# Multimodal Biometric Cryptosystem Involving Face, Fingerprint and Palm Vein

**B.Prasanalakshmi[1] , A.Kannammal[2], R.Sridevi[3]**

**[1] Research Scholar,**
**Bharathiar University,**
**Coimbatore, Tamilnadu,India**

**[2]Associate Professor,**
**Coimbatore Institute of Technology,**
**Coimbatore, Tamilnadu, India**

**[3]PG scholar**
**SCSVMV University,**
**Kanchipuram,Tamilnadu,India**

## ABSTRACT

**The proposed scheme involves an idea of including three biometric traits of a person where in the sense even if one fails the other trait could be utilised for verification or identity.Moreover the concept of cryptosystem is involved , where one of the biometric trait – the palm vein itself acts as a key to utilise the stored template database. The main idea in using one of the biometric trait as a key is that under any circumstance no two palm veins match unless it belong to same person. It is a valid key which no one can steal or misuse.**

**KEYWORDS : Mutimodal Biometrics, Face, Cryptosystem, Fingerprint , Palmvein.**

## INTRODUCTION

Personal identification technology is nowadays becoming more important in security systems. Today authenticating through traditional mode such as password, key, magnetic card etc., are vanishing and disliked by people since they could be stolen or easily forgotten. In order to fill this vanishing space biometric technology is emerging in wide number of systems. Also biometric systems have been an important area of research in these recent years. Two important utilizations of biometric systems are Authentication or Verification and Identification, which is based on the biometric trait enrolled. This enrolled biometric trait may be physiological or behavioral characteristic of a human being satisfying the requirements of universality, uniqueness, permanence and collectability. These biometric systems are non- deterministic, since a single entity when spoofed may be analyzed and the fact that usage of multimodal traits can avoid such spoofing problems we go on for multimodal biometric traits.

For the real time authentication since people prefer to have cards, the multimodal biometrics discussed above are invoked into the smart card which is a space specified token. The multimodal biometric traits taken under consideration are the Face and Fingerprint. In any biometric entity there are some features involved in it. These features constitute the pattern.

A number of researches have bridged the two potentially complementary security technologies- Biometrics and Cryptography. A biometric system is a pattern recognition system that recognises a person based on a feature vector derived from specific physiological or behavioural characteristics that the person possesses [1]. A vein pattern detection is proved to comply with this definition [2] and it provides many important biometric features as :

- Almost impossible to forge or copy.
- Biometric parameters are hidden from general view.
- Vein pattern is intricate enough to allow sufficient criteria for detecting even identical twins.

Throughout the last decade biometrics have gained popularity in application employed for identifying individuals. The accomplishment of its relevance in user authentication has revealed that numerous benefits could be obtained when cryptography is combined with Biometrics [3]. The systems that combine both biometric and Cryptography are called as Biometric Cryptosystems or Crypto-Biometric systems [4][5]. However numerous researchers have successfully designed many cryptosystems based on Biometrics to solve the problems, the entire power of Biometrics is not yet revealed in a complete manner [6]. One advantage of passwords over biometrics is that they can be

reissued. If a token or a password is lost or stolen, it can be cancelled and replaced by a newer version. This is not naturally available in biometrics. If someone's face is compromised from a database, they cannot cancel or reissue it. Cancelable biometrics is a way in which to incorporate protection and the replacement features into biometrics. It was first proposed by Ratha et al[7].

This is a method of enhancing the security and privacy of biometric authentication. Instead of enrolling with the true biometric trait , it is intentionally distorted in a r epeatable manner and this new trait is used. If, by some means, the old distorted trait is "stolen", an essentially "new" trait can be issued by simply changing the parameters of the distortion process. This also results in enhanced privacy for the user since his true biometric trait(under consideration) details are never used anywhere, and different distortions can be used for different types of accounts.

**INITIATIVE STEPS INVOLOVED**

## A. FINGER PRINT FEATURE EXTRACTION

A fingerprint is the feature pattern of one finger. It is believed with strong evidences that each fingerprint is unique. Each person has his own fingerprints with the permanent uniqueness. So fingerprints have being used for identification and forensic investigation for a long time. A fingerprint is composed of many ridges and furrows. These ridges and furrows present good similarities in each small local window, like parallelism and average width. However, shown by intensive research on fingerprint recognition, fingerprints are not distinguished by their ridges and furrows, but by Minutia, which are some abnormal points on the ridges. Among the variety of minutia types reported in literatures, two are mostly significant and in heavy usage: one is called termination, which is the immediate ending of a r idge; the other is called bifurcation, which is the point on the ridge from which two branches derive. Valley is also referred as Furrow, Termination is also called Ending, and Bifurcation is also called Branch.

Two representation forms for fingerprints separate the two approaches for fingerprint recognition.

The first approach, which is minutia-based, represents the fingerprint by its local features, like terminations and bifurcations. This approach has been intensively studied, also is the backbone of the current available fingerprint recognition products. The second approach, which uses image-based methods [8 ] [9 , tries to do matching based on the global features of a whole fingerprint image. It is an advanced and newly emerging method for fingerprint recognition.

The fingerprint feature vector is created as the steps indicated below:

- Image Pre-processing
- Minutiae extraction
- Minutiae pre-processing
- Minutiae matching

**Step 1 :** Image enhancement done using Histogram equalisation and Fast Fourier transform.
**Step 2:** using local adaptive thresholding the fingerprint image is binarised.
**Step 3:** ROI extraction is done in a t wo step process.

A. For a fingerprint image of size 16 × 16 pixels the gradient values along x-direction ($g_x$) and y-direction ($g_y$) for each pixel of the block are calculated. Two Sobel filters are used to fulfil the task.

B. For each block, use the following formula to get the Least Square approximation of the block direction.

$tg2\beta = 2 \sum \sum (g_x * g_y) / \sum \sum (g_x^2 - g_y^2)$ for all the pixels in each block.

The formula is easy to understand by regarding gradient values along x-direction and y-direction as cosine value and sine value. So the tangent value of the block direction is estimated nearly the same as the way illustrated by the following formula.

$$tg2\theta = 2\sin\theta \cos\theta / (\cos^2\theta - \sin^2\theta)$$

C. With the estimated block direction, the blocks without significant information on ridges and furrows are discarded based on the following formulas:

$$E = \{2 \sum \sum (g_x * g_y) + \sum \sum (g_x^2 - g_y^2)\} / W*W*\sum \sum (g_x^2 + g_y^2)$$

For each block, if its certainty level E is below a threshold, then the block is regarded as a background block.

D. ROI is extracted using two operations OPEN and CLOSE . With these calculated values the ROI bound is calculated which is the (area of OPEN – area of CLOSE)

**Step 4:** An iterative thinning algorithm is proposed to eliminate the redundant pixels of ridges till the ridges are just one pixel wide.[10]

**Step 5:** The thinned ridge map obtained from previous step is then filtered by three other morphological operations to remove some H breaks, isolated points and spikes.

**Step 6 :** Minutiae marking is done using the usual 3×3 windowing method.

**Step 7:** False minutiae are removed using the following steps: The seven types of false minutiae are shown in Fig 1 .

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

**Step 8:** Terminations and bifurcations are unified. Orientation of each termination is represented by (tx,ty). Track a r idge segment whose starting point is the termination and length is D. Sum up all x-coordinates of points in the ridge segment. Divide above summation with D to get sx. Then get sy using the same way.

Get the direction from: atan((sy-ty)/(sx-tx)).

Step 9 :The resulting values gives the unified minutiae locations and orientation values which is formed as a feature vector $FP_v$.

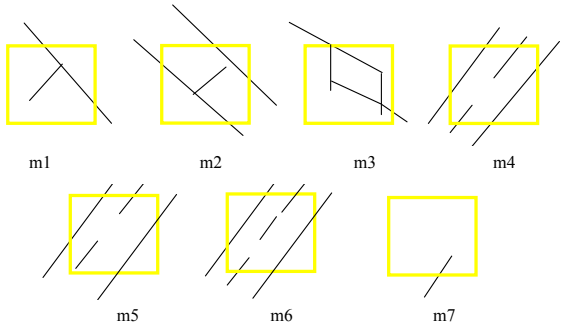



**Figure 1. False Minutiae Structures**

In Figure 1 m1 is a spike piercing into a valley. In the m2 case a spike falsely connects two ridges. m3 has two near bifurcations located in the same ridge. The two ridge broken points in the m4 case have nearly the same orientation and a s hort distance. m5 is alike the m4 case with the exception that one part of the broken ridge is so short that another termination is generated. m6 extends the m4 case but with the extra property that a third ridge is found in the middle of the two parts of the broken ridge. m7 has only one short ridge found in the threshold window.

Optimisation techniques at coding level and algorithm level are proposed to improve the performance of existing recognition systems.

### A. FACE FEATURE EXTRACTION

Let the data matrix X of the training samples of l classes be represented as $X= [x_1,.....,x_n]$ . Assume class consists of $N_i$ samples and the sum of all samples is N ie., $\sum_{i=1}^{1} N_i = N$ . Let the index set of samples from $i^{th}$ class be represented as $I_i$ ($1 \le i \le l$). The between class scatter matrix ($S_B$ ) , the within class scatter matrix ( $S_W$ ) and total scatter matrix ( $S_T$ ) are calculated u sing the class average sample $m_i = \left(1/N_i\right)\sum_{j\in I_i} X_j$ and the global average sample $m = \left(1/N\right)\sum_{j=1}^{N} X_j$ .where $S_B$ , $S_W$ and $S_T$ are given by the following formulae:

$$S_B = \sum_{i=1}^{l} N_i (m_i - m)(m_i - m)^T = H_b H_b^T \in R^{d\times d}$$

----------(1)

$$S_w = \sum_{i=1}^{l} \sum_{j\in I_i} (m_i - m)(m_i - m)^T = H_w H_w^T \in R^{d\times d}$$

----------(2)

$$S_T = \sum_{j=i}^{N} (x_j - m)(x_j - m)^T = H_t H_t^T \in R^{d\times d}$$

----------(3)

Where,

$$H_b = [\sqrt{N_1}(m_1 - m), \dots\dots\dots\dots, \sqrt{N_l}(m_l - m)] \in R^{d\times l}$$

----------(4)

$$H_w = [x_1 - m_{k1}, \dots\dots\dots\dots\dots, x_N - m_{kN}] \in R^{d\times N}, \quad m_{kj} = m_i$$

----------(5)

$$H_t = [x_1 - m, \dots\dots\dots\dots\dots\dots\dots, x_N - m] \in R^{d\times N}$$

---------- (6)

The average sample matrix is defined as

$$M = [m_1, \ldots\ldots\ldots\ldots\ldots\ldots, m_l] \in R^{d \times l}$$

The notations used in this paper are provided as appendix.

Now the steps involved for feature extraction are summarised as below:

**Step 1:** The initial precursor of the with – class scatter matrix $H_w$ is computed using Eqn 5.

**Step 2:** The initial average sample matrix M is calculated using Eqn.7

**Step 3:** For each sample *x* do,

1. Update M as $M \leftarrow [M\ x]$
   If *x* is a sample from a newly introduced class or,
   $M \leftarrow \frac{N_j . m_j + x}{N_j + 1}$, from the j[th] class
2. The precursor of the within class scatter matrix $H_w$ is updated as
   $H_w \leftarrow \left[H_w \sqrt{\frac{N_j}{N_j+1}}\left(x - m_j\right)\right]$

If *x* is a sample from the j[th] class.

**Step 4:** Perform eigen decomposition of the matrix $M^TM$ as $M^TM = V^TDV$.

**Step 5 :** Calculate the eigenvector matrix of $\sum = MM^T$ using $P \leftarrow MV_r D_r^{-1/2}$, where $D_r$ is a diagonal matrix with all non-zero eigenvalues, $V_r$ the corresponding eigenvector matrix, and r the rank of M.

**Step 6:** The between scatter matrix $\widetilde{\sum}$ and within class scatter matrix $\widetilde{S_w}$ are calculated in the intermediate space as

$\widetilde{\sum} \leftarrow (P^T M)(M^T P)$ and $\widetilde{S_w} \leftarrow (P^T H_W)(H_W^T P)$

**Step 7 :** Perform eigen decomposition of the matrix $\left(\widetilde{\sum}\right)^{-1}\widetilde{S_w}$ .

**Step 8:** The Discriminant matrix of the above obtained result is calculated using the formula U=PQ. Where Q is the eigenvector matrix of $\left(\widetilde{\sum}\right)^{-1}\widetilde{S_w}$ corresponding to k smallest eigenvalues.

The above obtained matrix is the feature vector of the face.

### B. KEY GENERATION FROM PALM VEIN

The cancelable vein template $U_D$ is divided in to two equal halves as $U_{D1}$ and $U_{D2}$.

$$U_{D1} = [u_{D1,}\ u_{D2}\ \ldots\ldots\ldots\ldots\ u_{Dn/2}]$$

and $$U_{D2} = [\ u_{D(n/2)+1}\ ,\ \ldots\ldots\ldots\ldots\ u_{Dn}]$$

The elements of $U_{D1}$ and $U_{D2}$ are shuffled as taking one element from a set and the modulo operation is performed between the current element and N/2, where N represents the total number of elements in $U_D$. The resultant value is denoted as **ind.** Subsequently the current element of $U_{D1}$ is placed in $\mathbf{SU}_{D2}$ at **ind[th]** position. The aforesaid process is repeated for all the elements of $U_{D1}$ and $U_{D2}$. Such shuffled value are stored in $\mathbf{SU}_{D1}$ and $\mathbf{SU}_{D2}$ Consequently the $\mathbf{SU}_{D1}$ and $\mathbf{SU}_{D2}$ are combined to form a vector $\mathbf{SU}_{D.}$

$$SU_D = [SU_{D1} \cup SU_{D2}]$$

The shuffled vector $\mathbf{SU}_D$ is converted into a matrix $\mathbf{MU}_D$ of size $MU_{size.}$

$$\mathbf{MU}_D = (a_{ij})\ MU_{size.}$$

Where $MU_{size} = \left(\sqrt{|SU_D|}\right)^2$

Finally the irrevocable key Vector $K_V$ is generated from the matrix $\mathbf{MU}_D$ . The final key is more secure and irrevocable.

### PROPOSED SCHEME –EXPERIMENT AND PERFORMANCE

The first stage in the proposed scheme starts with the capturing of face, fingerprint and palm vein data from different sensors. The templates of all the three data are achieved from the algorithms as discussed in above sections. The fingerprint template is normalised to 256 bit template to match the encryption process with the key generated from the palm vein. The fingerprint template is then prepared to be an encrypted one. A normal XOR operation is used to encrypt the fingerprint template and the encrypted fingerprint template is shown as,

$$E(n) = \sum_{i=1}^{n} fp(n) \oplus pv(n)$$

Where $E(n)$ represents the encrypted template for the size of template, n

$fp(n)$ represents the normalised fingerprint template

and $pv(n)$ represents the key generated from the palm vein.

The encrypted template $E(n)$ is a binary template which is transformed into a *2-D* vector $E_{ij}$

After encryption , $E(n)$ is encoded into the face image. Now $E_{ij}$ comprises the secret message to be hidden into the face image which is a binary vector. The secret message is shifted over 4 bits to the right. The Face template is also now converted into a stream of binary bits . The imbedded bits ie., the LSB is made zero in the cover image. Now the logical OR is applied between the secret image and cover image . The resulting image is the encoded image, which now contains the templates of all the biometric data used.

The decoding process is done as a reverse process of the previous action which results in the cover image (Face) and the secret image (Fingerprint + palm vein) . When the palm vein sample is scanned from the user at the time of verification / authentication the encrypted template is broken down into Fingerprint template and the palm vein , which inturn is used to recover the Face image.

## DISCUSSION AND RESULTS

A fingerprint database from the Fingerprint Verification Competition 2000 is used to test the experiment performance. The experiments shows that the proposed algorithm differentiates imposturous minutia pairs from genuine minutia pairs in a certain confidence level.

The following figure shows the Correct Score and Incorrect Score distribution:

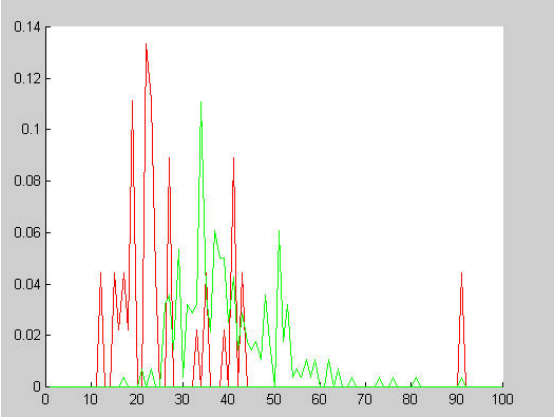



Figure 2 Distribution of Correct Scores and Incorrect Scores

Red line: Incorrect Score

Green line: Correct Scores

It can be seen from the above figure that there exist two partially overlapped distributions. The Red curve whose peaks are mainly located at the left part means the average incorrect match score is 25. The green curve whose peaks are mainly located on the right side of red curve means the average correct match score is 35. This indicates the algorithm is capable of differentiate fingerprints at a good correct rate by setting an appropriate threshold value.

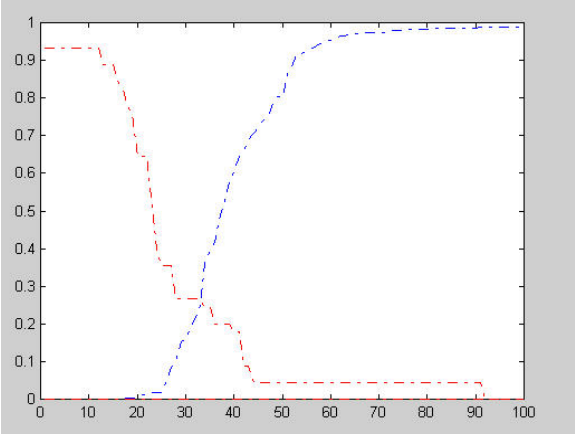



**Figure 3 Receiver operator characteristic curve**

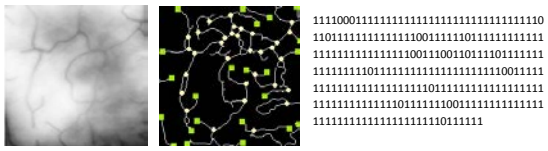
Blue dot line: FRR curve

Red dot line: FAR curve

The above figure shows the FRR and FAR curves. At the equal error rate 25%, the separating score 33 will falsely reject 25% genuine minutia pairs and falsely accept 25% imposturous minutia pairs and has 75% verification rate.

The high incorrect acceptance and false rejection are due to some fingerprint images with bad quality and the vulnerable minutia match algorithm.

As a next stage the palm vein image is extracted with tits features and the key is generated as shown in the following figure 4 .



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

**Figure 4. (a) ROI (b) Extracted Minutiae points (c) Generated Key**

With the above generated key the fingerprint features are embedded using the general XOR function. The final stage involves the encryption of the embedded image obtained from the previous stage into the face image on its features.

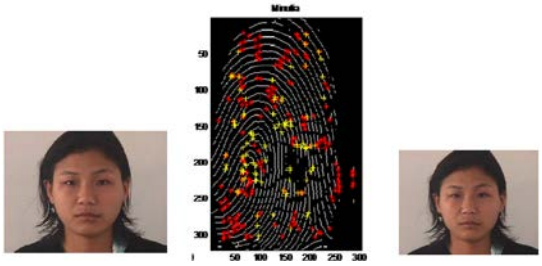


Figure 5: (a) Original face image (b) retrieved minutiae data (c) embedded face image

The retrieved minutiae data is stored as .dat file for further verification. About 14.266 % of the original face image is used for embedding.

The PSNR and MSE calculation is estimated as follows:

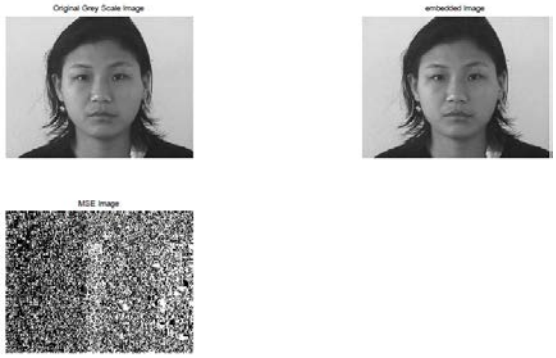


Figure ( a) Original grey scale image (b) Embedded image (c) MSE image.

The PSNR and MSE values obtained for the above image are 51.59 and 0.45 respectively.

On decrypting the embedded face image during verification process the .dat file of the realtime fingerprint is obtained and matched with the stored value. The palm vein image generates a key and decrypts the embedded image to obtain the original face image.

## CONCLUSION

On average when the entire system is implemented using MATLAB as individual modules it takes on average 50 seconds for enrolment and 22 seconds for verification . The estimated FRR is 0.01% and FAR is 0.00008% . If these are implemented as an on-card system or any smart card system as a future direction is expected to produce much better results.

## REFERENCES

[1] S.Prabhakar, S. Pankati, A.K.Jain, “Biometric Recognition : Security and Privacy Concerns”, IEEE Security and Priavcy, 2003, PP-33-42.

[2] Vein pattern recognition: www.fujitsu.com

[3] Chen.B and Chandran.V, “Biometric based cryptographic key generation from faces”, 9th Biennial Conference of Australian Pattern Recognition Society on Digital Image Computing Techniques and Applications, pp:394 -401, 3-5 Dec, 2007.

[4]Feng Hao, Ross Anderson, and John Daugman, “Combining Crypto with Biometrics Effectively”, IEEE transactions on Computers, vol 55(9), 2006.

[5]U. Uludag, S.Pankati, P.S and A.K.Jain, “Biometric cryptosystems: Issues and Challenges”, Proceedings of the IEEE 92, PP. 948-960, June 2004.

[6]Abishek Nagar, Chaudhury.S, “Biometrics based Asymmetric cryptosystem Design Using Modified fuzzy Vault Scheme”, 18th International Conference on Pattern Recognition, Vol 4, PP: 537-540, 2006.

[7] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," IBM systems Journal, vol. 40, pp. 614-634, 2001.

[8]Feng Hao,Ross Anderson, and John Daugman , “Combining Cryptography with Biometrics Effectively”, Technical results published by University of Cambridge Computer Laboratory ,2005.

[9]A.Jain, R.M.Bolle, S.Pankati, “Biometrics:Personal Identification in Networked Society” , Kluwer Academic Publishers, Dordrecht, 1999.

[10] P.MacGregor, R.Welford, “Veincheck: Imaging for security and personnel identification”, Advanced imaging, Vol6(7) , 1991 ,PP :52- 56.

[11] P.L.Hawkes, D.O.Clayden, “Veincheck research for automatic identification of people” , Presented at the Hand and Fingerprint Seminar at NPL, September 1993.

[12]Lingyu Wang, Graham Leedham ,David Siu-Yeung cho, “ Minutiae Feature Analysis for Infrared Hand Pattern Biometrics” , Pattern recognition Vol:41, ScienceDirect 2008,pp: 920-929.

[13]L.Waang, C.G.Leedham, " A Thermal Vein Pattern Verification Systems" ,Pattern recognition and Image analysis, Lecture notes in Computer Science , Vol :3687, Springer, 2005 ,pp .58-65.

[14]S.Im,H.Park,Y.Kim,S.Han,S.Kim, c.Kang, and C.Chung, " A Biometric Identification System by Extracting Hand Vein Patterns", Journal of the Korean Physical Society , Vol : 38(3) , 2001, pp. 268-272.

[15]Mohamed Shahin, Ahmed Badawi and Mohamed Kamel, "Biometric Authentication using Fast Correlation of Near Infrared hand Vein Patterns: ,International Journal of Biomedical sciences, Vol 2(3), 2007 ,ISSN 1306-1216.

[16]Eduard Sojka, " A new and Efficient Algorithm for Detecting the corners in Digital images" . Pattern recognition, Luc van Gool(Editor) ,LNCS 2449, pp.125 -132 ,Springer verlag ,2002.

[17]B.Prasanalakshmi, A.Kannammal, "A Secure Cryptosystem From Palm Vein Biometrics" . ACM International Conference Proceeding Series; Vol. 403 .Proceedings of the 2nd International Conference on Interaction Sciences: Information Technology, Culture and Human pp: 1401-1405 DOI: http://doi.acm.org/10.1145/1655925.1656183

[18] B.Prasanalakshmi , A.Kannammal, " Secure cryptosystem from Palm Vein Biometrics in Smart Card" Proceedings of the 2nd International Conference on Computer and Automation Engineering (ICCAE 2010) , Singapore PP-653-657 DOI: 10.1109/ICCAE.2010.5451311

[19] B.Prasanalaksmi, A.Kannammal, " Secured Authentication of Space- Specified Token with Biometric traits –Face and Fingerprint" , 2009 . International Journal of Computer Science & Network security , Vol. 9 No. 7 pp-231-234 http://paper.ijcsns.org/07_book/200907/20090732.pdf .