1 to 4 and obtained the best value is 2.

Step 4: Select the suitable places on pixels from previous result

$$q_t = \frac{q_t}{2^{|k|}} \quad (9)$$

Where t varies from 1 to z and k value is 2

Step 5: Perform few operations on the pixel using the following steps.

$$q_t = \prod_{t=1}^{z} q_t \left(x^3 \big/ x^2 + 1 \right) \quad (10)$$

Where x takes the value 2

Step 6:

$$q_t = \prod_{t=1}^{z} q_t (x^3 + x^2) / 2^{|k|} \quad (11)$$

In our experiment k=2, and x varied from 1 to 4. The final best value is 2.

Step 7:

$$q_t = \prod_{t=1}^{z} q_t \left(x + 1 \right) \quad (12)$$

Where x value is 2

Step 8: the superimposed image was obtained by varying the image quadrant wise and the derived outputs are as follows.

Quadrant – I

$$SI(i+m, j, k) = \sum_{i=1}^{m} \sum_{j=1}^{n} \sum_{k=1}^{3} E(i+m, j, k) + c(m, n, k) \quad (13)$$

Quadrant – II

$$SI(i, j, k) = \sum_{i=1}^{m} \sum_{j=1}^{n} \sum_{k=1}^{3} E(i, j, k) + c(m, n, k) \quad (14)$$

Quadrant – III

$$SI(i, j+n, k) = \sum_{i=1}^{m} \sum_{j=1}^{n} \sum_{k=1}^{3} E(i, j+n, k) + c(m, n, k) \quad (15)$$

Quadrant – IV

$$SI(i+m, j+n, k) = \sum_{i=1}^{m} \sum_{j=1}^{n} \sum_{k=1}^{3} E(i+m, j+n, k) + c(m, n, k) \quad (16)$$

E. Algorithm to separate the encrypted image from the superimposed image

Let Z be a total number of pixels in an image. Z = x*y
Let P_1, P_2, P_3……. Ps are pixels of an image SI (x, y)
Let assume, each pixel containing b_1, b_2…. b_8

$$p_k = \prod_{i=1, j=1}^{i=8, j=8} b_i o_{j-2}; o_j = 1, if\ j > 2 \quad (17)$$

Where k varies from 1 to z

Encrypted image E (m, n) = SI (x, y) (18)

F. Algorithm for separation of cover image

Let Z be a total number of pixels in an image. Z = x*y
Let p_1, p_2, p_3…….p_z are pixels in an image SI (x, y)

Let each pixel containing b_1, b_2 ….b_8

Step 1: Perform logical bitwise with each pixel presents in a superimposed image.

Let Z be a total number of pixels in an image. Z = x*y
Let p_1, p_2, p_3…….p_z are pixels in an image SI (x, y)
Let each pixel containing b_1, b_2 ….b_8

$$p_t = \prod_{t=1}^{z} p_t (x+1) \quad (19)$$

In our experiment k=2, and x varied from 1 to 4. The final best value is 2

Step 2: Perform the following operations on above resultant image pixel bits

$$p_t = b_i 2^{|l|} \ \ i = 1 to 8 \quad (20)$$

l is the factor to find suitable locations in a pixel places.
In our experiment *l* varied from 1 to 4. Best value is 2.

Where t varies from 1 to z

$$PR1 = SI(i, j, k) \quad (21)$$

Step 3: Partial output 2 obtained using the following equation

$$PR2(i+m, j+n, k) = \prod_{i=1}^{m} \prod_{j=1}^{n} \prod_{k=1}^{3} SI(i+m, j+n, k)(x+1) \quad (22)$$

Step 4: Partial output 3 obtained using the following equation

$$PR3(i+m, j, k) = \prod_{i=1}^{m} \prod_{j=1}^{n} \prod_{k=1}^{3} SI(i+m, j, k)(x+1) \quad (23)$$

Step 5: Perform the following operations on pixels of previous output.

$$p_t = b_i 2^{|l|} \ \ i = 1 to 8 \quad (24)$$

Where '*l*' separates, cover image from a superimposed image. We used *l* value is 1.

Step 6:

$$PR4(i,j,k) = \prod_{i=1}^{m}\prod_{j=1}^{n}\prod_{k=1}^{3} SI(i,j+n,k)(x+1) \quad (25)$$

Step 7: the first partial result obtained through the sum of partial result 1 and 2.

$$FR1 = \sum (PR1 + PR2) \quad (26)$$

Perform the following operations on pixels of FR1.

$$FR2 = p_t = b_i 2^{|l|} \;\; i = 1 to 8 \quad (27)$$

Where i vary from 1 to 8 and '*l*' is the key factor to separate cover image from superimposed image. We used *l* value is 2

Step 8: The cover image can be obtained using the following equation.

$$C(x,y) = FR2 + PR3 + PR4 \quad (28)$$

G. An Algorithm for unmasking Authentication Key

Step 1: Vary outer loop from 1 to maximum c_{max} characters.

Step 2: Vary inner loop from 1 to 2^n-1 where n=3

Step 3: Check messages (x_i, y_j) where i vary from 1 to max_c and j vary from 1 to 2^n-1; n=3

Step 4: compute Index value using the following equation

$$Index = Index(x_i + (2^n - 1)(y_i - 1) \quad (29)$$

Step 5: update message content by 1 w.r.t row and column if I(Index)%2 is equal to one.

Row x_i varies from 1 to max_c and column y_j vary from 1 to 2^n-1

H. Algorithm for decryption of encrypted image

Let the image be I and size are n x m x k
Where n is the number of rows, m is the number of columns and k is the number of bits to represent it.

Step 1: compute index value

$$index(i) = index(i) - 1$$

Where i vary from 1 to m

$$index(i) = index(i)\ n$$

$$new\_index(i) = \sum_{j=1}^{n} j + index(i)$$

Step 2: compute a key value based on an index

$$key(index(i)) = new\_index(i)$$

Step 3: decrypt an image using the following equation

$$I(rn,cm) = EI(rn,cm) \oplus key(index(i)) \quad (30)$$

Where n varies from 1 to n.

Implementation

The proposed method was implemented in MATLAB 7.12.0 (R2011a). Sample images were taken from FVC2002 [20]. Original fingerprint image size was 388X374 and TIFF image as shown in Fig.2. This image was encrypted using encryption algorithm and it was shown in Fig.3. Authentication key was embedded on a cover image as shown in fig.4. The cover image is a grayscale image. Finally superimposing of two image output is shown in fig. 5

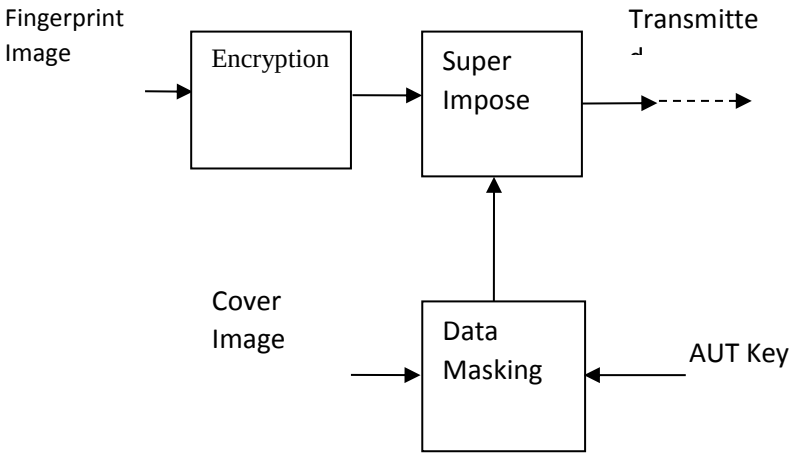


Figure 1a: Architecture of Encryption and Data Masking Stage at Client Side

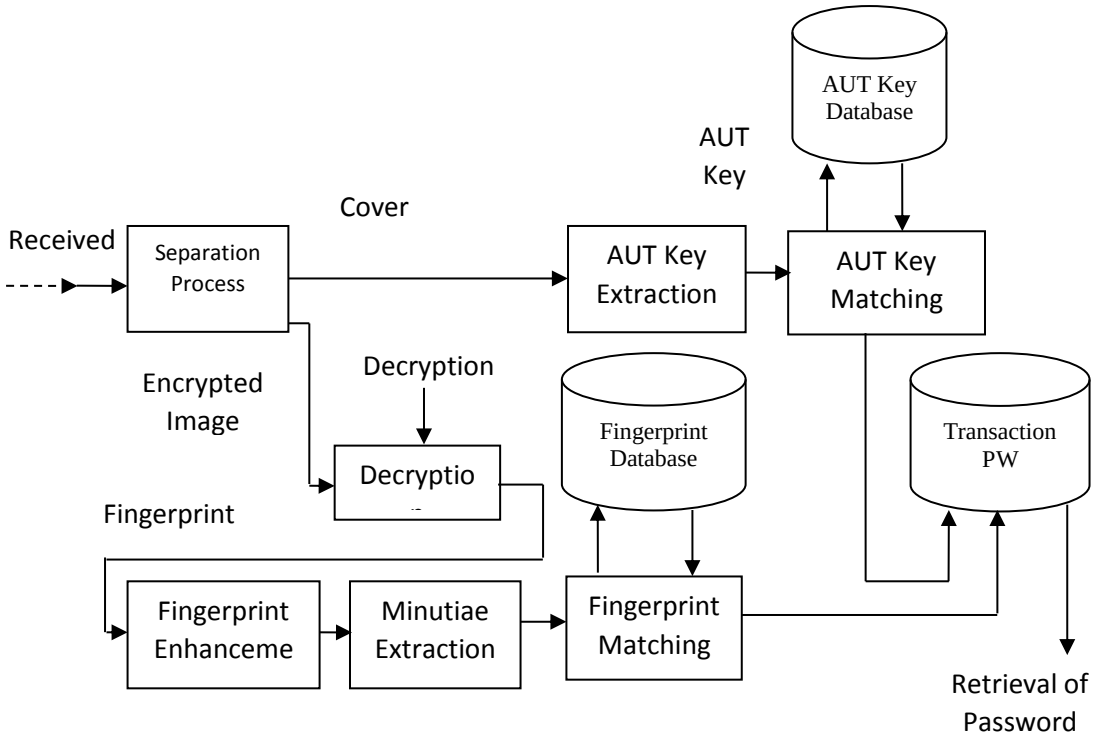
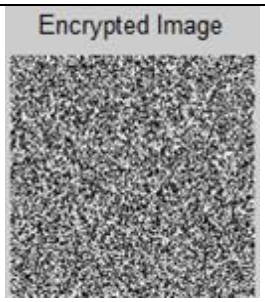
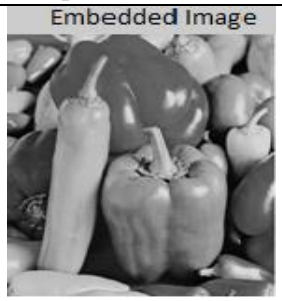
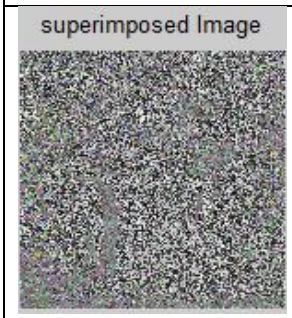
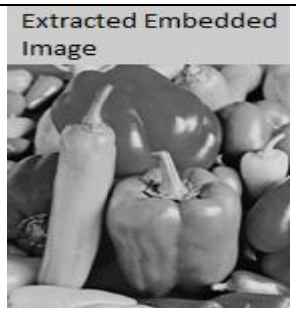


Figure 1b: Architecture of Fingerprint Matching and Retrieval of Transaction Password

Client side Outputs			
 **Fig. 2: 101_7.tif**	 **Fig. 3: Encrypted Image**	 **Fig. 4: Data Masking**	 **Fig. 5: Super Imposed Image**
Server side outputs			
 **Fig. 6: Super Imposed Image**	 **Fig. 7: Extracted Encrypted Image**	 **Fig. 8: Extracted Embedded Image**	 **Fig. 9: 101_7.tif**

I. Server side Output

At server side, encrypted image and embedded image are separated from the superimposed image as shown in fig.7 and 8. The original image was decrypted from an encrypted image as shown in fig. 9. Authentication key was extracted from the embedded image as shown in fig. 10.

In the proposed work, the retrieval of the password from a database with a high level of security was focussed. So, traditional fingerprint enhancement technique was used. After enhancement, fingerprint features were extracted and matched using minutiae and ridge as shown in fig.11, 12 and 13.

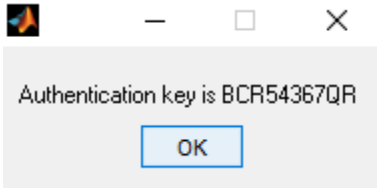


Fig. 10: Extraction of Authentication key

Fig. 11: Enhanced Image of 101_7.tif

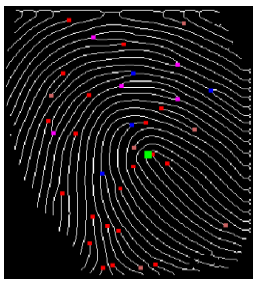


Fig. 12:. Minutiae Extraction

J. Various Test Images

The various test images of FVC 2002 (DB1_B) were used for testing process as shown in fig.13. The similarity score of test images are shown in table 1.

K. SPAM Steganalysis

Steganalysis is the process of identifying hidden data in an image. Our proposed algorithm was able to withstand biometric attacks and not shows hidden data in a cover image as shown in fig.14 and 15.

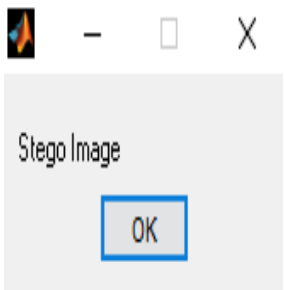


Fig. 14: Existing Technique

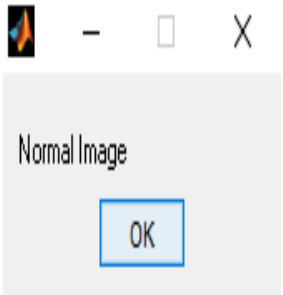


Fig. 15: Proposed Technique

After Fingeprint features extraction,

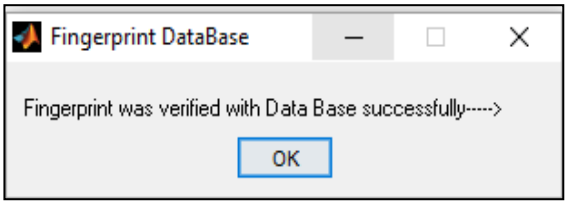


Fig. 16: Fingerprint Matching

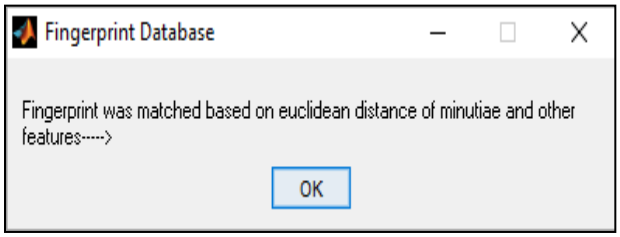


Fig. 17: Fingerprint Matching based on its Features

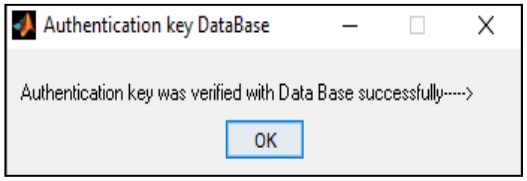


Fig. 18: Authentication key matching

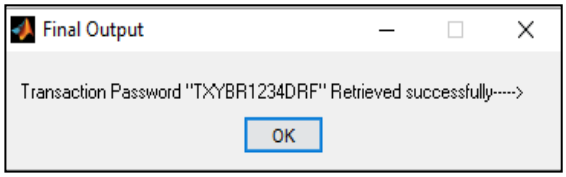


Fig. 19: Retrieval of Transaction Password

After extraction of Authentication key from cover image, Authentication key was matched with the database. The output was shown in fig.18. The transaction password has been retrieved from database successfully as shown in fig.19.

Evaluation

The authors have tested the similarity of various fingerprints with the test image and the similarity scores were calculated and results are shown in table.1.

ROC curves show a comparison between before and after enhancement of fingerprint as shown in figure 21. The proposed method acheived a net improvement of 25% and the performance impoved compared to the previous work.

The fingerprint enhancement algorithm were tested with FVC2002 DB3 database and the results are given below.
The number of fingerprint images are not matched before enhancement of fingerprint (B.E) = 83

The number of fingerprint images are matched after enhancement of fingerprint (A.E) = 62
Difference B.E-A.E = 21
Number of test images = 800

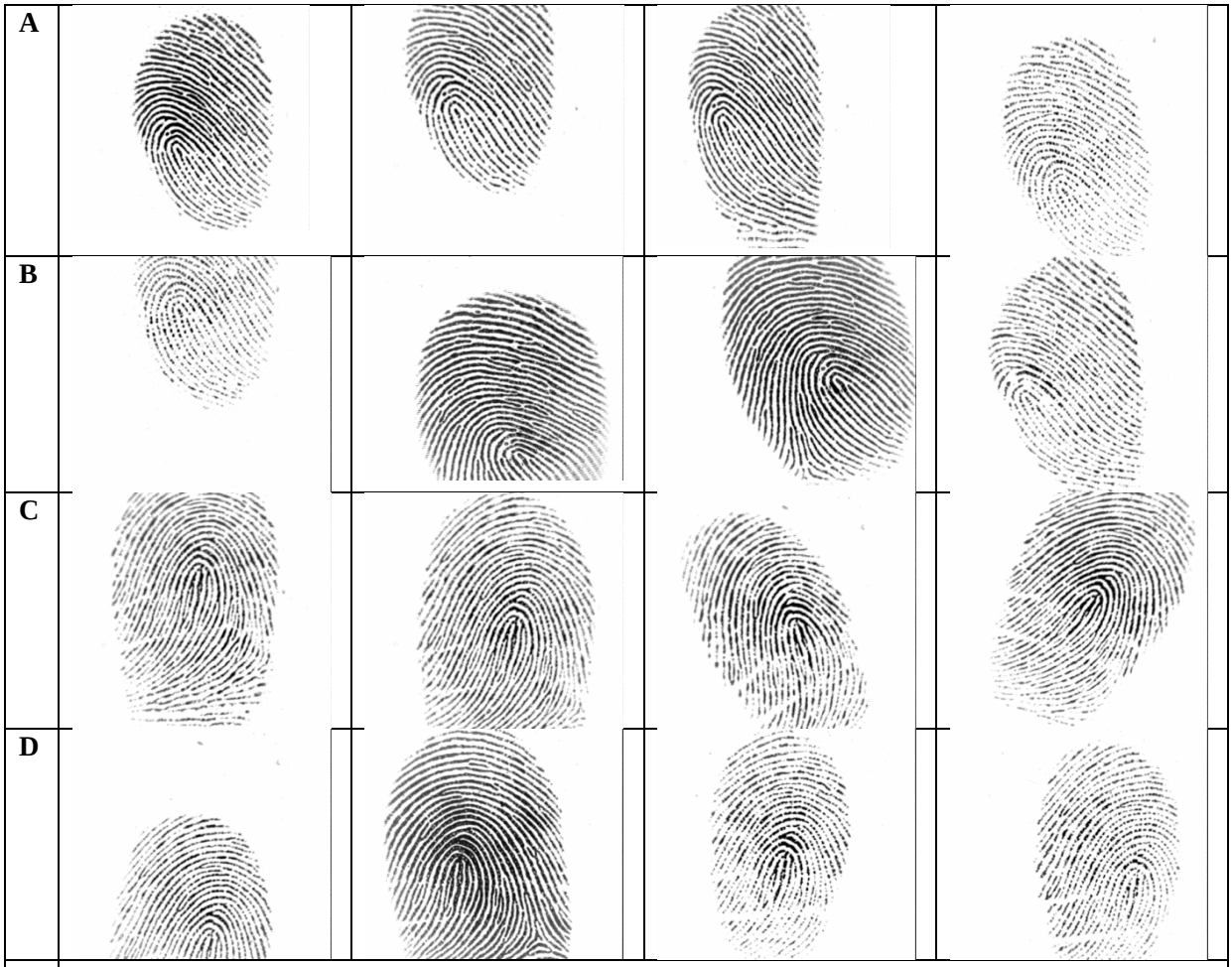


Fig. 13: a, b,c and d are test images of FVC2002(DB1_B)

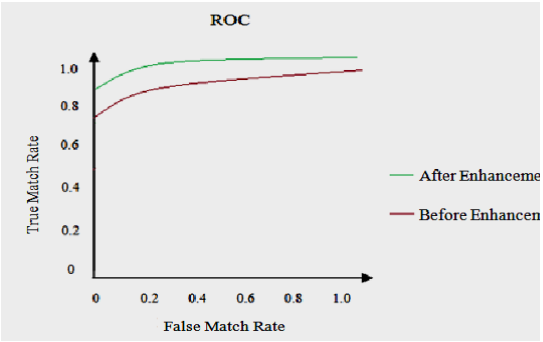


Fig. 21: ROC curves with and without Enhancement

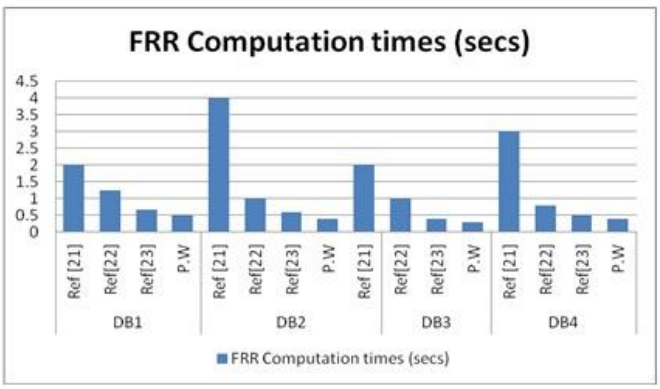


Fig. 22: Comparison of FRR for various algorithms

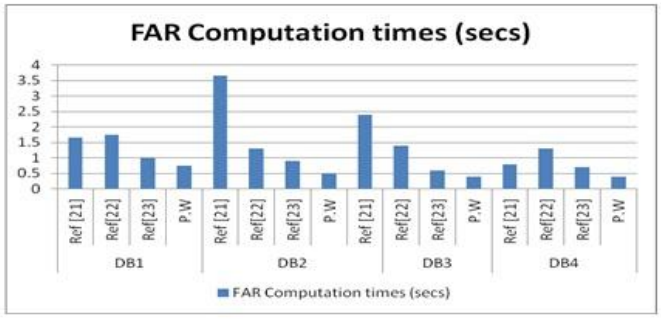


Fig. 23: Comparison of FAR for various algorithms

Conclusion

The previous studies focused on methodologies to retrieve data from the database using fingerprint. But the proposed algorithm acheived robust security since ,the method added two levels of security through fingerprint matching and authentication key matching. After the success of these stages, transaction password can be retrieved from transaction password database. This proves that good security was achieved during transaction. Unauthorized user cannot retrieve the transaction password if they do not know the authentication key. The similarity score of various test images and the Euclidean distance are as shown in figure.20. The Euclidean distance is very small for an authorized user

as shown in table.1. Hence the proposed method outperforms the existing technique when compared to FAR and FRR and other existing techniques. Infuture, this work would applicable in maintaining patient monitoring system and ensuring authentication of patient details using IoT.

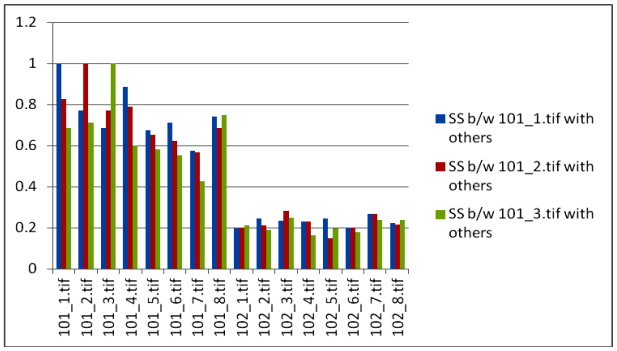


Fig. 24: Similarity Score

References

1. Ayman Mohammad Bahaa-Eldin, "A medium resolution fingerprint matching system", Ain Shams Engineering Journal (2013) 4, 393–408.

2. Baoxi Yuan; Fei Su; Anni Cai., "Fingerprint retrieval approach based on novel minutiae triplet features", Biometrics: Theory, Applications and Systems (BTAS), 2012 IEEE Fifth International Conference on Year: 2012, Pages: 170 - 175, DOI: 10.1109/BTAS.2012.6374573

3. Arun Ross, James Reisman, and Anil Jain,'' Fingerprint Matching Using Feature Space Correlation'', Appeared in Proc. of Post-ECCV Workshop on Biometric Authentication, LNCS 2359, pp.48-57, Denmark, June 1, 2002.

4. Kaizhi, C.; Aiqun, H., "Fingerprint Matching Using Texture Feature Extracted from Minutiae Neighborhood", Computational Intelligence and Communication Networks (CICN), 2012 Fourth International Conference on Year: 2012, Pages: 322 - 326, DOI: 10.1109/CICN.2012.115

5. Mangala R. Belkhede, Veena A. Gulhane, Dr. P.R. Bajaj,'' A FLC based Fingerprint Matching Algorithm for Images Captured with Android Camera for enhanced Security of Online Transaction'', The International Journal of Computer Science & Applications (TIJCSA), Volume 1, No. 3, May 2012 ISSN – 2278-1080.

6. Arun Ross, Anil Jain, James Reisman, "A hybrid fingerprint matcher", Pattern Recognition, Volume 36, Issue 7, July 2003, Pages 1661-1673

7. Ravi Garg and Shantanu Rane, "A keypoint descriptor for alignment-free fingerprint matching", TR2013-023 May 2013

8. Hang Yin, Xiaojun Jing, Songlin Sun,'' A novel algorithm for fingerprint singular points detection based'', Proceedings of IEEE CCIS2011.

9. Zhifan Gaol, Xinge Youl, Long Zhou, Wu Zeng,'' A novel matching technique for fingerprint recognition by graphical structures'', Proceedings of the 2011 International Conference on Wavelet analysis and Pattern Recognition, Guilin, 10-13 July, 2011

10. Peng Li, XinYang, KaiCao, XunqiangTao, RuifangWang, JieTian, ,''An alignment-free fingerprint cryptosystem based on fuzzy vault scheme'', Journal of Network and Computer Applications 33 (2010) 207–220.

11. Feng Liu, QijunZhao, DavidZhang n, ''A novel hierarchical fingerprint matching approach'', Pattern Recognition 44 (2011) 1604–1613.

12. Chouaib Moujahdi, George Bebis, Sanaa Ghouzali, Mohammed Rziza,'' Fingerprint shell: Secure representation of fingerprint template'', Pattern Recognition Letters 45 (2014) 189–196.

13. Yadigar Imamverdiyev, Andrew Beng Jin Teoh, Jaihie Kim,'' Biometric cryptosystem based on discretized fingerprint texture descriptors'', Expert Systems with Applications 40 (2013) 1888–1901.

14. Gaurav Bhatnagar, Q.M. Jonathan Wu, '' A Novel Chaotic Encryption Framework for Securing Palmprint Data'', Procedia Computer Science 10 (2012) 442 – 449.

15. Miao Qi, YinghuaLu, NingDua, YinanZhang, ChengxiWang, Jun Kong, '' A novel image hiding approach based on correlation analysis for secure multimodal biometrics'', Journal of Network and Computer Applications 33 (2010) 247–257.

16. Mohd Shahrimie Mohd Asaari, Shahrel A. Suandi, Bakhtiar Affendi Rosdi,'' Fusion of Band Limited Phase Only Correlation and Width Centroid Contour Distance for finger based biometrics'', Expert Systems with Applications 41 (2014) 3367–3382.

17. Haiyong Chen, Hailiang Chen, "A novel algorithm of fingerprint encryption using minutiae-based transformation", Pattern Recognition Letters, Volume 32, Issue 2, 15 January 2011, Pages 305–309.

18. Zhenxing Qian, Xinpeng Zhang, "Reversible Data Hiding in Encrypted Image with Distributed Source Encoding", IEEE Transactions on Circuits and Systems for Video Technology, DOI 10.1109/TCSVT.2015.2418611.

19. Sukumar. T, Santha. K.R., "An approach for secret communication using adaptive key technique for gray scale images," in Circuit, Power and Computing Technologies (ICCPCT), 2015 International Conference on , vol., no., pp.1-5, 19-20 March 2015.

20. http://bias.csr.unibo.it/fvc2002/databases.asp

21. P. Peer, "Fingerprint-Based Verification System A Research Prototype", IWSSIP 2010 - 17th International Conference on Systems, Signals and Image Processing, **(2010),** pp. 150-153.

22. T. Li, C. Liang and K. Sei-ichiro, "Fingerprint Matching Using Dual Hilbert Scans", SITIS, **(2009),** pp. 553559.

23. Iwasokun Gabriel Babatunde, "Fingerprint Matching Using Minutiae-Singular Points Network", International Journal of Signal Processing, Image Processing and Pattern Recognition, Vol. 8, No. 2 (2015), pp. 375-388