Biometric Encryption using Enhanced Finger Print Image and Elliptic Curve

G. Mary Amirtha Sagayee[1], S Arumugam[2], and G.S.Anandha Mala[3]

[1]Affiliated to the Department of Information Systems and Communications, Anna University, Chennai
[2]Department of Computer Science and Engineering, Nandha Engineering College, Erode, Tamil Nadu, India
[3]Department of Computer Science and Engineering, St Joseph College of Engineering, Chennai, India

Abstract
The greatest strength of biometrics is that it does not change over time. But at the same time while using it directly for enhancing the security in network system, if that data has been compromised, its compromised forever[1]. Therefore, cancellable biometrics will increase the privacy which means that the true biometrics are never stored or revealed to the authentication server. Biometrics, cryptography and data hiding will provide good perspectives for information security. Most of the researchers confirmed that the finger print is widely used than the iris or face and more over it is the primary choice for most privacy concerned applications. Also many mathematicians proved that Elliptic Curve is the best solution for Cryptography[10]. For finger prints applications, choosing proper sensor is at risk. The proposed work deals about, how the image quality can be improved by introducing image fusion technique at sensor levels. The results of the images after introducing the decision rule based image fusion technique are evaluated and analyzed with its entropy levels and root mean square error. Then the resultant enhanced image is used for extracting the key for ECC applications.

Keywords
Finger Print Image, Wavelet Neural Network, Image Fusion, Entropy, RMSE, Cryptography, ECC, Prime Field.

1. Introduction

The requirements of identification and authentication are increasing day by day in real time on line and offline applications. The Public as well as the private sectors are in a great need to identify to whom they are dealing with. Many security models for identification and authentications are available.

Most of the researches were demonstrating that Biometric is the ultimate solution for identification and authentication, since it is proved as reliable and universally acceptable identification/authentication methods in many application areas[15]. Biometric is referred as automatic system that uses measurable, physical or physiological characteristics or behavioral traits to recognize the identity of an individual. It is the characteristics of an individual (e.g. face, voice, fingerprint, gait, hand geometry, iris, gene, etc.). While comparing with traditional identify / authentication systems, biometrics offers greater security. In recent development of Information Technology, secured communication has become necessary. Cryptography is a kind of secret writing by which two parties can communicate with secret messages[17].

Due to the popularity of biometrics and cryptography, the information security is becoming as a common demand in all applications area. Enhancing the identification and authentication system using cryptography and biometrics are providing high assurance[14]. In the past decades, a lot of efforts have been taken in the combination of biometric and cryptography. There are two issues in this combination, such as the quality of the biometric image in data acquisition and the security/privacy concerns in enhancing information security[2]. We proposed an approach to enhance the biometric image by image fusion technique and to enhance the security by generating the cryptographic key from this enhanced biometric image.

In many researches, it is confirmed that the finger print is widely used than iris or face and more over it is the primary choice for most privacy concerned applications. It is most popular in market, comprising 32% of the total market due to the low cost implementation and high level of accuracy[15].

Many algorithms are proposed in Cryptography, which are based on symmetric and asymmetric key. In asymmetric cryptography system, private and public keys are involved, which is based on mathematical functions rather than on substitution and permutation. Elliptic Curve Cryptography (ECC) is a public-key cryptography system[10], in which a key pair is selected so that the problem of deriving the private key from the corresponding public key is equivalent to solve a computational problem that is believed to be intractable.

In this paper, we derived a mathematical approach for generating the key for ECC from the fingerprint image. The rest of the paper is organized as follows. In Section II, the fingerprint image enhancement by decision rule based image fusion technique and then the feature extraction from the enhanced fingerprint image are provided. Section III provides the mathematic approach to derive the cryptographic key from the resultant image template that is cable of providing better authentication / identification with security. Finally the conclusions are summarized in Section IV.

Manuscript received July 5, 2013
Manuscript revised July 20, 2013

2. DECISION RULE BASED FINGER PRINT IMAGE ENHANCEMENT

A. Image Enhancement:

The major drawback of fingerprint technology is contact nature of sensors such as inability of the sensing process to accommodate dirt and other environment[19]. The ability of the system to perform well is based almost solely based upon the quality of the biometric captured.
Multi-modal biometrics, or biometric fusion, is the process of combining information from multiple biometric readings, either before, during or after a decision has been made regarding identification or authentication from a single biometric. Fused Biometric image has the possibility to make identification more secure and more accurate than single biometric systems[2].
In our research, we think objects carry the information of interest, each pixel or small neighboring pixels are just one part of an object. Thus, we proposed a region-based fusion scheme. When make the decision on each coefficient, we consider not only the corresponding coefficients and their closing neighborhood, but also the regions the coefficients are in. We think the regions represent the objects of interest.

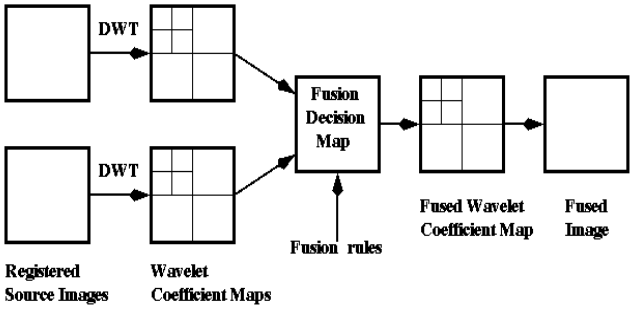

Figure. 1 Block Diagram region-based image fusion Technique.

In the proposed approach, the Neural Network and Fuzzy Logic approach can be used for image fusion. Such a image fusion could belong to a class of image fusion in which case the features could be input and decision could be output. The help of Neuro-fuzzy of fuzzy systems can achieve this.
The pixel level image fusion using the above approach by using Fuzzy Logic and the process of defining membership functions and rules for the image fusion process using FIS (Fuzzy Inference System) editor of Fuzzy Logic toolbox in Matlab are provided below as an algortithm.

B. Algorithm:

Step 1: Read the images into the variables M1 & M2 respectively. Variables MI and M2 are images in matrix form where each pixel value is in the range from 0-255. Use Gray color map.
Step 2: Apply wavelet decomposition and form spatial decomposition Trees and Convert the images in column form which has C= zl*sl entries.
Step 3: Create fuzzy interference system.

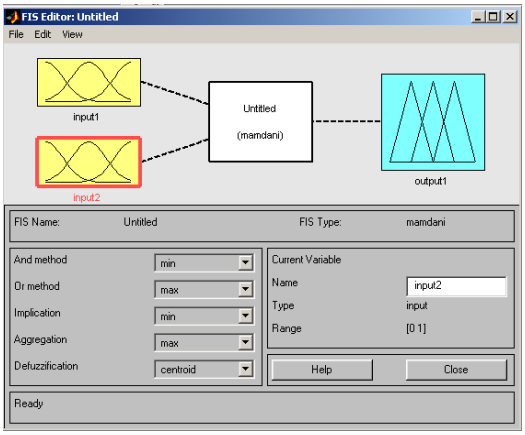

Figure 2. Fuzzy Interference creation

Step 4: Decide number and type of membership functions for both the input images by tuning the membership functions.

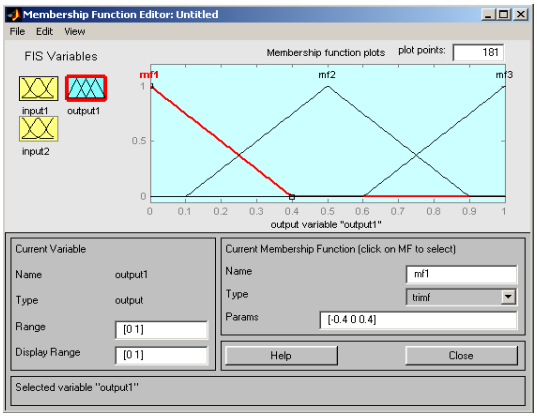

Fig 3. Tuning membership functions

Figure 3. Tuning the membership functions

Step 5: For num=l to C in steps of one, apply fuzzification using the rules developed above on the corresponding pixel values of the input images which gives a fuzzy set represented by a membership function and results in output image in column format.

Step 6: Convert the column form to matrix form and display the fused image.

C. Performance Evaluation

The performance evaluation is done by quantitative measures such as (1) Information Entropy and (2) Root Mean Square Error.

For an image consists of L grey levels, the entropy is defined as:

$$H = -\sum_{i=1}^{L} P(i)\log_2 P(i) \quad \text{..... (1)}$$

where is the probability (here frequency) of each grey scale level. As an example a digital image of type uint8 (unsigned integer 8) has 256 different levels from 0 (black) to 255 (white). It must be noticed that in combined images the number of levels is very large and grey level intensity of each pixel is a decimal, double number. But the equation is still valid to compute the entropy.

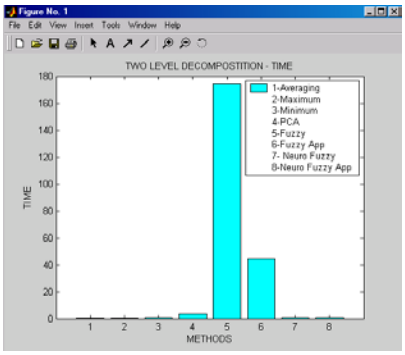

Figure 4. Time Analysis

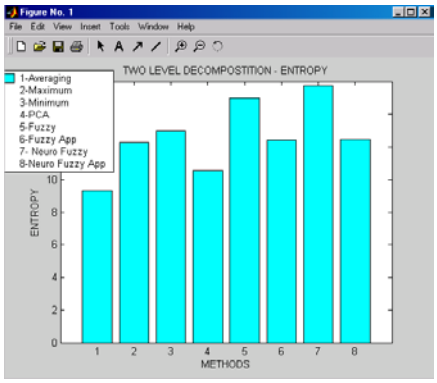

Figure 5. Entropy Analysis

For images with high information content the entropy is large. The larger alternations and changes in an image give larger entropy and the sharp and focused images have more changes than blurred and misfocused images. Hence, the entropy is a measure to assess the quality of different aligned images from the same scene.

The Root Mean Square Error between the reference image, I and the fused image is defined as: F

$$RMSE = \sqrt{\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\left[I(i,j) - F(i,j)\right]^2}{N.M}} \quad \text{....(2)}$$

where and i, j denotes the spatial position of pixels, M and N are the dimensions of the images. This measure is appropriate for a pair of images containing two objects.

Firstly, a "ground truth" image needs to be created that can be quantitatively compared to the fusion result images. This is produced using a simple cut-and-paste technique, physically taking the "in focus" areas from each image and combining them. The quantitative measure used to compare the cut-and-paste image to each fused image was taken from [1]

$$\rho = \sqrt{\frac{\sum_{i=1}^{N}\sum_{j=1}^{N}\left[I_{gt}(i,j) - I_{fd}(i,j)\right]^2}{N^2}}, \quad \text{...(3)}$$

where Igt is the cut-and-paste "ground truth" image, Ifd is the fused image and N is the size of the image. Lower values indicate greater similarity between the images Igt and Ifd and therefore more successful fusion in terms of quantitatively measurable similarity.

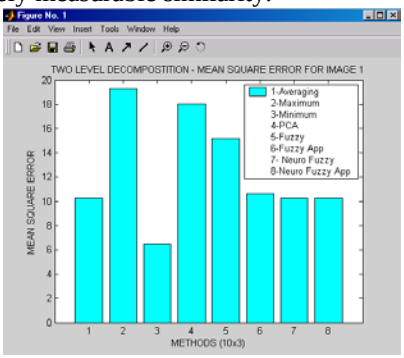

Figure 6. MSE for Source Image

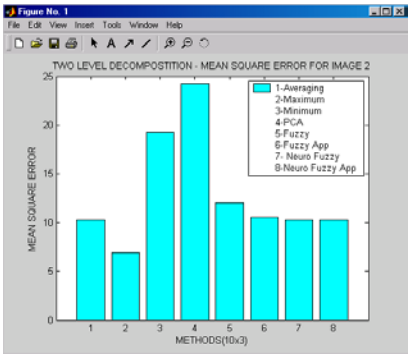

Figure 7. MSE for Fused Image

The following table shows the results for the various methods used. The average pixel value method, the pixel based PCA and the DWT methods give poor results relatively to the others as expected.

Table 1: Results of Various Fusion Methods

Different Tech		Entropy	Process Time	Mean Square Error	
				Image1	Image2
Two Max	Averaging	9.3198	0.5150	1.0241e+004	1.0241e+004
	Maximum	12.2813	0.5150	1.9268e+004	6.9486e+003
	Minimum	12.9647	0.5460	6.9486e+003	1.9268e+004
	PCA	10.5563	3.3280	1.8058e+004	2.4251e+003
Two Max Fuzzy		14.9813	174.7040	1.5173e+004	1.2026e+004
Two Max Fuzzy App		12.4181	44.7030	1.0643e+004	1.0581e+004
Two Max Neuro Fuzzy		15.7258	0.8750	1.0241e+004	1.0241e+004
Two Max Neuro Fuzzy App		12.4556	0.6250	1.0241e+004	1.0241e+004

In order to evaluate the results and compare these methods two quantitative assessment criteria Information Entropy and Root Mean Square Error were employed. In fact if the result of fusion in each level of decomposition is separately evaluated visually and quantitatively in terms of entropy, no considerable differences are observed. Experimental results demonstrated indicate that LPT algorithm reaches its best quality in terms of entropy in lower levels than DWT.

The RMSE values represented in Table show that neither LPT nor DWT has better performance in all levels, although the best result belongs to the LPT method. However the RMSE results compared to quality and entropy of fused images indicate that RMSE cannot be used as a proper criterion to evaluate and compare the fusion results.

Finally the experiments showed that the LPT approach is implemented faster than DWT. Actually LPT takes less than half the time in comparison with DWT and with regard to approximately similar performance, LPT is preferred in real-time applications. Fuzzy and Neuro-Fuzzy algorithms have been implemented to fuse a variety of images. The results of fusion process proposed are given in terms of Entropy and Variance. The resultant image after fusion is considered for further process.

III ELLIPTIC CURVE CRYPTOGRAPHIC KEY GENERATION FROM FINGER PRINT IMAGE

A. Cryptographic Key Generation:

Elliptic curves are mathematical constructs that have been studied by mathematicians since the seventeenth century.

In 1970s, private keys, which are not known to others, are used by both parties. In 1976, another method was devised by Rivest, Shamir and Adleman[6] for using cryptography with public key distribution. Both methods made fundamental use of the arithmetic in some algebraic object.

In 1997,Victor S.Miller[10] has suggested that the Elliptic Curves gives solutions to many issues in providing high security by finding the curves whose group orders are divisible by a small prime in order to provide a fast algorithm. Also It could reduce the problem of calculating discrete logarithms to the Diffe-Hellman problem.[5]

The following section will give the algorithms for embedding minutiae on elliptic curve and the biometric based key generation method. To encode plaintexts as points on some elliptic curve E defined over a finite field Fp. Here plaintext is nothing but the minutiae co-ordinate which is extracted from the fingerprint. Minutiae is represented in three co-ordinate system as (x,y,θ). To map the minutiae on to the elliptic curve, this three co-ordinate minutiae are converted into one co-ordinate system and then this single co-ordinate value is mapped on to elliptic curve.

Therefore in the proposed algorithm, by using these co-ordinates, the private key is generated. To generate the key, all the minutiae co-ordinates of the given image are to be extracted.

B. Algorithm:

First, add all x co-ordinates, y co-ordinates and co-ordinates separately and then take average value each co-ordinates separately. This resultant average values of X and Y co-ordinates are in decimal representation and the co-ordinate θ will be in radians.

Now this average values are converted into binary string separately subject to the condition that the input image should be resized into 256x256 array during preprocessing of the image for minutiae extraction. So maximum value for each co-ordinates require 9 bits for each X and Y co-ordinates to represent 256 and θ□ require maximum of 3 bits.

Finally, these three binary strings are converted into one co-ordinate value by concatenation these three binary strings, which will give the private key for the given finger print image. The algorithm for the above processes follows as below:

Step 1: Get the binary values X_{Bi}, Y_{Bi} and θ_{Bi} of X_i, Y_i and θ_i for ginve ith minutiae. 1<i< 0, where 0 is a number of minutiae.

Step 2: Concatenate all the binary values in the following order.

M_{Bi} = X Location (9bits) | Y Location (9bits) | Angle (3 bits)

Step 3: Convert the above concatenated binary string M_{Bi} to decimal to get the single co-ordinate value M_{1i}.

Let K be a large enough integer so that the failure probability of 1 out of 2^k will be satisfied when the plaintext m is attempted to imbed; in practice k=30. Suppose message units are integers 0 <= m <= M, then finite filed should be selected to satisfy q>Mk. Therefore the integers are from 1 to Mk in th form mk+j, where 1<=j<=k [3]. Thus the given m, for each j = 1,2,…,k obtain an element x of Fp corresponding to mk+j by using the following equation.

$$Y^2 = x^3 + a\,x + b \qquad \ldots(4)$$

Step 1: Let k = 30

Step 2: Xi = MBi + j whre 1 <=j<=k

Step 3. For each Xi, compute Yi using the following equation.

$$F(X_i) = Y_i^2 = X_i^2 + aX_i + b \bmod p$$

Step 4: If $f(X_i)$ is non square, then increment j by 1 and try again with new X_i.

Step 5: If j reaches K, then increment k

Step 6: Repeat the above steps for all minutiae

Step 7: Mapped points P_{mi} E(F_q)

Thus the single co-ordinate value is mapped on to the elliptic curve.

B. Experimental Results:

In real time application, it is applied in such a way that the enhanced finger print is given as input to the Minutiae Extractor. Output of Minutiae Extractor is the list of Minutiae Co-coordinators, which is given as input to the Key Generator, which will generates the biometric based keys private key and public key. Then elliptic curve digital signature generator generates digital signature for a given message using private key. This signature can be validated using elliptic curve digital signature validate using message and corresponding public key.

The minutiae extractor is implemented using Matlab on the window operating system. The various operations prime field, methods are available in java class and the remaining filed inversion and elliptic curve point operations over GF(P) and key generation, signature generation and verification programs are tested by using java.

More than 50 finger print images were tested using different ECC parameter sets. The results of the modules – minutiae extractor, key generator, signature generator and signature verifier are provided below:

The ECDSA using prime field biometric parameters are as follows:

- *The purpose is to test that signature can be generated and verified by using prime filed parameter which are derived from biometric image.*
- *The prerequisites are the finger pring and ECC parameters.*
- *The test data needed are the sample finger print image, Certicom Parameter and NIST Parameters.*
- *The steps to procced are to extract the minutiae from finger print, generate the keys from the* biometric data, generate the signature and verity it.

Figure 8. Finger Print Image

The following shows the results of the key generator, signature generator and signature verifier.

Table 2. Sample ECC parameter set

p	0158685C903F164390BA955
a	0C8AE4F7DE8918AA9FAB2260
h	1
S	B8ACF4D697D76786515175D2358C7B46DCABD6
r	00D7AE4F6ED9880AA9FBA626
b	00627E7EA0126AD68A7C1273
n	0148685D803EF905D7F57D46
X	00D021D85DBF9E50BA94C0A
Y	0007F73D1f779745CF676D0A
m	This is to verify the text

Table 3 The sample outputs

Module	Variable Name	Value
Key generation	Private Key	257981957269385662968496793
	Public Key X	2365189347632654981723800887
	Public Key Y	2693871048763968073865001799
Signature Generation	Signature r	3289502968703196832958701855
	Signature S	2098481759837465900471947699
Signature verification	v	3289502968703196832958701855
	Status	v = r, signature accepted

IV. Conclusion

In the recent development of Information Technology, communication with security is becoming as a necessary component in any application development. Also, Security is the foundation to privacy.

Our proposed work consists of two parts. In the first part of our work, the used of DWT, Fuzzy and Neuro Fuzzy, the fusion of biometric images were studied and identified that the Decision Rule Based Image Fusion Technique could be used in order to obtain a good quality image for further processing.

In the second part of our work, we proposed a method Elliptic Curve Cryptography by using Biometric Data, which provides greater security and more efficient performance than the first generation public key techniques (RSA and Diffie-Hellman). Even now it is in use because of the benefits and compatibility with security in terms of computational and bandwidth requirements.

The primary focus of our work is to obtain the cryptography key to secure the network by using enhanced biometric image. A combination of biometrics and cryptography will provide higher level of assurance for the legal information. Hence our work will enhance the cryptographic systems performance by improving the problem of key management.

Our future research will be focused on deriving the elliptic curve co-efficient from multimodal biometric measurement, by which the security and privacy could be enhanced.

References

[1] A.K. Jain, Y. Chen and M. Demirkus, "Pores and Ridges: High Resolution Fingerprint Matching Using Level 3 Features", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol 29, No 1, January 2007

[2] Huiqing Chen Gang Dong, Andawell Corp., Beijing; "Fingerprint Image Enhancement by Diffusion Processes" Image Processing, 2006 IEEE

[3] Koblitz.N A course in Number Theory and Cryptography, New York, Springer Verlog, Second Edition, 1994.

[4] Rebecca Heyer, "Biometrics Technology Review 2008", Defense Science and Technology Organization.

[5] Yvo Desmedt, editor, Advances in Cryptology – Crypto '96 volume 1109 of Lecture Notesin Computer Science, pages 271-281, New York, 1994, Springer-Verlag.

[6] Ronald Rivest, Adi Shamir and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. Comm. Assoc. Comput. March, 21:120-126, 1978.

[7] Shutao Li, James T. Kwok, Ivor W. Tsang, Yaonan Wang, " Fusing images with different focuses using support vector machines" IEEE Transactions on Neural Networks, 15(6):1555- 1561, Nov. 2004.

[8] P. J. Burt and R. J. Lolczynski, " Enhanced image capture through fusion" In Proc. the 4th Intl. Conf. on Computer Vision, pages 173-182, Berlin, Germany, May 1993.

[9] Z. Zhang and R. Blum, "A categorization of multiscale-decomposition-based image fusion schemes with a performance study for a digital camera application" Proceedings of the IEEE, pages 1315 -1328, August 1999.

[10] Victor S Miller. "Elliptic Curves and their use in Cryptograph", Advances in Cryptology Crypto '85, Lecture Notes in Computer Science, 218[1986), Springer-Verlab, 417-426.

[11] A. Bodo. Method for producing a digital signature with aid of a biometric feature.German patent DE 42 43 908 A1. June 30, 1994.

[12] G.J Tomko, C. Soutar and G.J Schmidt. Fingerprint controlled public key cryptographic system. U.S. Patent 5541994, July 30, 1996.

[13] C. Soutar, D Rogerge, A.Stoianov, R.Gilroy and B.B.K Vijaya Kumar. Biometric Encryption – Entrollment and Verification Procedures. Proc. SPIE, Optical Pattern Recognition IX, v. 3386,pp.24-35 1998.

[14] A. Burnett, F. Byrne, T.Sowling, and A.Duffy. A Biometric Identity Based Signature Scheme. Applied Cryptography and Network Security Conference, Columbia University, New York, USA, 2005.

[15] A.K. Jain, A. Ross, and S. Pankanti. Biometrics: A Tool for Inforamtion Security. IEEE transactions on information forensics and security, vol. 1, No.2, June 2006,pp.125-143.

[16] A. Juels and M.Sudan. A fuzzy vault scheme, proceedings 2002 IEEE International Symposium on Information Theory, Piscataway, NJ, p.408,2002.

[17] U. Uludag, S. Pankanti, S. Prabhakar, and A.K. Jain. Biometric Cryptosystems: Issues and Challenges. Proceedings of the IEEE, v.92,no. 6,June 2004, pp. 948-960.

[18] G.J. Tomko, C.Soutar, and G.J. Schmidt. Biometric controlled key generation. Oct. 21,1997

[19] Hong. L, Wan.Y and A. Jain, Fingerprint Image Enhancement: Algorithm and Performance Evaluation, IEEE

Trans. Pattern Analysis and Machine Intelligence, vol. 20, no.8, pp 777-789, 1998.
[20] National Institute of Standards and Technology, Digital Signature Standard, FIPS Publication 186, 1994.

Mary Amirtha Sagayee received B.E degree from Bharathidasan University, Thiruchirapalli, India in 1994, M.E degree from Anna University, Chennai 2005. Currently she is pursuing Ph.D degree from Anna University, Chennai, India.

G.S.Anandha Mala received B.E degree from Bharathidhasan University, Trichy, India in Computer Science & Engineering in 1992, M.E degree in University of Madras in 2001 and Ph.D degree from Anna University, Chennai, India in 2007. Currently she is working as Professor in St.Joseph's college of Engineering, Chennai, India, and heading the department of Computer Science and Engineering. She has published 20 technical papers in various international journal / conferences. She has 15 years of teaching experience on graduate level. Her area of interest includes Software Engineering,Grid Computing and Image Processing.

Arumugam received his Bachelors Degree and Maters Degree program at P.S.G. College of Technology, Coimbatore from the University of Madras in Electrical Engineering and Applied Electronics respectively in the year 1971 and 1973. He received his Ph.D. Degree in Computer Science and Engineering at College of Engineering, Chennai from Anna University. He held various positions as Lecturer., Assistant Professor, Professor and Principal at Government Colleges. He has guided 13 PhD. and 2 M.S.(By Research) scholars and presently guiding 24 Research Scholars. He has published more than 100 papers in International/National/Journals/Conferences. He is the holder of one Indian patent. He is member in professional bodies IEEE, IE(I), IETE, ISTE, and CSI. .Presently he is working as CHIEF EXECUTIVE OFFICER, Nandha Educational Institutions, Erode