International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

# Fingerprint Authentication using Adaptive RBF

**Fremina James[1], Dr. Prasanna V Kumar[2], Manoj Kumar Singh[3]**

[1]Assistant.Professor, Department of ISE, Brindavan College of Engineering, Bangalore, Karnataka, India

[2]Professor, Department of IT, R.V.College of Engineering, Bangalore, Karnataka, India

[3]Director, Manuro Tech Research Pvt.Ltd., Bangalore, Karnataka, India

**Abstract:** ***In this paper, we have proposed an adaptive radial basis function neural network which is based on adaptions of center and spread parameters involved in network design. This adaption is achieved through stochastic approach. Proposed adaptive form of architecture is applied to authenticate the fingerprint images. From individual fingerprint image, features based change is given to define the corresponding values of weights and radial basis function. Proposed method has shown remarkable advantage over fixed radial basis function neural network in feature extraction from fingerprint images***

**Keywords:** Biometrics, Authentication, Fingerprint, Radial basis function, center, spread parameter.

## 1. Introduction

With the advent of electronic banking, e-commerce, and smartcards and an increased emphasis on the privacy and security of information stored in various databases, automatic personal identification has become a very important topic.

Accurate automatic personal identification is now needed in a wide range of civilian applications involving the use of passports, cellular telephones, automatic teller machines, and driver licenses. Traditional knowledge-based(password or Personal Identification Number (PIN)) and token-based (passport, driver license, and ID card) identifications are prone to fraud because PINs may be forgotten or guessed by an imposter and the tokens may be lost or stolen. Therefore, traditional knowledge-based and token-based approaches are unable to satisfy the security requirements of our electronically interconnected information society as shown in Figure 1.

A recent survey showed that a fraud of around $450 million occurs every year with master card and credit card fraud which in turn is due to identity fraud. A perfect identity authentication system will necessarily have a biometric component. Eventually, a foolproof identity authentication system will have all the three components (knowledge-based, token-based, and biometrics).

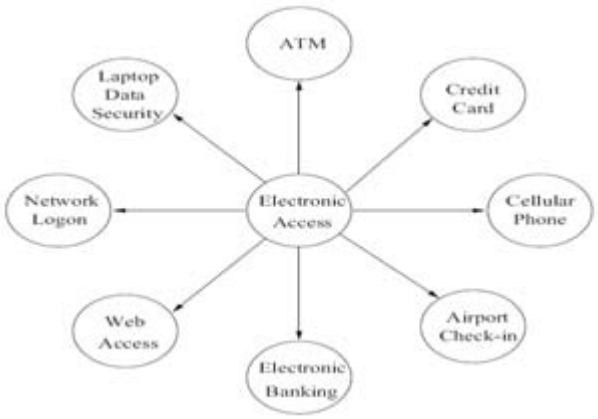



**Figure 1:** Various electronic access application that require biometric authentication

In this paper, we have focused only on the biometric component of an automatic identification system which is based on fingerprint biometric identification system in particular.

Biometrics, which refers to identifying an individual based on his or her physiological or behavioral characteristics, has the capability to reliably distinguish between an authorized person and an imposter. Since biometric characteristics are distinctive, it cannot be forgotten or lost, and the person to be authenticated needs to be physically present at the point of identification. Biometrics is inherently more reliable and more capable than traditional knowledge-based and token-based techniques. Biometrics also has some disadvantages. For example, if a password or an ID card is compromised, it can be easily replaced. However, once a biometrics is compromised, it is not possible to replace it. Similarly, users can have a different password for each account, thus if the password for one account is compromised, the other accounts are still safe. However, if a biometrics is compromised, all biometrics-based accounts can be broken-in. Amongst the various biometrics available such as the face, fingerprint, hand geometry, iris, retina, signature, voice print, facial thermo gram, hand vein, gait, ear, odor, keystroke dynamics, etc. , fingerprint-based identification is one of the most mature and proven technique.

## 2. Literature Survey

In [1] a proposal has been made for fingerprint authentication system for a mobile phone security application. A prototype of system is developed from the platform of BIRD E868 mobile phone with external fingerprint capture module. In [2] a new concept of FingRFis proposed as ongoing fingerprint research framework that links all fingerprint system components with some other supporting tools for performance evaluation. FingRF aims to provide a facility for conducting fingerprint research in a reliable environment. Moreover, it can be extended to include both off-line and on-line operational modes. A critical issue in biometric systems is to protect the template of a user which is typically stored in a database or a smart card. The fuzzy vault construct is a biometric cryptosystem

that secures both the secret key and the biometric template by binding them within a cryptographic framework. In [3] a fully automatic implementation of the fuzzy vault scheme based on fingerprint minutiae is presented. Since the fuzzy vault stores only a transformed version of the template, aligning the query fingerprint with the template is challenging task. Fingerprint verification is not only used to unlock these smartphones, but also used in financial applications such as online payment. Therefore, it is very crucial to secure the fingerprint verification mechanism for reliable services. In [4], authors have identified a few vulnerabilities in one of the currently deployed smartphones equipped with fingerprint verification service by analyzing the service application. In the last few years, fingerprint-based authentication has been widely used and implemented in smartphone with a type of small area sensor called "touch sensor". [5] presents an approach that used phase component of image for matching called Phase-Only Correlation (POC) method that is highly robust against noise, brightness change, and image shifting.

[6] presents scalable, efficient, and reliable privacy-preserving fingerprint authentication based on minutiae representation. The method is probably secure by leveraging the Yao's classic Garbled Circuit (GC) protocol. While the concept of using GC for secure fingerprint matching has been suggested earlier, to the best of our knowledge, no prior reliable method or implementation applicable to real fingerprint data is available. In [7] there is a Proposal for a secure means for fingerprint biometric authentication, which has the capability to deliver the user's privacy, their fingerprint template protection, and robustness against the various variations in terms of noise.

## 3. Functional Approach of RBF

In practice, the supervised training of the neural network can be considered as the curve fitting process. The network is presented with training pairs, each consisting of a vector from an input space along with a desired network response. Through a defined learning algorithm, the network performs the adjustments of its weights so that error between the actual and desired response is minimized relative to some optimization criteria. Once trained, the network performs the interpolation in the output vector space. A nonlinear Mapping between the input and the output vector spaces can be achieved with radial basis function.

The architecture of the RBF NN consists of three layers as shown in Fig2: an input layer, a single layer of nonlinear processing neurons known as hidden layer and the output layer. The output of RBFNN is calculated according to Equation (1).

$$y_i = f_i(x) = \sum_{k=1}^{N} W_{ik}\phi_k(x, c_k) = \sum_{k=1}^{N} W_{ik}\phi_k\left(\|x - c_k\|_2\right) \quad (1)$$

i=1, 2,….m

Where $x \in \Re^{n\times 1}$ is an input vector, $\phi_k(.)$ is a function from $\Re^{+}$ to $\Re$, $\|\cdot\|_2$ denotes the Euclidean norm, $W_{ik}$ are the weights in the output layer.N is the number of neurons in the hidden layer, and $c_k \in \Re^{n\times 1}$ is the RBF centers in the output space. For each neuron in the hidden layer, the Euclidean distance between its associated centers and the input to the network is computed. The output of the hidden layer is a nonlinear function of the distance. Finally the output of the network is computed as a weighted sum of the hidden layer outputs. The functional form of $\phi_k(.)$ is assumed to be given and is mostly Gaussian function as given by Equation (2).

$$\phi(x) = \exp\left(-x^2/\sigma^2\right) \quad (2)$$

Where $\sigma$ parameter controls the "width" of RBF and is commonly referred as spread parameter. The centers are defined points that are assumed to perform an adequate sampling of the input vector space. They are usually chosen as a subset of the input data.

In the case of the Gaussian RBF, the spread parameter $\sigma$ is commonly set according to the following heuristic relationship Equation (3).

$$\sigma = \frac{d_{\max}}{\sqrt{k}} \quad (3)$$

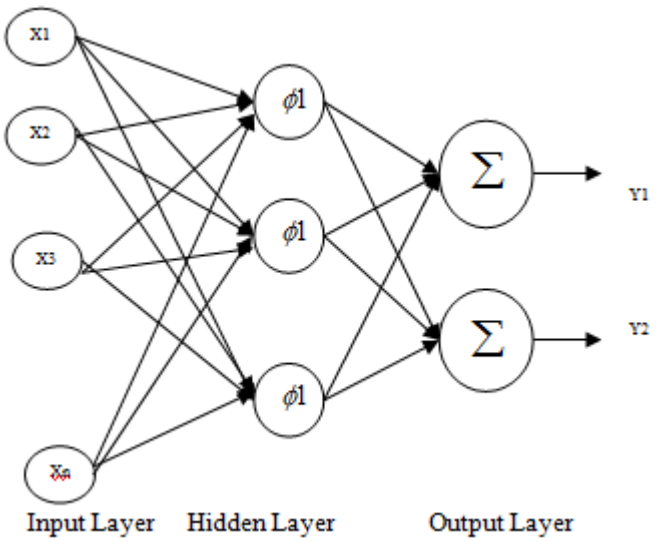



**Figure 2:** RBF NN architecture

Where $d_{max}$ is the maximum Euclidean distance between the selected centers and K is the number of the centers. Using Eq.3 the RBF of a neuron in the hidden layer of the network is given by

$$\phi(x, c_k) = \exp\left(-\frac{k}{d_{\max}^2}\|x - c_k\|^2\right) \quad (4)$$

### 3.1Training algorithm for an RBF NN with fixed centers

1) Choose the centers for the RBF function. The centers are chosen from the set of input vectors.
   A sufficient number of centers have to be selected in order to ensure adequate sampling of the input vector space.
2) Calculate the spread parameter for the RBF function
3) Initialize the weights in the output layer of the network to some small random number.
4) Calculate the output of the neural network.
5) Solve for the network weights.

Conventionally the center values are randomly sampled from the data set and the standard deviation is measured using the Euclidean distance available. This approach is appropriate only when there is highly concentrated data set available as very little variation exists. The performance can be improved by providing the optimal value of centers and corresponding standard deviations. The training of the parameters is a crucial part. Each parameter is updated based on the error in the output. Approach based on gradient mechanism is applied for the updating during each iteration.

### 3.2 Adaptive RBF NN

In the fixed center based RBF NN, there is only one adjustable parameter of network available and it is weights of the output layer. This approach is simple, however to perform adequate sampling of the input, a large number of centers must be selected from the input data set. This produces a relatively very large network.

In proposed method there are possibilities to adjust all the three set of network parameters that is weights, position of the RBF centers and the width of the RBF, Therefore, along with the weights in the output layer, both the position of the centers as well as the spread parameter for every processing unit in the hidden layer undergoes the process of supervised training. The first step in the development is to define instantaneous error cost function as

$$J(n)=\frac{1}{2}|e(n)|^2=\frac{1}{2}\left[y_d(n)-\sum_{k=1}^{N}w_k(n)\phi\{x(n),c_k(n)\}\right]^2 \quad (5)$$

When the chosen RBF is Gaussian, Equation (5) becomes

$$J(n)=\frac{1}{2}\left[y_d(n)-\sum_{k=1}^{N}w_k(n)\exp\left(-\frac{\|x(n)-c_k(n)\|_2^2}{\sigma_k^2(n)}\right)\right]^2 \quad (6)$$

The equations for updating the network parameters are given by Equation (7) to Equation (9).

$$w(n+1)=w(n)-\mu_w\frac{\partial}{\partial w}J(n)\Big\rangle_{w=w(n)} \quad (7)$$

$$c_k(n+1)=c_k(n)-\mu_c\frac{\partial}{\partial c_k}J(n)\Big\rangle_{c_k=c_k(n)} \quad (8)$$

$$\sigma_k(n+1)=\sigma_k(n)-\mu_k\frac{\partial}{\partial c_k}J(n)\Big\rangle_{\sigma_k=\sigma_k(n)} \quad (9)$$

#### 3.2.1 Adaptive RBF algorithm

1) Choose the centers of the RBF function. The centers are chosen from the set of input vectors.
2) Calculate the initial value of the spread parameter for the RBF function
3) Initialize the weights in the output layer of the network to some small random values.
4) Present an input vector, and compute the network output according to Equation (10)

$$\hat{y}(n)=\left[\sum_{k=1}^{N}w_k\phi\{x(n),c_k,\sigma_k\}\right] \quad (10)$$

1) Update the network parameters according to Equation (11) to Equation (13)

$$w(n+1)=w(n)+\mu_w e(n)\psi(n) \quad (11)$$

$$c_k(n+1)=c_k(n)+\mu_c\frac{e(n)w_k(n)}{\sigma_k^2(n)}\phi\{x(n),c_k(n),\sigma_k\}\{x(n)-c_k(n)\} \quad (12)$$

$$\sigma_k(n+1)=\sigma_k(n)+\mu_\sigma\frac{e(n)w_k(n)}{\sigma_k^3(n)}\phi\{x(n),c_k(n),\sigma_k\}\|\{x(n)-c_k(n)\}\|^2 \quad (13)$$

Where

$\psi(n)=[\{\phi(n),c_1,\sigma_1\},\phi\{x(n),c_2,\sigma_2\},.....\phi\{x(n),c_N,\sigma_N\}]^T$

$e(n)=\hat{y(n)}-y_d(n)$

$y_d(n)$ Is the desired network output, and $\mu_w,\mu_c,\mu_\sigma$ are appropriate learning parameters.

vi. Stop if the network converges, else go to step 4.

## 4. Finger Print as an Input Image

In the proposed concept the finger print image is considered as a whole instead of considering only the minutiae features. This has several advantages.

- The absence of any dominant minutiae feature caused by an accident, at the time of authentication may generate a negative response which is not acceptable.
- The extraction of minutiae is a tedious task. The extraction process completely depends upon the extraction algorithm used which becomes a subjective task.
- The minutiae features extracted vary with time.
- All the minutiae feature considered are macroscopic. There may exist several other important features which may be omitted but are visible when observed through deep vision.
- There is a need for pre-processing the image before extraction which may be time consuming.

To overcome all the short comings if the complete image is considered then the computational efficiency can be improved thereby improving the performance.

## 5. Experiment Results: Existing Versus Proposed System (Fixed RBF Versus Adaptive RBF)

To get the benefits with developed method number of fingerprint images have been taken for training purpose and both, fixed RBF and Adaptive RBF are applied independently for 100 iterations. Performance analysis is given in terms of obtained mean square error at the end as shown in Tables for all 10 different images. For first image, convergence characteristic, spread parameters adaptability and center position are shown in Fig3 to Fig5.

Comparative convergence characteristic for all the different cases are shown in Figure 6. It is evident that there is much lower MSE achieved with Adaptive RBF in comparison to fixed RBF in all cases. Experimentally 10 different gray scale fingerprint images are taken; each has a size of 512*512 pixels .Preprocessing is applied to each image in terms of normalization and division of each image as set of 10*10

pixel block. A RBF neural architecture containing 100 input nodes, 10 hidden nodes and 1 output node is created. Initialization of all weights is defined by random numbers by a uniform distribution in the range of [-0.5 0.5].

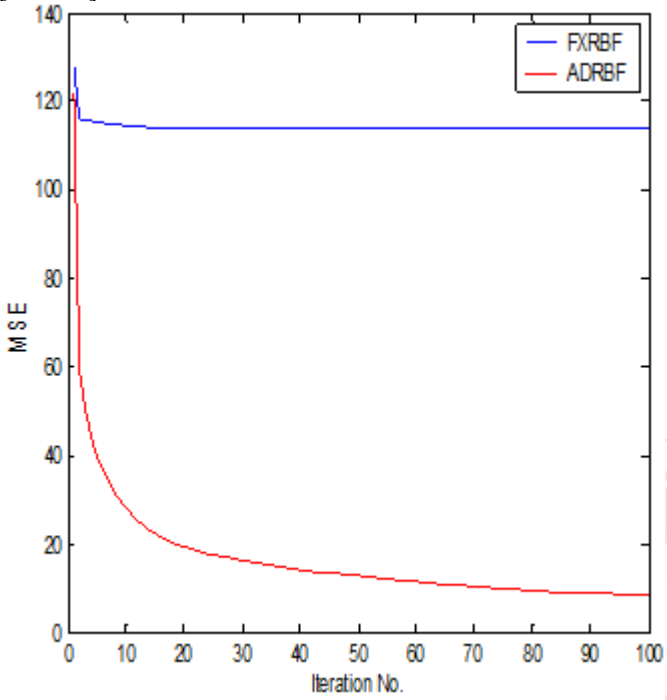



**Figure 3:** Relative convergence characteristic

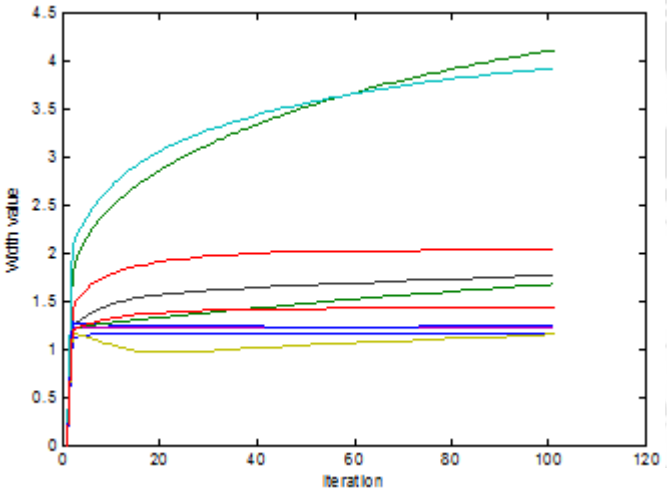
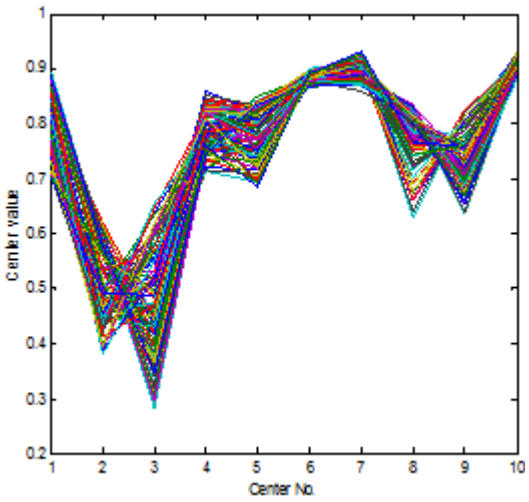



**Figure 4:** Adaptability of spread parameters over iterations




.**Figure 5:** Adaptability of center position for all 10 hidden nodes

**Table1:** Obtained Spread Parameters

| |
|---|
| FXRBF 1.2 |
| ADRBF 1.1593 4.1113 2.0301 3.9228 1.2300 1.1493 1.7644 1.2371 1.6728 1.4359 |

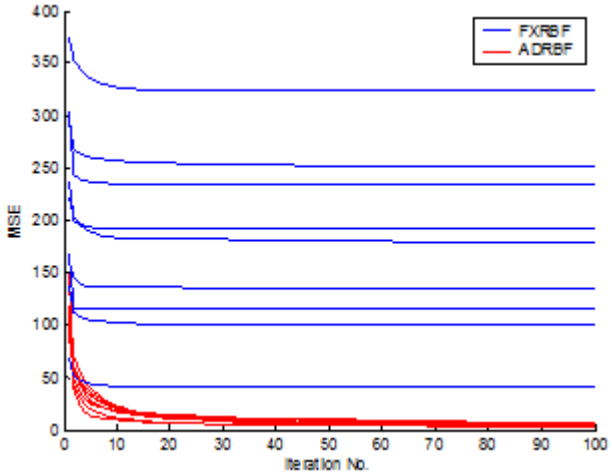



**Figure 6:** Comparative convergence characteristic for all images

**Table2:** MSE for all images at completion of training

| Image No. | FXRBF | ADRBF |
|---|---|---|
| 1 | 233.6456 | 5.2295 |
| 2 | 179.0486 | 7.2204 |
| 3 | 115.5387 | 4.5286 |
| 4 | 323.1047 | 2.9412 |
| 5 | 99.4260 | 5.8948 |
| 6 | 252.1058 | 3.5966 |
| 7 | 191.8951 | 3.1487 |
| 8 | 135.0327 | 5.1638 |
| 9 | 40.8406 | 3.9223 |
| 10 | 82.3403 | 3.5692 |

## 6. Fingerprint Authentication

Adaptive RBF is applied to authenticate the fingerprint images in development of correlation strength. Once, learning of one image is completed, the generated correlation strength

for each block is taken as output generated by neural network for that block and stored in an array which is defined for that particular image. In result an array corresponding to each image carries as much number of DC values as the number of blocks available in an image. Trained weights, center position and spread parameter corresponding to each image are also stored. In other words corresponding to each image there is an array containing a degree of correlation, a set of trained weights, centers position and spread parameters in memory.

In the test case, when any one of the image among those which have been trained is applied, preprocessing is applied to normalize and divide into same size of block (10*10). Degree of correlation is calculated with respect to stored set of weights. Absolute difference in correlation is obtained with each stored correlation value. Position of minimal total difference is established as final recognition of image and corresponding action is defined accordingly depending upon the nature of recognition, absolute or custom one. Fingerprint Images taken for simulation to create the data set are shown in Fig.7.Their correlation strength values are stored in the same order.

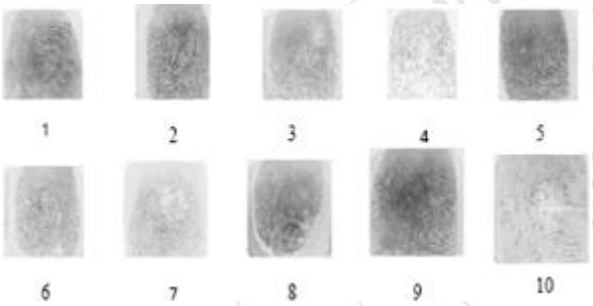



**Figure 7**: Fingerprint images taken in experiment

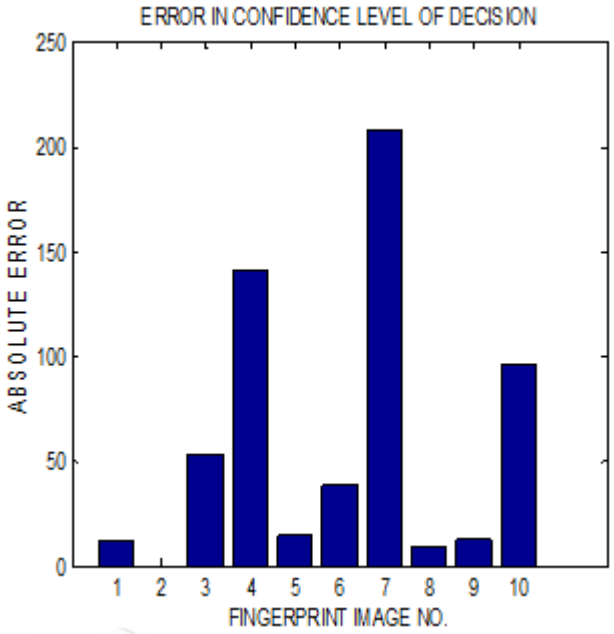



**Figure 8**: Error in correlation strength for authentication of image 2

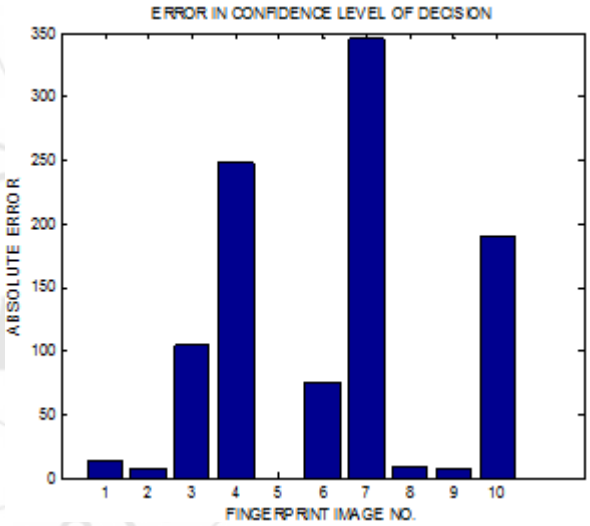



**Figure 9**: Error in correlation strength for authentication of image 5

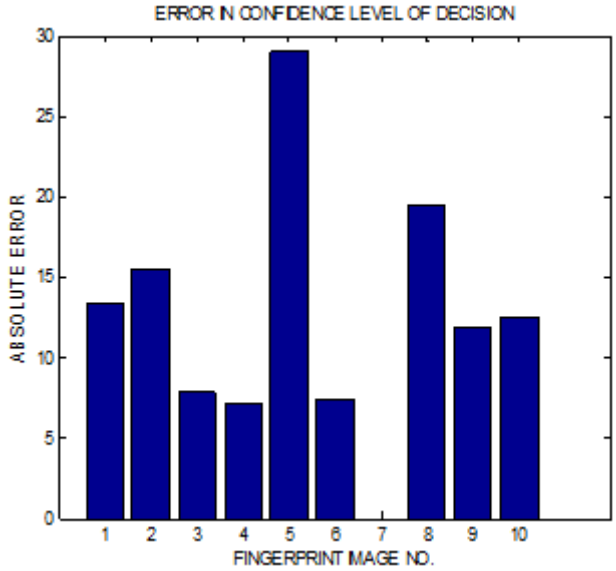



**Figure 10**: Error in correlation strength for authentication of image 7

Three different test case results for image 2, 5, and 7 are shown in Fig. 8 to Fig. 10 and their corresponding correlation strength is shown in Table3. It is clear that there is minimum error in correlation strength corresponding to the specified input fingerprint position which makes sure of authentication. It can be observed that there is very high difference in error of correlation obtained at the authentication process.

**Table3:** Correlation strength deviation for different test case

| Test Image | | | | | |
|---|---|---|---|---|---|
| 2 : | 11.3332 | **0** | 52.9743 | 140.9315 | 14.4134 |
| 38.2484 | 207.0811 | 8.6420 | 12.2872 | 95.8884 | |
| 5 : | 13.8222 | 7.3013 | 105.3545 | 247.8311 | **0**74.8439 |
| 345.0218 | 8.3119 | 8.0945 | 189.7724 | | |
| 7 | 13.3519 | 15.5148 | 7.8198 | 7.1600 | 29.0262 |
| 7.3909 | **0** | 19.4247 | 11.8748 | 12.4860 | |

## 7. Conclusions

We have proposed adaptive RBF neural network to authenticate the fingerprint images. Three different parameters have been applied to make the RBF adaptive like output layer weights, center position and spread parameters of RBF. Proposed method shows much lower value of MSE when compared to value obtained with fixed RBF. Because of presence of three different control parameters in RBF, there is higher robustness achieved in authentication process of fingerprint. Proposed solution also does not require storing the template of fingerprint images for recognition purpose, hence there is a high level of protection available with respect to personal information available with fingerprints and omits the chances of duplication.

## Reference

[1] Qi Su, Jie Tian, Xinjian Chen,Xin Yang,"A Fingerprint Authentication System Based on Mobile Phone", Audio- and Video-Based Biometric Person Authentication,Volume 3546 of the series Lecture Notes in Computer Sciencepp. 151-159

[2] Ali Ismail Awad,Kensuke Baba,"FingRF:A Generalized Fingerprints Research Framework", Technology, Volume 62 of the series lecture notes of the institute for computer science, social informatics.

[3] KarthikNandakumar,Anil K .Jain,SharathPankanti,"Fingerprint-Based Fuzzy Vault: Implementation and Performance", IEEE Transactions on Information Forensics and Security ( Volume: 2, Issue: 4, Dec.2007 )

[4] Young-Hoo Jo, Seong-Yun Jeon, 2 Jong-HyukIm and Mun-KyuLee,"Security Analysis and Improvement of Fingerprint Authentication for Smartphones". Mobile Information Systems, Volume 2016 (2016), Article ID 8973828.

[5] NabilahShabrina,TsuyoshiIsshikiHiroaki Kunieda,"Fingerprint authentication on touch sensor using Phase-Only Correlation method", Information and Communication Technology for Embedded Systems (IC-ICTES), 2016 7th International Conference .

[6] Ye Zhang, FarinazKoushanfar,"Robustprivacy-preserving fingerprint authentication",Published in: Hardware Oriented Security and Trust (HOST), 2016 IEEE International Symposium .

[7] Fremina James, Prasanna V Kumar, Manoj Kumar Singh, "Mixed Noise Tolerant Fingerprint Authentication Using Neuro", International Journal of Computer Engineering and Information Technology. VOL. 8, NO. 4,2016