International Journal of Security (IJS)

ISSN : 1985-2312

VOLUME 4, ISSUE 5

PUBLICATION FREQUENCY: 6 ISSUES PER YEAR

International Journal of Security (IJS)

Volume 4, Issue 5, 2010

Edited By
Computer Science Journals
www.cscjournals.org

Editor in Chief Dr. Wei Wang

International Journal of Security (IJS)

Book: 2010 Volume 4, Issue 5

Publishing Date: 20-10-2010

Proceedings

ISSN (Online): 1985-2320

IJS Journal is a part of CSC Publishers

http://www.cscjournals.org

Published in Malaysia

Typesetting: Camera-ready by author, data conversation by CSC Publishing Services – CSC Journals, Malaysia

CSC Publishers

Editorial Preface

This is the fifth issue of volume fourth of The International Journal of Security (IJS). The Journal is published bi-monthly, with papers being peer reviewed to high international standards. The International Journal of Security is not limited to a specific aspect of Security Science but it is devoted to the publication of high quality papers on all division of computer security in general. IJS intends to disseminate knowledge in the various disciplines of the computer security field from theoretical, practical and analytical research to physical implications and theoretical or quantitative discussion intended for academic and industrial progress. In order to position IJS as one of the good journal on Security Science, a group of highly valuable scholars are serving on the editorial board. The International Editorial Board ensures that significant developments in computer security from around the world are reflected in the Journal. Some important topics covers by journal are Access control and audit, Anonymity and pseudonym, Computer forensics, Denial of service, Network forensics etc.

The coverage of the journal includes all new theoretical and experimental findings in the fields of computer security which enhance the knowledge of scientist, industrials, researchers and all those persons who are coupled with computer security field. IJS objective is to publish articles that are not only technically proficient but also contains information and ideas of fresh interest for International readership. IJS aims to handle submissions courteously and promptly. IJS objectives are to promote and extend the use of all methods in the principal disciplines of computer security.

IJS editors understand that how much it is important for authors and researchers to have their work published with a minimum delay after submission of their papers. They also strongly believe that the direct communication between the editors and authors are important for the welfare, quality and wellbeing of the Journal and its readers. Therefore, all activities from paper submission to paper publication are controlled through electronic systems that include electronic submission, editorial panel and review system that ensures rapid decision with least delays in the publication processes.

To build its international reputation, we are disseminating the publication information through Google Books, Google Scholar, Directory of Open Access Journals (DOAJ), Open J Gate, ScientificCommons, Docstoc and many more. Our International Editors are working on establishing ISI listing and a good impact factor for IJS. We would like to remind you that the success of our journal depends directly on the number of quality articles submitted for review. Accordingly, we would like to request your participation by submitting quality manuscripts for review and encouraging your colleagues to submit quality manuscripts for review. One of the great benefits we can

provide to our prospective authors is the mentoring nature of our review process. IJS provides authors with high quality, helpful reviews that are shaped to assist authors in improving their manuscripts.

Editorial Board Members
International Journal of Security (IJS)

Editorial Board

Editor-in-Chief (EiC)

Associate Editors (AEiCs)

Editorial Board Members (EBMs)

Table of Content

Volume 4, Issue 5, December 2010

Pages

Protection of Patient Identity and Privacy using Vascular Biometrics

C. Lakshmi Deepika cldeepika@yahoo.com
Department of Biomedical Engineering
PSG College of Technology
Coimbatore -641004, India.

Dr. A. Kandaswamy hod@bme.psgtech.ac.in
Department of Biomedical Engineering
PSG College of Technology
Coimbatore -641004, India.

C. Vimal vimalc@ieee.org
Department of Biomedical Engineering
PSG College of Technology
Coimbatore -641004, India.

Abstract

Biometric systems are being used in hospitals to streamline patient registration and identification, as an effective measure to protect patient privacy and prevent identity theft. Many Hospitals and Healthcare institutions are turning towards Vascular Biometrics which complements the biometric recognition with hygiene and improved accuracy. In this paper, a multimodal hand vein system and a multibiometric fingerprint-hand vein biometric system are proposed. The multimodal hand vein system is a non-invasive, contactless and fast system, which uses two different feature sets extracted from each hand vein image. The multibiometric system captures both the fingerprint as well as the hand vein of the patient and hence offers even more improved performance though the speed and the cost of the system as well as the hygiene are reduced. We have used the Euclidean classifier to calculate the performance rates namely the False Rejection Rate (FRR) and False Acceptance Rate (FAR) of the Vein System and the Fingerprint-Vein System. We have performed this analysis using a volunteer crew of 74 persons. The FRR and FAR were 0.46% and 0.7% in the former case and 0% and 0.01% in the latter case respectively. The multimodal or the multibiometric system could be used based of the Hospital's requirements.

Keywords: Fingerprint, Vein, Biometrics, Fusion, Multimodal, Multi-biometric, FRR, FAR

1. INTRODUCTION

Today Biometric technology is spreading everywhere including hospitals. Biometrics is more accurate than names and numbers for collecting patient records. Some of the biometric identifiers include fingerprints, voice, face, and iris scans in physiological biometrics, and signatures, gait, keystroke dynamics in behavioral ones. These human traits possess the properties, such as universality, uniqueness, permanence, collectability, acceptability, and circumvention. Universality means that the particular biometric should be present for everyone universally and uniqueness

means that it should be unique to every person, even for identical twins. Permanence means that it should not change with time and Collectability means that it should be possible to acquire the biometric easily using simple electronic instruments and Circumvention means that it should not be possible to imitate or fake the particular biometric. A Face Recognition system is sensitive to illumination, pose and facial expressions of the subject. Facial accessories can also be easily spoofed by a static photo / moving video and further remain alike for identical twins. Hand Geometry is not very distinctive and cannot be used to identify an individual from a large population. The accuracy and speed of iris recognition systems are very high, but the cost and the amount of user participation required are also high [2, 3]. Fingerprint is a very popular biometric which is known for its high accuracy, ease of integration and low costs. Fingerprint scanners and processing algorithms are available in plenty. Though fingerprint is a universally accepted technology, one leaves traces of fingerprint everywhere and hence it can be easily traced and used to spoof the biometric system. Damage of fingerprint is common for people who do lot of manual work. Further fingerprint requires the user to put his finger in contact with the sensor. This results in dirt and moisture on the scanner which will then give noisy images. Vein Pattern is the network of blood vessels beneath the skin and this pattern is believed to be unique to every individual. Any part of the human body can be used for personal identification; however the hand veins are preferred since they are very close to skin and easily accessible. The hand vein biometric has scored very well in all the tests of the International Biometric Group (IBG) and according to Mr.Victor Lee, Senior Consultant at the International Biometric Group, vein patterns are really unique. The veins are present beneath the skin and overrule the possibility of an intruder obtaining access to it. Further vein patterns are not damaged or obscured by cuts, wounds or diseases. Vein pattern acquisition is a contact less technology and hence is more hygienic. The fingerprint and hand vein structures are randotypic traits, which form during the early phases of the embryonic development and are unique to identical twins and even to the left and right hands of the same person.

Currently, biometric systems are being used in hospitals to streamline patient registration and identification, as an effective measure to protect patient privacy and prevent identity theft. Hospitals are interested in implementing Vein biometric systems as they provide a way to identify patients who arrive unconscious at the emergency room. According to the IBG, Vein is the only biometric on par with the iris scans in terms of accuracy, which is of significant importance in hospitals to avoid mismatch between the patient and the medical record. Further vein recognition does not require any contact with the scanner and hence does not raise an issue with germs or bacteria. With several healthcare companies stepping into Vein biometrics, research in the same is gearing up. We wanted to measure the performance score of the vein pattern biometric, which is presented in this paper along with a detailed analysis of the same. We acquired the vein images using a low cost near IR camera. The morphological features in the form of bifurcations (branches) and terminations (endings) also called the minutiae were extracted from the vein images. A feature vector was created by concatenating the spatial coordinates of the positions of the minutia points. This was called the template, which is nothing but the representation of the particular biometric trait used for storage and further comparison. To test the uniqueness of the hand vein, it was necessary to acquire more number of images. Since we were not able to identify any publicly available hand vein database, we created our own database with a volunteer crew of 74 persons belonging to various age groups and both the gender [4]. It was noticed that the vein image obtained from a person at one instance may not be the same at another instance due to imperfections of producing the hand for acquisition such as rotation, scaling and translation. So the vein image was obtained for each person at ten different instances. Templates were generated for all the 740 images and tested to find out whether they were unique by a simple means, namely cross correlation, as a first step before going in for rigorous pattern matching. But from the cross correlation plot, it could be observed that the uniqueness was not very high. This could be attributed to the loss of details in vein images due to the low cost imaging setup. It was also necessary to fix a benchmark with popularly used biometric systems to assess the performance of hand veins. Since fingerprint is a very popularly used biometric, we compared the randomness of the hand veins with the fingerprints of the same person. For this a similar database with the same volunteer crew was created using the Verifinger Fingerprint acquisition

device. Fingerprint templates were created using similar fingerprint minutia points. A cross correlation plot between fingerprint templates was drawn. On comparing the vein and fingerprint plots, the fingerprints were found to be more unique than the hand veins for the given imaging setups of both the biometric identifiers. So to increase the randomness of the hand vein feature vector, we created one more feature vector by extracting the statistical data namely the moments from the hand vein images and fused this second feature vector with the first one which was created based on the morphology of the veins. Now the hand vein system is called multimodal. We again compared the randomness of the new vein template with that of the fingerprint template. It was noticed that the randomness of the fused hand vein feature vector was much higher than that of the fingerprint. So we proceeded to assess the performance by using two parameters namely the FAR (False Acceptance Rate) and FRR (False Rejection Rate). The rate of accepting the fake user (imposter) is called FAR and the rate of rejecting the genuine user as an imposter is called FRR. In this paper we have used the Euclidean Distance Classifier to classify a user as a genuine user or as an imposter. We obtained an FRR and FAR of 0.46% and 0.7% respectively for the multimodal hand vein templates. We also found out the performance of the fingerprint and the FRR and FAR were 4.81% and 2.07% respectively. Thus the Hand Vein system scores well in the various features of an ideal biometric system namely, non-invasiveness, contactless, speed and accuracy.

The experiment was extended to see if there was a further improvement in accuracy if a multibiometric system was used. Hence we fused the feature vectors of the fingerprint and hand vein templates and used the same distance based classifier to find the FRR and FAR. They were found to be 0% and 0.01% respectively. There is no biometric technology which would be equally suitable and feasible universally. The choice of the biometric system depends on the application and the environment. Hence we propose the hand vein system with fused morphological and statistical feature sets as an effective biometric system where the factors of hygiene, anti-spoof, cost-effectiveness and speed are more important. In an application where the utmost accuracy is required, a multibiometric system has to be used. The rest of the paper is organized as follows: Section II deals with Vein Image Acquisition, Section III with Vein Image Processing, Section IV with Fingerprint Image Acquisition, Section V with Fingerprint Image Processing, Section VI with Evaluation of the Multimodal System and Section VII with Evaluation of the Multibiometric System. The conclusions are provided in Section VIII.

2. VEIN IMAGE ACQUISITION

Vein Pattern Recognition is relatively an unexplored area in Biometrics and hence no public database is available. To validate our proposed fusion method, we have created a database of vein images of 74 individuals. Blood vessels are present beneath the skin and hence are not visible to the human eyes or the conventional cameras, which are sensitive to light only in the wavelengths 400 –700nm. The imaging techniques used to capture vascular images are X-rays, Ultrasonic Imaging and Infrared Imaging. Infrared Imaging is a non-invasive contact less technique and hence is preferred over the others. There are two IR imaging technologies, the Near IR and Far IR Imaging. The Far-IR imaging technique captures the thermal patterns emitted by the human body. This thermal profile is unique even to identical twins. Near IR cameras on the other hand capture radiation in the range 800 – 1100 nm of the electromagnetic spectrum. The experiments conducted by Wang Lingu and Graham Leedam [9] show that Near IR imaging is comparatively less expensive and also gives good quality vein images. They have also found that Near IR imaging is more tolerant to environmental and body conditions and provides a stable image. ZhongBo Zhang et al [10], Junichi Hashimoto et al[11] use Finger Vein Patterns. However since the hand veins are bigger, we use the veins at the back of the hand. Lin and Fan [12] use the palm veins, captured by an Infracam, a high cost IR camera.

We propose a relatively low cost imaging setup using a WAT 902H near IR camera. With our setup, we found that when the fist is clenched, the veins appear more prominent in the captured image rather than the veins in the palm. Hence we have captured the vein pattern at the back of the hand. According to Medical Physics, the hemoglobin in blood is sensitive to light in the

wavelength range of 800 – 1100 nm and absorbs the same. Hence the blood vessels in the superficial layer of the body appear dark compared to the other parts of the hand. The WAT 902H is a monochrome CCD camera. To increase the sensitivity of the capturing setup, an IR filter of 880 nm wavelength is mounted in front of the camera lens. An unexposed Ektachrome color film served effectively as an IR filter. An IR source consisting of IR LEDs was used to illuminate the back of the hand [13-18]. The output of the camera which is an analog signal is transferred to the computer using a PIXCI frame grabber. Ten images were obtained from each of the 74 individuals. A database of 740 images was thus created. The acquisition was done in a normal office environment at room temperature. The skin colors of the subjects varied from fair to dark. The distribution of the age of the subjects varied from 21 years to 55 years. The images were obtained for both the gender. It was observed that age, gender and skin colors do not play any role in the clarity of the vein image obtained.

The failure to enroll rate which measures the proportion of individuals for whom the system is unable to generate templates was found to be 0.1%. Fig 1 shows the Image Acquisition setup we have used to capture Vein Images. The user has to place his hand in the 'hand placement area' with the fist clenched.

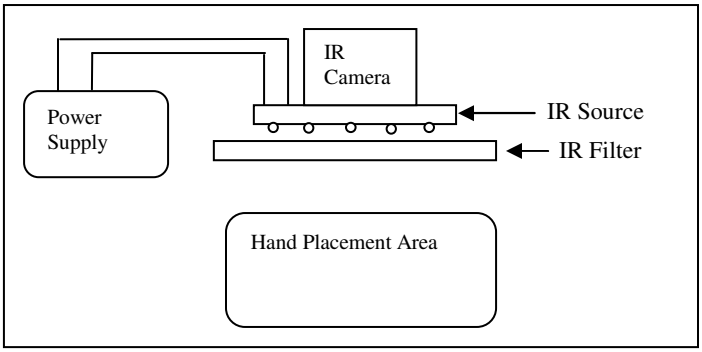

FIGURE 1: Outline of the Image Acquisition Setup

We observed that acquired vein images are independent of skin color and unique to both the left and right hands. The Acquisition setup used in our system is a low cost setup. The WAT 902H camera is a low cost camera compared to cameras like the Thermal Tracer, Infracam, etc. Also, we have fabricated our own LED power source whose radiation is also well within the acceptable limits, namely 5,100 Watts/sq.m..The IR filter we have used is easily and cheaply available than the conventional IR filters such as the Hoya filters.

3. VEIN IMAGE PROCESSING AND FEATURE EXTRACTION

The captured raw vein image has unwanted details such as hair, skin, flesh and bone structures. The image is also contaminated with noise due to extraneous lighting effects and sensor noise. Hence, before extracting the morphological features, pre-processing is done as shown in Fig 2.

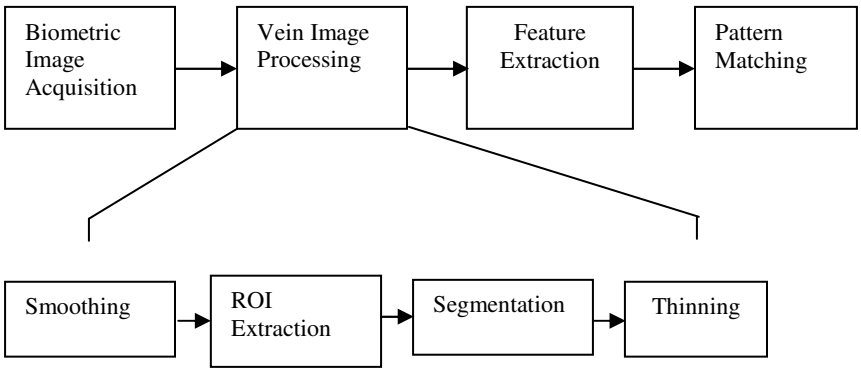

FIGURE 2: Entire Setup

3.1 Smoothing

Noise introduces high frequency components in the image. Median filter is popularly used to remove noise [14,17-18]. We propose an anisotropic diffusion process similar to the physical diffusion process where the concentration balance between the molecules depends on the density gradient. In anisotropic diffusion, for the given image u(x,y,t), the diffusivity 'g' depends on the gradient as shown in (1)

$$\begin{aligned} g &\rightarrow 0 \ for \ |\nabla u| \rightarrow \infty \\ g &\rightarrow 1 \ for \ |\nabla u| \rightarrow 0 \end{aligned} \qquad (1)$$

We have calculated the gray value of each pixel iteratively depending on the gray value gradient in a 4-pixel neighborhood surrounding the pixel. The gradient is calculated using the non-linear diffusion function 'g' so that the smoothing is more over the homogenous regions rather than the edges, so that the edges remain sharp. The noisy and noiseless images are shown in Fig 3.

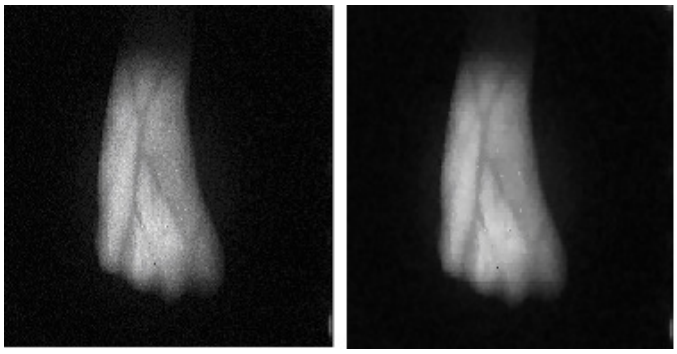

FIGURE 3: Noisy and Noiseless Images

3.2 ROI Selection

We propose an iterative method to extract the ROI. The hand image is binarised to extract its outline as shown in Fig 4(a). Horizontal and Vertical scans are done to assess the size of the image as the size differs from person to person. A rectangle is generated and centered on a window. The size of the rectangle, which depends on its length and breadth, is altered in accordance with the size of the hand by altering an amplification factor. The portion of the hand inside the rectangle is extracted as the region of interest as seen in Fig 4(b) and further in Fig 5(a).

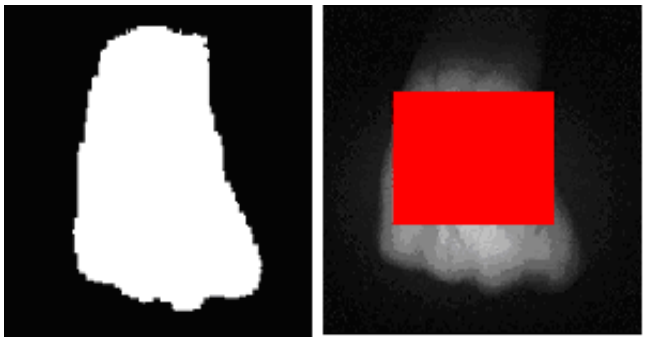

FIGURE 4: (a) Binarised hand image **(b)** ROI Selection

3.3 Segmentation

Ling u Wang et al and Kejun Wang et al [19] use a local dynamic threshold based segmentation process where the threshold is determined for each pixel by examining an r x r neighborhood of each pixel. In order to reduce the complexity by reducing the number of times the threshold is calculated, we propose a histo-threshold based segmentation to extract the vein structure from the background of the flesh and skin. It is seen that the gray level intensity values of the vein image vary at different locations of the image. Hence different threshold values are chosen for different gray levels in the image. The gray levels available in the image are extracted from the histogram of the image. The thresholds chosen are 0, 255 and all minima extracted from the histogram. This method reduces the number of thresholds determined and hence the complexity of the segmentation process.

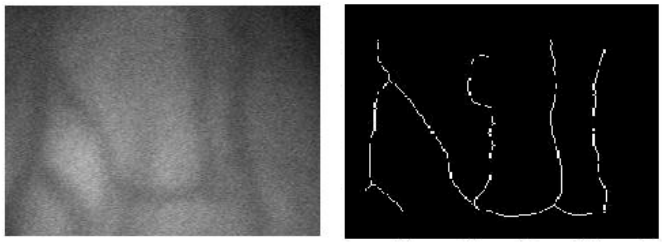

FIGURE 5: (a) ROI **(b)** Thinned Image

3.4 Thinning

The segmented vein image is skeletonised by a morphological operation called thinning. Fig 5(b) shows the thinned image, where the veins have shrunk to a minimally connected stroke. Then the operator “spur” is used to remove the end points of lines without allowing objects to break apart.

Now, it is required to extract the so called minutia points which are nothing but the bifurcations and terminations in the vein image. Kejun Wang et al [19] have extracted the endpoints and cross points from vein images similar to the extraction of minutiae points in a fingerprint image. However this method is a extensive process due to additional process of removing false minutiae. We propose to extract the corners in the vein image as suggested by Sojka [8]. He defines a corner as an intersection of two straight non-collinear gray value edges. Let ‘Q’ be an image point and let Ω be its certain neighborhood. The probability ‘P’ of any point ‘X’ lying in Ω having the same brightness as ‘Q’ is calculated. Let g(X) be the size of the brightness gradient and $\varphi(X)$ represent the direction of the brightness gradient at ‘X’. Let w(r(X)) be a weight function that represents the distance between ‘Q’ and ‘X’ as seen in (2).

$$W = \sum_{X_i \in \Omega} P(X_i) w(r(X_i)) \qquad (2)$$

$$\mu_{\varphi} = \frac{1}{W} \sum_{X \in \Omega} P(X_i) w(r(X_i) \varphi(X_i) \quad (3)$$

$$\sigma_{\varphi}^{2} = \frac{1}{W} \sum_{X_i \in \Omega} P(X_i) w(r(X_i))[\varphi(X_i) - \mu_{\varphi}]^2 \quad (4)$$

The image points for which the size of the gradient of brightness is greater than a predefined threshold (we have fixed it to be 30) are considered to be the candidates for the corners. The minutiae points have a structure as seen in Fig 6. The distances between the points are calculated and are shown in Table 1.

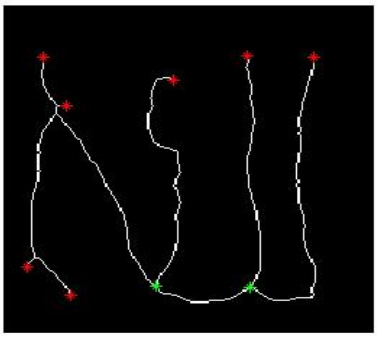

FIGURE 6: Minutia Points of Veins

9.0091	18.6605	25.9185	34.1359	36.3658
45.5350	46.8286	48.1460	61.7604	62.7712
92.1861	100.9359	103.0000	108.4836	116.7833
122.3319	125.3357	128.5756	130.9969	131.5991
133.8963	145.2548	148.9285	153.0000	163.9538

TABLE 1: Distances between Minutia points

The graph in Fig 7 shows the distribution of minutia points for 5 persons. It can be seen that they are well apart and unique to each person.

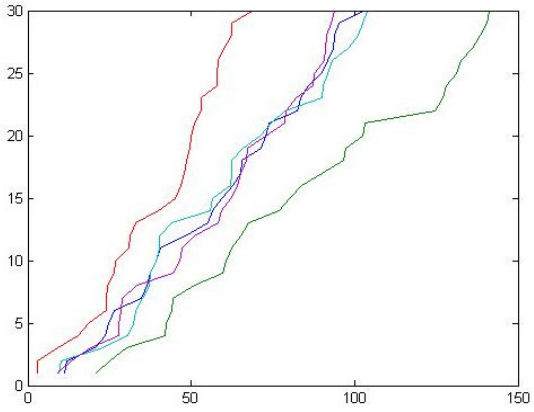

FIGURE 7: Endpoint and cross point distances for 5 persons

The minutia points are concatenated to form the feature vector. The uniqueness of the templates (feature vectors) of different persons decides to a large extent the accuracy of a biometric system. Hence to find out how far apart the feature vectors are, we picked up some samples and estimated the cross correlation between them which is seen in Fig 8. The plot in Fig 8 does not help to arrive at any conclusion. By and large, fingerprint is one of the ancient and still popular biometric used all over the world. Fingerprint scanners and processing algorithms are available in plenty. Hence we wanted to compare the randomness of the hand veins with that of the fingerprint.

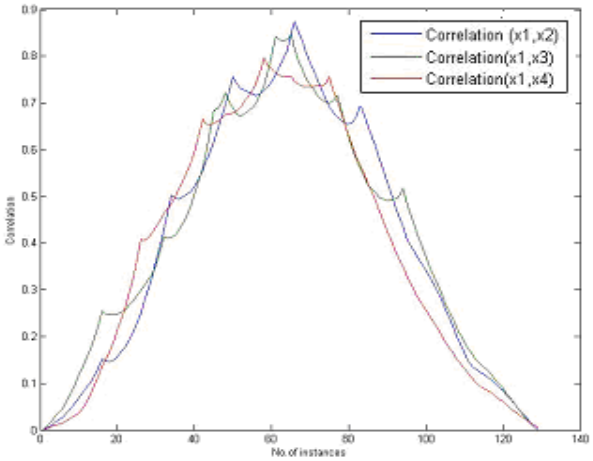

FIGURE 8: Cross Correlation Plot of Hand Vein

4. FINGER IMAGE ACQUISITION

"Verifinger" fingerprint scanner shown in Fig 9 was used to scan and digitize the images of the right thumbs of the subjects. The subjects were advised to present only the right thumb to maintain consistency and to give only the necessary pressure on the sensor since too much of pressure would create distorted and noisy images. The sensor was interfaced to the computer to transfer the fingerprint images for further processing.

FIGURE 9: Fingerprint Scanner

The Fingerprints in the database had variations among themselves since the skin dryness, oiliness and roughness varied for each person.

FIGURE 10 (a): Fingerprint with multiple cuts

While most of the images were clear, some people had multiple cuts and sometimes wide cuts in both the left and right thumb and hence were not able to enroll in the database at all.

FIGURE 10 (b): Fingerprint with wide cuts

These cuts result in loss of efficiency compared to clear images as shown in Fig 10(c)

FIGURE 10 (c): Clear Fingerprint Image

4. FINGERPRINT PROCESSING

The fingerprint images obtained from the scanner have ridges and furrows. The parts of interest are the bifurcations (branches on ridges) and terminations (endings of ridges). The dirt or residual remains on the scanner can result in noise. A simple gaussian filter was sufficient to remove noise. The image also had several broken ridges. Hence rigorous enhancement was needed before further processing.[6] The image was repaired by using Fast Fourier Transform (FFT). The FFT was performed on small sized blocks of 32x32 pixels as seen in (5).

$$F(u,v) = \sum_{x=0}^{M-1} \sum_{y=o}^{N-1} f(x,y) \exp\{-j2\Pi \left[\frac{ux}{M} + \frac{vy}{N} \right]\} \quad (5)$$

Where u = 0, 1…31 and v = 0,1,…31. M,N = size of the image. f = input image, F=FFT image. The FFT of each block is multiplied by its magnitude a set of times, in order to boost the dominant frequencies in each block. The enhanced image is obtained by taking the Inverse Fourier Transform of the product as seen in (6).

$$g(x,y) = F^{-1}\{F(u,v) \mid F(u,v) \mid^k \quad (6)$$

Where g(x,y) is the enhanced image and 'k' is an experimentally determined constant. The optimal value of 'k' was 0.45. For this particular value, the holes in the ridges were filled up. Above 0.45, false joining of ridges was seen to occur. The Inverse Fourier Transform which gives back the image in the spatial domain was obtained using (7).

$$f(x,y) = \frac{1}{MN} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} F(u,v) \exp\{j2\Pi[\frac{ux}{M} + \frac{vy}{N}]\} \quad (7)$$

To improve the overall contrast of the fingerprint image, FFT enhancement was followed by Histogram Equalisation and the final enhanced image is as seen in Fig 11.

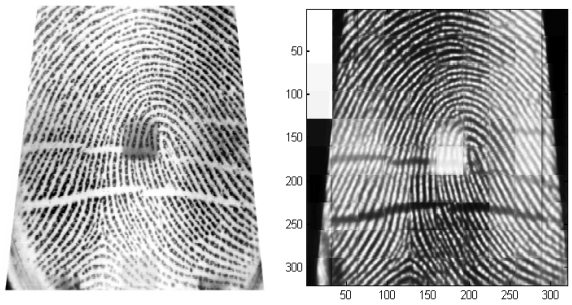

FIGURE 11: (a) Original Image **(b)** Enhanced Image

It could be seen that there are unwanted information at the boundaries of the fingerprint image. Hence the image had to be segmented to extract the region with maximum information. Before segmentation, the image was binarised as seen in Fig 12. The binarisation method adopted was a locally adaptive binarisation method where the mean intensity value of every 16 x 16 block was calculated and based on it, every pixel value in the block was transformed to 1 if its intensity was greater than the mean and made to be zero, if its intensity value was less than the mean. Now, in the image, the ridges are black and the furrows are white so that it is easy to discern the terminations and bifurcations.

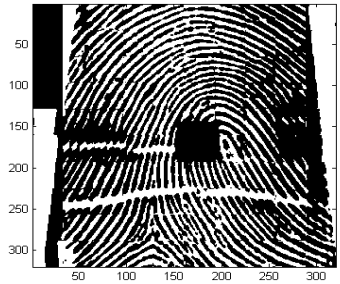

FIGURE 12: Binarised Image

Segmentation of the background from the rest of the image was carried out as a two step process: First, the direction of each 16 x 16 block was estimated. Since the background would have the minimum number of ridges and furrows, it would have the minimum gradient. The gradient in both 'x' and 'y' directions, namely gx and gy were calculated for each block using the Sobel filter, whose masks are: [1 2 1;0 0 0;-1 -2 -1] and its transpose. The certainty level of each block was calculated using (8). The blocks with certainty level

$$E = \{2\sum\sum(gx * gy) + \sum\sum(gx^2 - gy^2)\}/W * W * \sum\sum(gx^2 + gy^2) \qquad (8)$$

Below 0.05 were segmented out as background as seen in Fig 13(a).

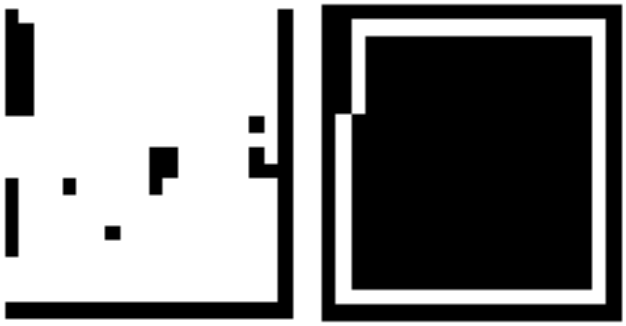

FIGURE 13: (a) Background Blocks **(b)** Morphologically Transformed Image

The background blocks are seen at the boundary as well as inside the image. The blocks inside the image were eliminated using the morphological operations Dilation followed by Erosion as seen in Fig 13(b)

To obtain the region of interest, we propose a method of ROI extraction, where, from the set of columns of pixels with information greater than zero, the column with minimum information is chosen to be the leftmost column of the area of interest and the column with maximum information becomes the rightmost column. The transpose of the image is taken and same process is repeated to get the top and bottom of the ROI as seen in Fig 14 (a). The ROI was multiplied with the binarised image to get the binarised ROI as seen in Fig 14(b). The next step in the process was skeletonising the image. The binarised RoI was reduced to a single pixel thickness by a thinning process. This is essential to mark accurately the minutia points. The thinned image is shown in Fig 15(a).

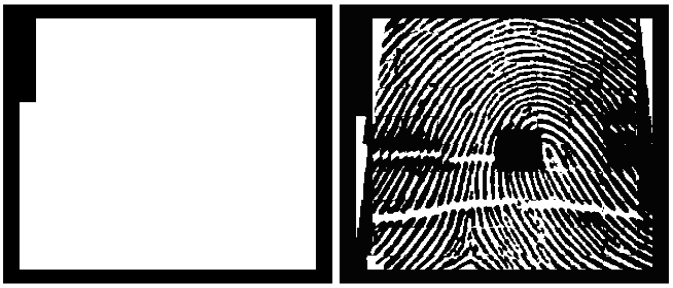

FIGURE 14: (a) ROI Boundary **(b)** ROI in Image

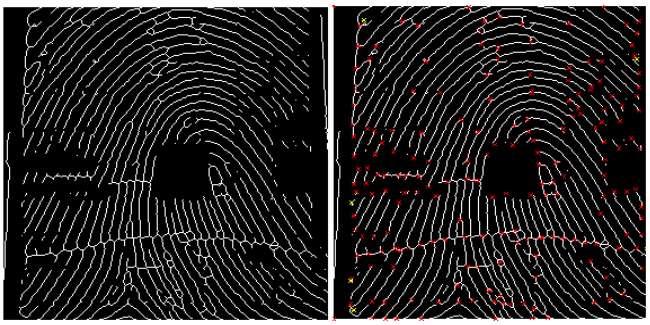

FIGURE 15: (a) Thinned Image **(b)** Minutia Points

The termination points and bifurcation points on the ridges are called minutiae. However false ridge breaks and false ridge cross connections would result in false minutiae. To remove these points, the inter ridge width was calculated and the termination and bifurcation points on the same ridge separated by the inter ridge distance were removed. The minutia were extracted using the method proposed by Sojka, similar to the extraction process used for vein images. The minutia points are marked in Fig 15(b). Fig 16 shows the distribution of the x, y, θ values of the minutia points of two persons.

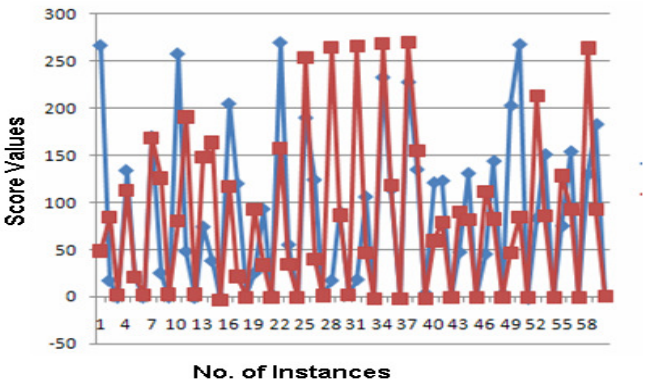

FIGURE 16: Minutiae Distribution for two persons

It can be seen that they are unique to some extent. In order to compare with the hand vein we obtained the cross correlation plot of the fingerprint which is shown in Fig 17.

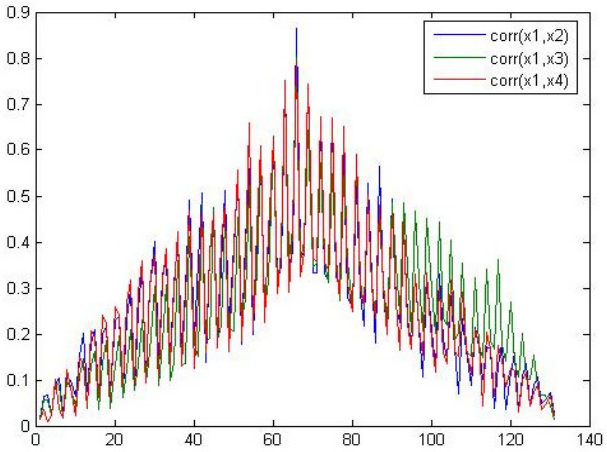

FIGURE 17: Cross Correlation Plot of Fingerprint

Comparing Fig 8 and Fig 17, we see that the correlation or similarity is more between hand veins than the fingerprint. Even though there are various advantages such as spoof-resistance, contactless acquisition, etc., the randomness and hence the accuracy of the hand vein system is low. This is due to the low cost imaging setup we have used which fails to capture a few veins that do not appear prominent enough. Hence to improve the randomness with the same imaging setup, we propose a fusion method.

6. EVALUATION OF MULTIMODAL SYSTEM

To increase the randomness of the hand vein feature vector, we propose addition of more information to it, by fusing yet another feature set, namely the statistical data.

Each feature vector can be considered as a random variable and the distribution of the feature vectors taken at ten different instances with the same subject, as a random process. Moments are calculated for all the seventy-four random processes. In our paper we have used seven invariable moments as proposed by Hu, to describe each random variable, namely the feature vector. For a discrete image f (i,j), of size M x N, its geometry moment in p+q ranks, where p,q are constants can be defined as in (9).

$$M_{pq} = \sum_{i=1}^{M} \sum_{j=1}^{N} i^p j^q f(i, j)$$
$$i \in M, j \in N \qquad (9)$$
$$Set\ \mu_{pq} = \frac{M_{pq}}{M^r}, r = \frac{(p + q + 2)}{2}$$

The 7 absolute moments which are rotation scaling and translation invariant are taken as given by (10)

$$M_1 = \mu_{20} + \mu_{02}$$
$$M_2 = (\mu_{20} - \mu_{02})^2 + 4\mu^2_{11}$$
$$M_3 = (\mu_{30} - 3\mu_{12})^2 + (3\mu_{21} - \mu_{03})^2$$
$$M_4 = (\mu_{30} + \mu_{12})^2 + (\mu_{21} + \mu_{03})^2$$
$$M_5 = (\mu_{30} - 3\mu_{12})(\mu_{30} + \mu_{12})[\mu_{30} + \mu_{12})^2 - 3(\mu_{21} + \mu_{03})^2]$$
$$+ (3\mu_{21} - \mu_{03})(\mu_{21} + \mu_{03})[3(\mu_{30} + \mu_{12})^2 - (\mu_{21} + \mu_{03})^2 \qquad (10)$$
$$M_6 = (\mu_{20} - \mu_{02})[(\mu_{30} + \mu_{12})^2 - (\mu_{21} + \mu_{03})\ ] +$$
$$4\mu_{11}(\mu_{30} + \mu_{12})^2(\mu_{21} + \mu_{03})$$
$$M_7 = (3\mu_{12} - \mu_{03})(\mu_{30} + \mu_{12})[(\mu_{30} + \mu_{12)})^2 - 3(\mu_{21} + \mu_{03})^2]$$
$$+ (\mu_{30} - 3\mu_{12})(\mu_{21} + \mu_{03})[3(\mu_{30} + \mu_{12})^2 - (\mu_{21} + \mu_{03})^2]$$

The moments take on values for one instance of a person as follows for example: 19.61538, 381.7633, 383.7633, 769.5266, 592171.2, 296085.6, -592171. The distribution of moments for 5 different instances of the same person is shown in Fig 18.

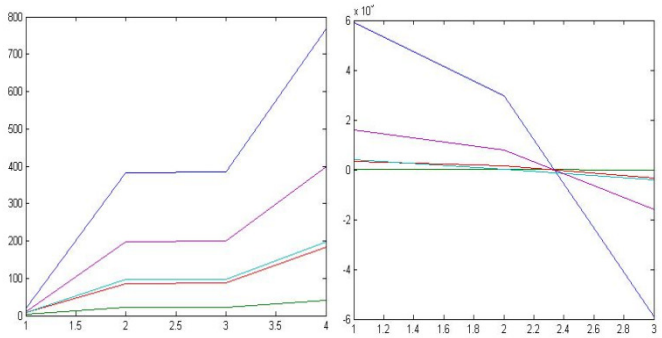

FIGURE 18: Moments M1, M2, M3, M4 and M5, M6, M7

It can be seen the moments calculated are indeed rotation, scaling and shift invariant. The feature vectors created using the two different feature extraction algorithms are fused to form a single feature vector. It can be seen from the distributions that the minutia points and moments are entirely two different entities with different nature and different distributions in space. Being totally independent modalities, these two data sets, when fused give a feature vector whose randomness is further increased, this in turn enhances the accuracy of the system. This was verified by again observing the cross correlation between the fused feature vectors as shown in Fig 19

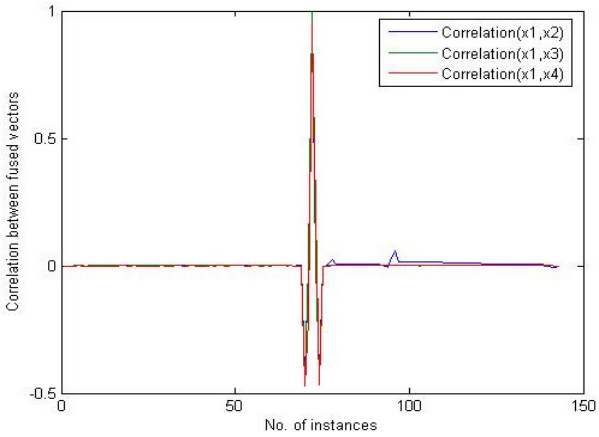

FIGURE 19: Cross correlation among Fused Vectors of the Hand Veins

It can be seen that the variation between different subjects is more, or the correlation is less when the pattern classification is done using the fused vectors. Hence we consider only the feature vectors created by concatenating the morphological data and statistical data, for identification and now the system is said to be multimodal.

To compare the performance scores of the Hand vein and Fingerprint systems, it was necessary to create a fingerprint database. Using the same volunteer crew of 74 persons from whom we obtained the hand veins, we obtained the fingerprint images. Ten instances of fingerprints are stored for each person. For calculating the score, for each person, five are taken as the standard set and five are taken as the testing set. The similarity between the standard images and the test images was measured using the Euclidean Distance Metric. Euclidean distance classifier uses genuine and imposter score for classification. The genuine score is generated by calculating the Euclidean Distance between the testing set and the standard set of the same individual. Same procedure is followed for all the individuals in the database. The distance will be less between the various instances of the same persons. Thus the total count of genuine score is 74x5x5=1850.

Imposter score is generated by calculating the Euclidean distance between a person's testing set and the standard set of all other members. It is repeated for all individuals. Thus the total count of imposter score is 370x365=135050.

A Threshold is set based on the genuine and imposter scores. If the Euclidean distance calculated is less than the threshold, they are recognized as genuine persons. If the score is greater than the threshold, the person is recognized as an imposter. The genuine and imposter scores are shown in Fig 20(a) and (b) respectively.

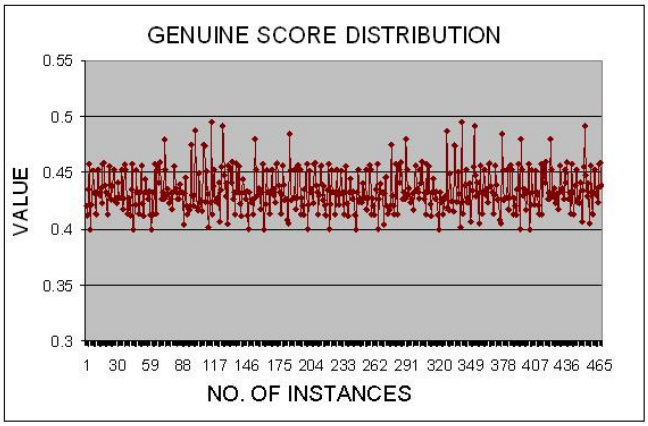

FIGURE 20 (a): Genuine Score Distribution of Fingerprint

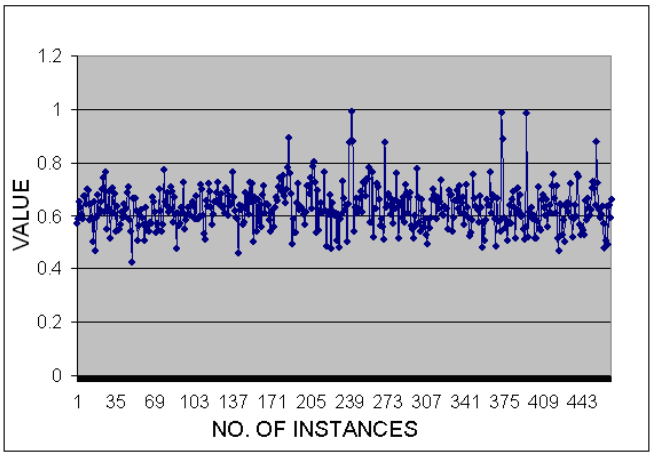

FIGURE 20 (b): Imposter Score Distribution of Fingerprint

The Euclidean distances between the input feature vector and those in the database are calculated using (11)

$$W(k) = \sum [(f_{iw} - f^{k}{}_{iw})^2 / (\delta^{k}{}_{iw})^2] \qquad (11)$$

Where, f_{iw} is the 'i'th feature of the input feature vector and f_{iw}^{k} is the 'i'th feature of the template feature vector in the database, δ_{iw}^{k} is the standard deviation of the template set.
If the distance between the input vector and the vectors in class 'k' are less than a threshold, then the input hand vein is classified as the 'k'th class.

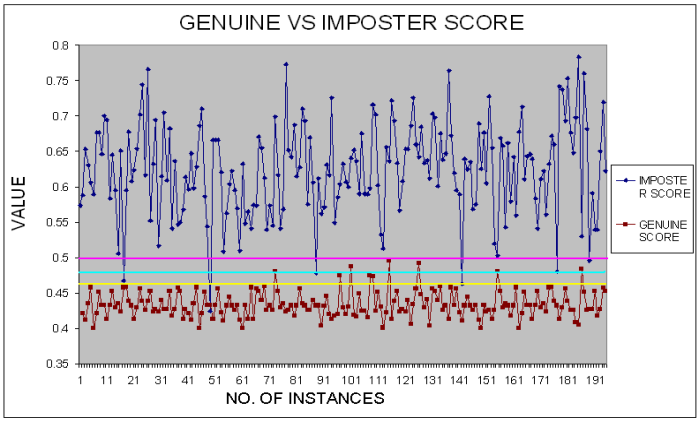

FIGURE 21: Genuine Vs Imposter Scores for Fingerprint

It can be seen in Fig 21 that the genuine score and imposter score overlap at certain points. Hence an optimal threshold is chosen so that, if the match score is less than the threshold, the person is recognized as a genuine user and if greater than the threshold, the person is recognized as an imposter. The case where a true user is considered as an imposter and rejected is called false rejection; and the case where an imposter is recognized as a true user is called false acceptance. The False Acceptance Rate (FAR) and the False Rejection Rate (FRR) vary according to the threshold chosen as seen in Table 2.

Threshold	FAR(%)	FRR(%)
0.5	2.02	1.4
0.475	**1.2**	**1.52**
0.46	0.9	2.7

TABLE 2: Determination of FAR and FRR for Fingerprint

The threshold is chosen to be 0.475, since it has optimal FAR and FRR. Similarly the genuine and imposter scores of the hand vein pattern were calculated for the fused vectors and are shown in Fig 22(a) and (b).

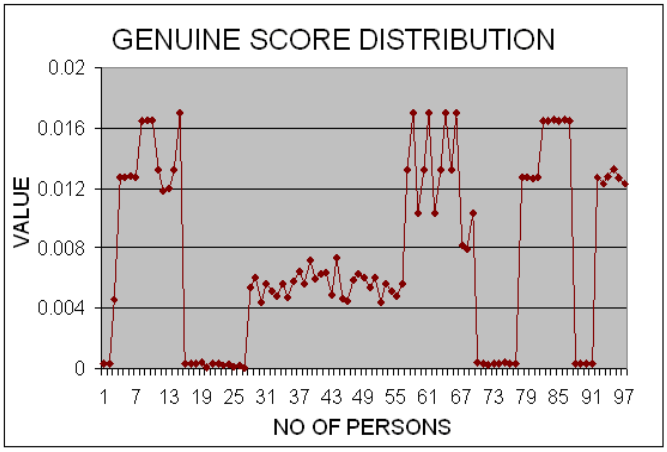

FIGURE 22(a): Genuine score Distribution for Hand Veins

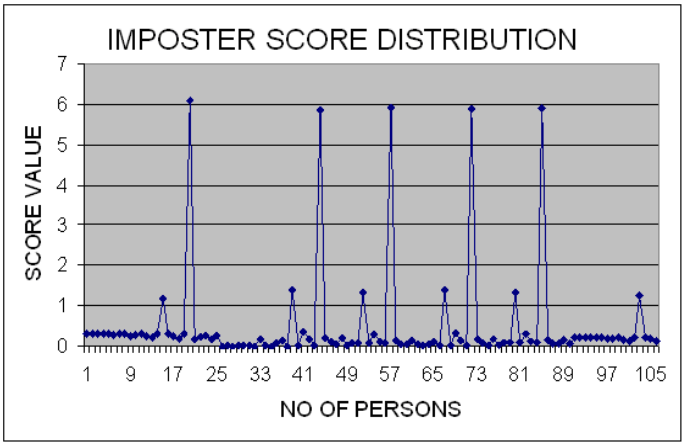

FIGURE 22(b): Imposter score Distribution for Hand Veins

From the genuine and imposter scores we fixed the threshold to be 0.01, where we had minimum overlapping of both the distributions. With this threshold, we obtained an FAR of 0.7 and FRR of 0.46.

It can be seen that the hand vein system with fused feature vectors performs much better than the fingerprint. Another type of multi-biometric system is one which fuses the feature sets of two different biometric modalities and is called a multbiometric system. Section VII discusses the performance of the multibiometric system which fuses the hand vein and fingerprint features.

7. Evaluation of Multi-Biometric System

Here the fusion was done by concatenating the feature set of vein and fingerprint. Let X= {x1, x2…xm} and Y= {y1, y2…yn} denote the feature vector representing the information extracted from vein and fingerprint respectively. Vector Z is formed by concatenation of these two feature sets. However the two feature sets had widely varying range and scale of values. Hence normalization was done to the feature vector before concatenation, to ensure that they are in the same range and scales of values. Min-max normalization performs a linear transformation on the original data. Suppose that min and max are the minimum and the maximum values for attribute A. Min-max normalization preserves the relationships among the original data values. It maps a value v of A to new_v in the range [new-min, new-max] by computing new_v as seen in (12)

$$new\_v = \frac{v - \min_x}{\max_x - \min_x}.(new\_\max_x - new\_\min_x) + new\_\min_x \qquad (12)$$

Let X_{norm} and Y_{norm} represent the normalized feature sets of vein and fingerprint. These features are then concatenated into a single feature set as concat= (X_{1norm}… X_{2norm} ……Xm_{norm} ...$Y_{1\ norm}$, $Y_{2\ norm}$, ……Yn_{norm}). The resultant vector was not of an optimal length. Hence the redundant features in the fused set were removed using "K-means" clustering techniques, which choose the most proximate feature to the mean of the cluster.

Similar to the previous case, the Imposter and Genuine scores were calculated and are shown in Fig 23 (a) and (b).

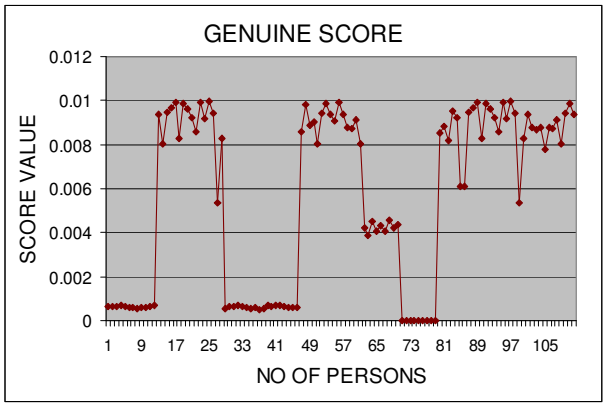

FIGURE 23(a): Genuine Score Distribution for Fingerprint-Hand Vein System

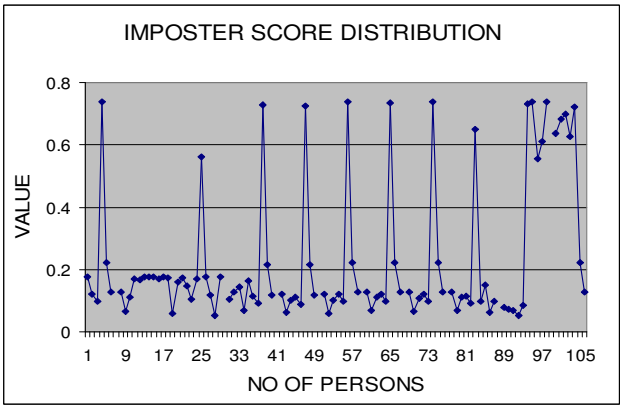

FIGURE 23(b): Imposter Score Distribution for Fingerprint-Hand Vein System

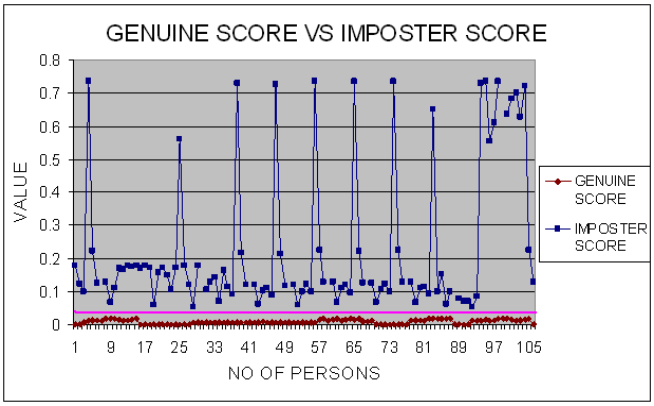

FIGURE 24: Genuine Score vs. Imposter Score for the Fingerprint-Hand Vein System

With the threshold of 0.03, obtained from Fig 24, an FRR of 0% and FAR of 0.01% were obtained for the Fingerprint-Hand vein system.

Biometric System	FAR(%)	FRR(%)
Fingerprint	4.81	2.07
Multimodal Hand Vein System	0.46	0.7
Multi-biometric Fingerprint-Hand Vein System	0	0.01

TABLE 3: Comparison of proposed Biometric Systems

Reference	Methodology	Imaging	Database	Performance
T. Tanaka and N.Kubo [15]	FFT based phase correlation	Near Infra Red, HDF	25 Users	FAR – 0.73% FRR – 4%
C. L. Lin and K. C. Fan [12]	Multi-resolution analysis and combination	Thermal Handvein Imaging	32 Users	FAR – 1.5% FRR – 3.5%
L. Wing and G. Leedham [23]	Line Segment Hausdorff distance matching	Thermal Hand Vein Imaging	12 Users	FAR – 0% FRR – 0%
Y. Ding, D. Zhuang and K. Wang [24]	Distance between feature points	Near IR Imaging, HDF	48 Users	FAR – 0% FRR – 0.9%
J. M. Cross and C. L. Smith [25]	Sequential Correlation in Vein maps	Near IR Imaging, HDF	20 Users	FAR – 0% FRR – 7.9%
A. Kumar and K.Venkata Prathyusha [16]	Matching vein triangulation and shape features	Near IR Imaging Contactless	100 Users	FAR – 1.14% FRR – 1.14%
Proposed Fingerprint-Hand Vein Multi-biometric System	Extraction and Fusion of highly random feature sets to improve performance	Near IR Imaging & Optical Fingerprint Sensor	74 Users	FAR –0 % FRR – 0.01%

TABLE 4: Comparative Summary of available literature on Hand Vein (Back Surface) Based Authentication

8. CONCLUSION AND DISCUSSIONS

From our detailed literature survey on Biometrics in general, we find that the Hand Veins have better circumvention. They can also be obtained equally for peoples of all skin colors. The Multimodal Handvein system is a contactless and hence hygienic biometric identification system suitable for hospitals. It gives a fairly good performance with FAR of 0.46 and FRR of 0.7. A choice of an even more high performance system is suggested in this paper, namely, a multi-biometric system. In situations where hygiene can be compromised for increased accuracy, the multi-biometric system which uses fingerprint and hand veins can be used. This system gives an FAR of 0% and FRR of 0.01%. Further hand vein and fingerprint are traits which are very less prone to damage even in critical cases like accidents. It can also be easily acquired without much patient cooperation. Thus the proposed multi-biometric system using fingerprint and hand vein is ideal for use in healthcare environments.

Increasing the randomness of the biometric template is proposed in this paper for improving the accuracy of the system. As discussed in the earlier sections, when the constituents of a feature vector are highly independent of each other, the randomness of the vector increases. The feature vectors used in the proposed fingerprint-handvein multibiometric system, comprise of the statistical and morphological feature sets of the handvein which are highly independent of each other.

There are several citations in literature that biometric systems based on multiple biometrics are more accurate than systems which depend on a single biometric. As seen in the earlier discussions, hand vein is a biometric identifier whose circumvention is much appreciated than other biometric traits and hence has an inherent quality of high randomness. The performance of the hand vein system can be improved by supplementing it with another biometric. Fingerprint is a very popular, proven, cost effective technology. Hence we have fused the fingerprint with hand vein to create the feature vector which in turn further increases the randomness of the template and hence the performance of the system. The fusion of multiple feature sets as well as multiple biometrics have led to a very remarkable performance rates, namely the FAR of 0% and FRR of 0.01%

9. ACKNOWLEDGEMENT

The author thanks the Management of PSG College of Technology for the facilities and support extended. The author also thanks the staff and student members of the Biomedical Engineering and ECE departments of the same college for their cooperation.

10. REFERENCES

1. http://www.cesg.gov.uk/site/ast/biometrics/media/Biometric/SecurityConcerns.pdf

2. A K Jain, A Ross, and S Pankanti. *"Biometrics: A Tool for Information Security"*. IEEE Transactions on Information Forensics and Security, 1(2):125-143, 2006

3. Nandakumar, K. *"Multibiometric Systems: Fusion Strategies and Template Security"* Doctor of Philosophy, Michigan State University, 2008

4. Uludag U., Ross A., Jain A.K. *"Biometric Template Selection and Update: A Case Study in Fingerprints"*. Pattern Recognition, 37(7):1533-1542, 2004

5. Dass S.C, Jain A.K.. *"Fingerprint Based Recognition"*. Technometrics, Technometrics, 49(3):262–276, 2007

6. Wuzhili. *"Fingerprint Recognition"*. Doctor of Philosophy, Hong Kong Baptist University, 2002

7. Kaur M, M Singh, A. Girdhar, and P. Sandhu. *"Fingerprint Verification System using Minutiae Extraction Technique"*. Proceedings of World Academy of Science, Engineering and Technology, 36: 2008

8. E Sojka. "*A New and Efficient Algorithm for Detecting the Corners in Digital Images*". Pattern Recognition, Luc Van Gool (Editor), LNCS 2449:125-132, 2002

9. Z Zhang, S Ma, X Han. "*Multiscale Feature Extraction of Finger-Vein Patterns Based on Curvelets and Local Interconnection Structure Neural Network".* Proceedings of the 18th International Conference on Pattern Recognition (ICPR '06), Hong kong, 2006

10. J Hashimoto Information & Telecommunication Systems Group, Hitachi, Ltd. *"Finger Vein Authentication Technology and its Future".* Symposium on VLSI Circuits Digest of Technical Papers, 2006

11. N Miura, A. Nagasaka, and T Miyatake. *"Feature Extraction of Finger-Vein Patterns Based on Repeated Line Tracking and its Application to Personal Identification"*. Machine Vision and Applications, 15(4):194-203, 2004

12. C Lin. and K Fan. *"Biometric Verification Using Thermal Images of Palm Dorsa Vein Patterns"*. IEEE Transactions on Circuits and systems for Video Technology, 14(2):188-195, 2004

13. J Cross and C Smith. *"Thermo graphic Imaging of the Subcutaneous Vascular Network of the Back of the Hand for Biometric Identification"*. Proceedings of 29th International Carnahan Conference on Security Technology, Institute of Electrical and Electronics Engineers, Sanderstead, 20–35, 2009

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, 38(3):268-272, 2001

15. T Tanaka and N Kubo. *"Biometric Authentication by Hand Vein Patterns"*. SICE, Annual Conference 249-253, Sapporo, August 2004

16. A Kumar, K Prathyusha. *"Personal Authentication Using Hand Vein Triangulation and Knuckle Shape"*. IEEE Transactionss on Image Processing, 18(9):2127-2136, 2009

17. M Shahin, A. Badawi, M Kamel. *"Biometric Authentication using Fast Correlation of Near Infrared hand vein patterns"*. International Journal of Biomedical sciences, 2(3): 2007

18. T Ko. *"Multimodal Biometric Identification for Large User Population using Fingerprint"*. Face and Iris Recognition, Proceedings of the 34th Applied Imagery and Pattern Recognition Workshop (AIPR05), Washington, DC, 2005

19. K Wang, Y Zhang, Z Yuan and D Zhuang. *"Hand Vein Recognition based on Multi supplemental features of multi-classifier fusion decision"*. Proceedings of the IEEE International Conference on Mechatronics and Automation, Luoyang, Henan, June 2006

20. Jain, Bolle R., and S. Pankanti. *"Biometrics: PersonalIdentification In Networked Society"*. Kluwer Academic Publishers, Dordrecht, 1999

21. W LingYu, G Leedham. *"Near and Far Infrared Imaging for Vein Pattern Biometrics*". Proceedings of the IEEE International Conference on Video and Signal Based Surveillance (AVSS'06), Sydney, Australia, 2006

22. [22] J Duncombe. "*Infrared navigation—Part I: An assessment of feasibility (Periodical style)"*. IEEE Trans. Electron Devices, 11:34–39, 1959

23. L Wang and G Leedham. *"A thermal hand-vein pattern verification system".* Pattern Recognition and Image Analysis, Springer, 3687:58–65, 2005

24. Y Ding, D Zhuang and K Wang. *"A study of hand vein recognition method"*. Proceedings of IEEE International Conference on Mechatronics & Automation, Niagara Falls, Canada, 2106-2110. Jul. 2005

25. J Cross, and C Smith. *"Thermo graphic imaging of the subcutaneous vascular network of the back of the hand for biometric identification"*. Proc. IEEE 29th Annu. Int. Carnahan Conf. Security Technology, Sander-Stead, Surrey, U.K, 20–35, 1995

Determining an Optimal Number of Access Points Using GPS Data to Secure a Wireless Network Environment

Iyad Aldasouqi iyad@rss.gov.jo
Royal Scientific Society
Information Technology Center
Amman, 11941, Jordan

Walid Salameh walid@psut.edu.jo
Princess Sumaya University for Technology
The King Hussein School for Information Technology
Amman, 11941, Jordan

Abstract

Determination of the position enables location awareness for mobile computers in any place and persistent wireless computing. In addition utilizing location information, location aware computers can render location based services possible for mobile users. In order to design and implement a technique to identify the source network interface card, a feasibility study should be done to keep the project within the budget; also tracking of new technologies will enhance the methodology of choosing these techniques. Wireless Local Area Network (WLAN) is vulnerable to malicious attacks due to their shared medium in unlicensed frequency spectrum, thus requiring security features for a variety of applications. This paper will discuss a technique that helps in determining the best location for access points using GPS system, in order to choose the optimal number of them; which guide to localize and identify attacks with optimal IDS method and cheapest price. The other thing is to locate the intruder within the monitored area by using a hybrid technique, which came from exist techniques, by focusing on the advantages of these techniques and come with a new one to give more accurate results with less price by using available resources.

Keywords: Security, Sensors, Access points, Wireless, Authentication

1. INTRODUCTION

WLAN is a flexible data communications system that can use either infrared or radio frequency technology to transmit and receive information over the air. Also WLAN has been widely used in many sectors starting from corporate, education, finance, healthcare, retail, manufacturing, warehousing, clinics airports and schools; since it can overcome the physical limitations of wired communications and the simplicity of its installation, so it increases the user flexibility, employee motivations, and reduces the cost. Furthermore, the WLAN infrastructure can be applied to provide indoor location service without deploying additional equipment [19]

The use of different technologies (attenuators, amplifiers, antennas, and software) can be attached by smart attackers, but the attacker cannot masquerade the identity of the user; because in this case he should be located on the same location of the user or at the location of access points. However, to secure the network, we have to cover the area with certain pattern of

access points; so we can be sure that each access point has the ability to cover its own area and can identify the login users depending on his/her identity and physical location. By this the network will be secured against any attack and the budget of the project will be under control.

In the last decade, researchers have proposed a number of WLAN positioning techniques for (local area) wireless networks [26,27,28,29]. Despite the cost advantage and productivity offered by WLAN, the used radio waves in wireless networks create a risk, and give a chance for the hackers to attack the network. So the real challenge is to boost employee demand for access to their enterprise's wireless network beyond the area of their office workstation. In addition, the controlling of the quality and strength of the security (Signal propagation, characteristics, limited bandwidth and other) is another challenge which the designer of the network should consider.

The Global Positioning System (GPS) is used for position location, navigation, and precision timing. It accomplishes this using three segments: (1) satellites, (2) ground control centers, and (3) receivers. Anyone can simply go online and get a map of the exact location of an insecure network identified by a war driver [16]. But unfortunately, the GPS system cannot be used effectively inside buildings and in dense urban areas due to its weak signal reception when there are no lines-of-sight from a MS to at least three GPS satellites [18], for this reason the experiment in this paper done outdoor using the same AP which will be used indoor to now the coverage of each AP.

1.1 Wireless Network

The physical architecture of WLAN is simple. Basic components of a WLAN are access points (APs) and Network Interface Cards (NICs)/client adapters. In addition Wireless frequencies are designed to be used by anyone with a wireless receiver (NIC)

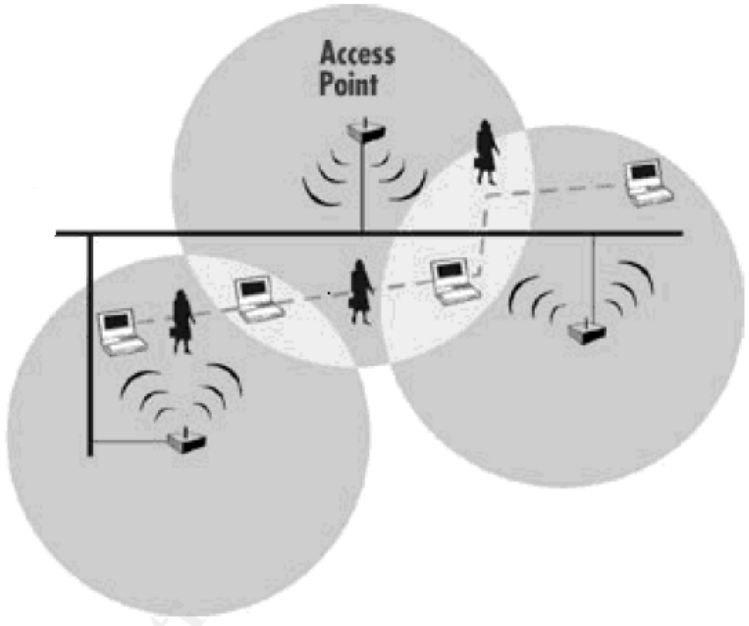

FIGURE 1: WLAN Coverage [1]

A wireless local area network (WLAN) is a flexible data communications system that can use either infrared or radio frequency technology to transmit and receive information over the air. In order to extend WLAN range, and facilitate the user mobility a multiple access points is required, which is one of the main benefits of WLAN. Therefore, it is very important to ensure that users can move seamlessly between access points without having to log in again and restart their applications.

To control the spread of WLAN, a standards was started in order to keep the rangers of wireless waves within ranges and to organize the work, e.x in 1997, 802.11 was implemented as the first WLAN standard. It is based on radio technology operating in the 2.4 GHz frequency and has a maximum throughput of 1 to 2 Mbps. The currently most spread and deployed standard, IEEE 802.11b, was introduced late 1999. It still operates in the same frequency range, but with a maximum speed of 11 Mbps.

According to a study by the Gartner Group, approximately 50 percent of company laptops around the world will be equipped for WLAN by 2006 [3]. Therefore, nowadays all laptops are equipped by WLAN from different vendors with almost the specifications with small differences.

1.2 Detecting and preventing network intrusions

Intrusion detection (ID) considered as a type of security management system (device or application) for computers and networks activities for malicious activities or policy violations. An ID system gathers and analyzes information by monitoring the events from various areas within a computer or a network to identify possible security breaches or possible incidents, which include both intrusions (attacks from outside the organization or out side.

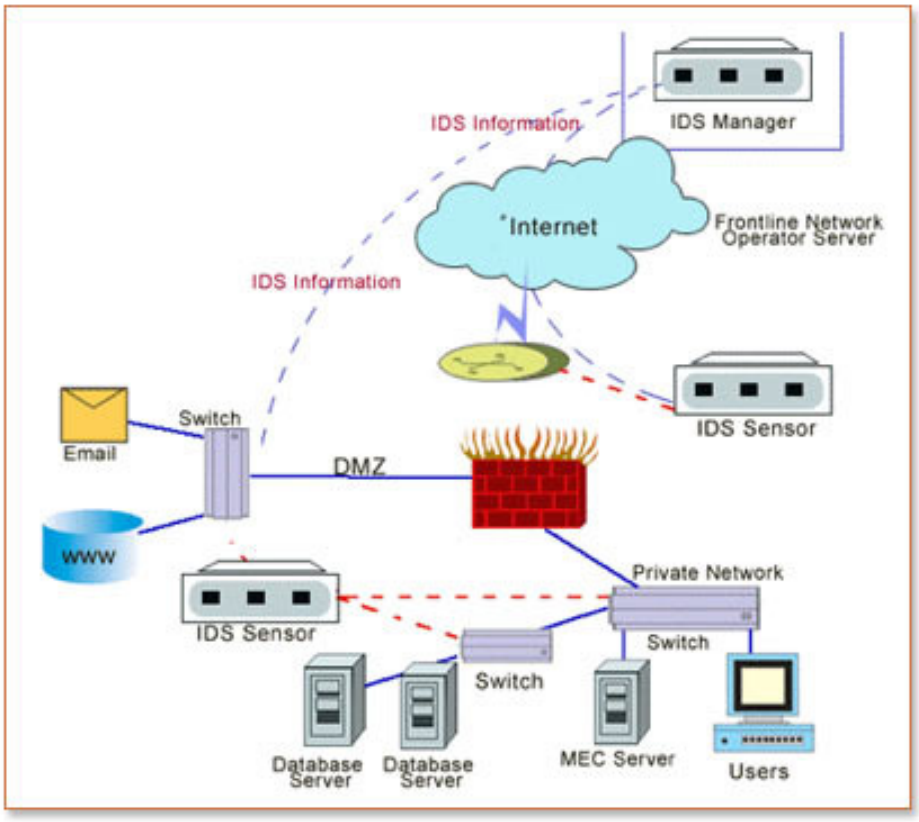

Figure 2: Security Technologies - Intrusion Detection System
(Source: http://indiacyberlab.in/security-awareness/security-technologies.htm)

IDS differ from a firewall, in which a firewall looks out for intrusions in order to stop them from happening. In addition the firewall limits the access between networks in order to prevent intrusion, but can not do the same for an attack from inside the network. Where the IDS evaluates a suspected intrusion once it has taken place and signals

Intrusion detection functions can be summarized as:

- Monitoring and analyzing both user and system activities
- Analyzing system configurations and vulnerabilities
- Assessing system and file integrity
- Ability to recognize patterns typical of attacks
- Analysis of abnormal activity patterns
- Tracking user policy violations

1.3 MAC Spoofing

The phrase "MAC address spoofing" in this context relates to an attacker altering the manufacturer-assigned MAC address to any other value. This is conceptually different than traditional IP address spoofing where an attacker sends data from an arbitrary source address and does not expect to see a response to their actual source IP address. MAC address spoofing might be more accurately described as MAC address "impersonating" or "masquerading" since the attacker is not crafting data with a different source than is their transmitting address. When an attacker changes their MAC address they continue to utilize the wireless card for its intended layer 2 transport purpose, transmitting and receiving from the same source MAC. [4]

Recently some devices can be found on the market, which can easily change the MAC address. By using these tools, the attacker modifies either the MAC or the IP address of the victim in order to adopt another identity in the network.

To illuminate the spoofing, there are three techniques:

1. Sequence number analysis
2. Transceiver fingerprinting:
3. Signal strength analysis:

1.4 Access Point location

The access point is the first gate that the hacker is thinking to use, and so the best and suitable place for WLAN access points is outside the firewall. Therefore, only legitimate users based on MAC and IP addresses can be able to access the firewall. However, this is considered a perfect solution; since MAC and IP addresses can be spoofed, so by this approach it is difficult for a hacker to attack the network; because we are working with physical layer, which is hard to frog and not easy as the MAC address; since the information in this layer is inherent to radio characteristics and the physical environment, in addition it is used to differentiate devices.

Furthermore, the ability to track and check the location of people or equipment in real time has a large number of application areas such as child safety, prisoner tracking and supply chain to name but a few [23]. Therefore, Over the past two decades a large number of commercial and research location aware systems have been developed [24].

This paper is divided into four sections. Starting by introduction, then by describing available methods to eliminate attacks "IDS"; after that, the approach to increase the security of the network by using minimum number of access points. And the last section is a real test to verify the suggested approach. Finally ending with conclusion and future works.

2. SPOOFING ATTACK AND RELATED WORK

There are many available techniques which can detect different types of intrusion, the differences between these techniques are in performance and in the ability to detect and locate the intruder, and this section summarized some of famous techniques which can do that with an easy implementation and reasonable budget. In addition, these solutions require the cooperation of the APs [29-33].

Location estimation systems based on radio signal strengths can be classified into two main categories [17]: (1) Radio-Propagation Models (2) Empirical-Fit Models. Some of these

techniques are used for localization and spoof detection, and others for detection only. Localization considers all measurements gathered received signal strength (RSS) are from a single station; therefore it matches a point in the measurement space with a point in the physical space. Where spoofing detection tries to determine whether the signals are definitely from the same station or not.

2.1 Detecting and Localizing Wireless Spoofing Attacks

It is a method for detecting spoofing and locating the positions of the attacks. This method uses the K-means cluster analysis, and then to localize the position of the attacker it integrates the attack detector into a real-time indoor localization system. In addition it uses two algorithms (once at a time) a) Area-based and b) point-based to localize the intruder; since both algorithms have the same relative errors as in the normal case.

As an implementation and evaluation of this method, the authors used both an 802.11 (WiFi) network as well as an 802.15.4 (ZigBee) network. And they proofed that it is possible to detect wireless spoofing with both a high detection rate and a low false positive rate, thereby providing strong evidence of the effectiveness of the K-means spoofing detector as well as the attack localizer.[5]

2.2 Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength

To monitor any network either a hardware solution (ex. Air monitor AM) or a software solution is needed, sometimes both hardware and software with the same solution (ex. sniffer) can be found. This method beside using the access points uses AM to monitor the traffic, which can be consider as load on the network, but some solution gives the priority for the security. And also developed a RSS profiling algorithm based on the Expectation-Maximization (EM), in which they referenced to Gaussian Mixture Model (GMM) [6]. After RSS receive transmitter's signal, immediately calculate the differences, and if there is any it will consider it as a potential spoofing attack.

In addition this method developed two global detection algorithms which are focusing on:[7]

1. Combine local statistics from multiple AMs.
2. Works on the frame sequence output by the merger.

Also it has a role in improving networking intrusion detection via some contributions:[7]

1. Discovered that antenna diversity is the major cause of multimodal RSS patterns.
2. Presented a new GMM profiling algorithm.

2.3 Detecting Identity Based Attacks in Wireless Networks Using Signal-prints

This method proposed a technique to detect spoofing attacks using a signal-print, which depends on RSS for a MAC address measured at multiple AMs. The authors ideas built upon that a transmitting device can be robustly identified by its signal print, where the access point will work as a sensor which sensing the signal strength values. The using of signal strength makes the attackers jammed and also they do not have as much control regarding the signal prints they produce; each signal-print is represented as a vector of signal strength measurements. In addition the authors used 802.11 networks, but the same technique can be applied to other wireless LAN technologies.

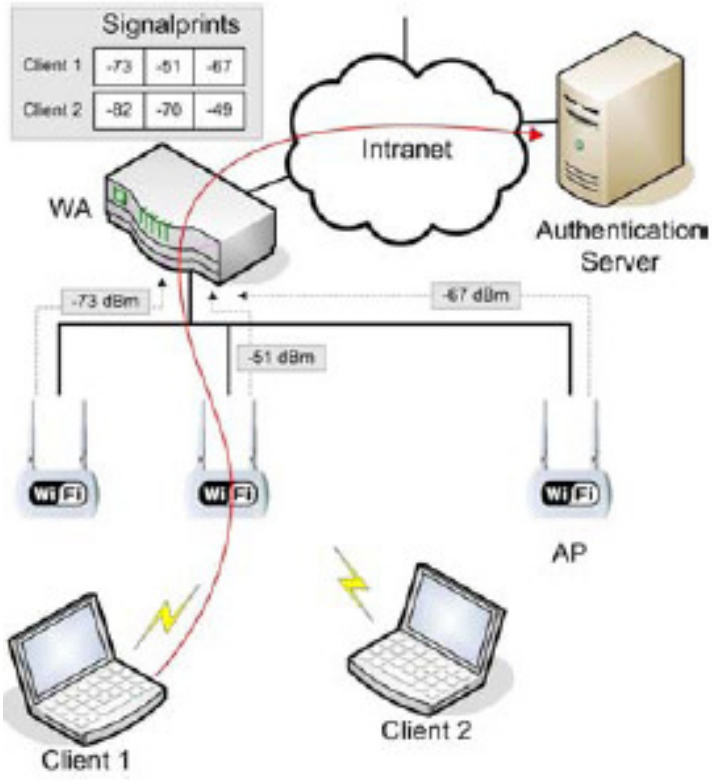

FIGURE 3: Signal-print creation [9]

The Signal-print is used because it is hard to spoof, since its attenuation is a function of the distance between clients and access points.

In addition Signal-prints are strongly correlated with the physical location of clients, with similar signal-prints found mostly in close proximity. [9]

2.4 Wireless Client Puzzles in IEEE 802.11 Networks: Security by Wireless

It is a protection method which assists an AP to preserve its resources by discarding fake requests, while allowing legitimate clients to successfully join the network. Rather than conditioning a puzzle's solution on computational resources of highly heterogeneous clients, the puzzles utilize peculiarities of a wireless environment such as broadcast communication and signal propagation which provide more invariant properties. [10]

The puzzle is a question about which other stations are in the client's signal proximity as in figure.4, and can thus be labeled as neighbors. The received signal strength of neighbors is strong, contrary to non-neighbors which are received weakly in relation to a certain signal value. In other words it is security by wireless application; since it is exploit the chaotic and erratic character of radio communications, describing the radio of the neighborhood, do the mutual verification via the broadcasting. And depending on the new location of the client (N) there will be different solutions. [7]

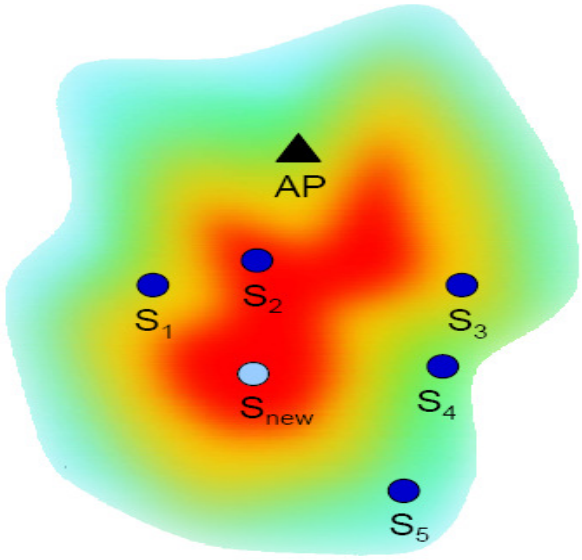

FIGURE 4: Signal Proximity [10]

2.5 Advancing Wireless Link Signatures for Location Distinction (AWLS)

This method is used to locate the transmitters even if the location changed. So it will enforce physical security by identifying illegal transmitter and preventing them from accessing the network.

A sophisticated physical-layer measurement is used to locate distinction. This done by compared two existing location distinction methods: [11]

1. Channel gains of multi-tonal probes: where the channel frequency response is sensitive to each multipath. An impulse in the time domain is a constant in the frequency domain, and thus a change to a single path may change the entire multiple tone link signature.
2. Channel Impulse Response (CIR): it uses a time domain signature, which support it with more robust against channel small changes.

By combining the benefits of these two methods a new link measurement have been developed, which called the complex temporal signature.

2.6 PARADIS: Physical 802.11 Device Identification with Radiometric Signatures

This method used passive radio-frequency analysis to identify the location. They measure artifacts of individual wireless frames in the modulation domain, identify a suite of differentiating features, and apply efficient 802.11-specific machine-learning based classification techniques to achieve significantly higher degrees of accuracy than prior best known schemes. [12]

PARADIS uses a large five distinct features from the modulation domain, namely, frequency error, magnitude error, phase error, I/Q offset, and sync-correlation of the corresponding wireless frame. Also PARADIS is located at the boundary of the analog and digital domains of wireless hardware.

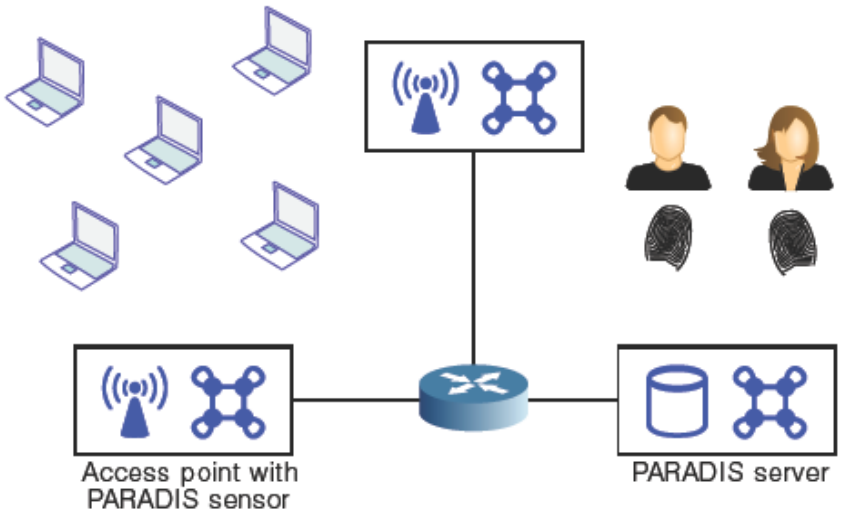

FIGURE 5: PARADIS schematic [11]

3. PROPOSED SOLUTION

A related solution is discussed in [7], but here the issue is not only the security, but also the implementation with taken the budget into the consideration is another issue.

Most of the discussed methods were depended on signal-print technique [9] (direct or indirect), which means it is a reference for most of the methods even though some of these methods claim about its results, false alarm and statistics.

As a solution, after understanding the concept of each method we found the strongest methods are the signal-print [9] and the Puzzles [10]; since the ability of identifying and localizing attack are high compared with other method.

Positioning is a process to obtain the spatial position of a target [25], and since the signal-print is an alternative for Puzzle, we suggest to use some of Puzzle's technique (the ability of knowing the neighbor) inside signal-print and come up with a hybrid approach, by which we can reduce the load on the network and be able to distinguish close clients, not only that but come up with testing and evaluation technique, which can minimize the number of access points to the optimum number without affecting on the security level.

The suggested ideas can be summarized as below:

1. Using Signal-print as an authentication technique; since it depends on the signal strength.
2. Using the Puzzles features:
   a. SSL, TCP and as a countermeasure against spam.
   b. If the received signal strengths are equal, use Puzzle's authentication technique in order to locate the neighbors (using AI to determine when to use any of them), Puzzle's authentication illustrated in figure 6. And the frame format as in shown in figure 7.

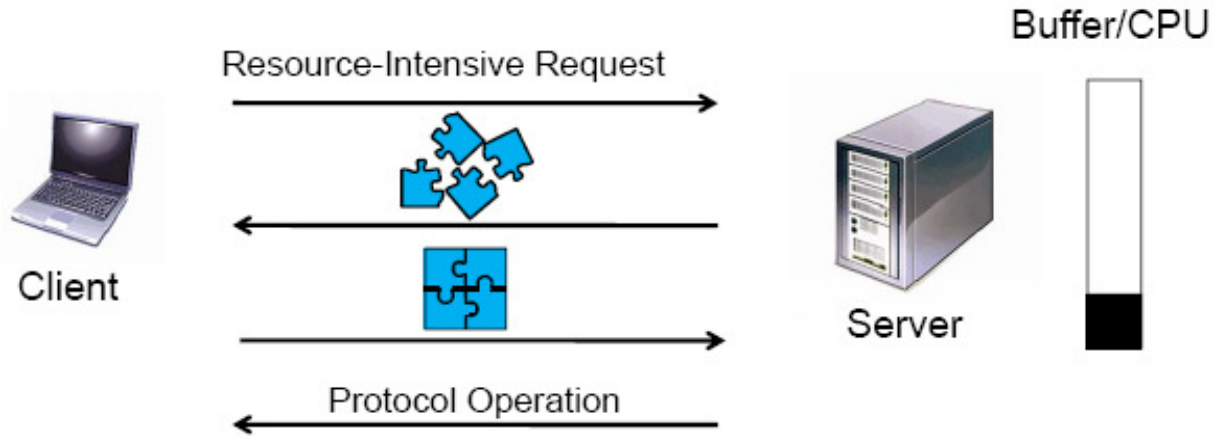

FIGURE 6: Puzzle's authentication concept

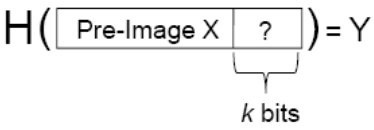

FIGURE 7: Puzzle's frame format [15]

3. Draw the network diagram to organize the network, by using network drawing software (ex. OMNet++), in order to come with a network diagram similar to figure.8.

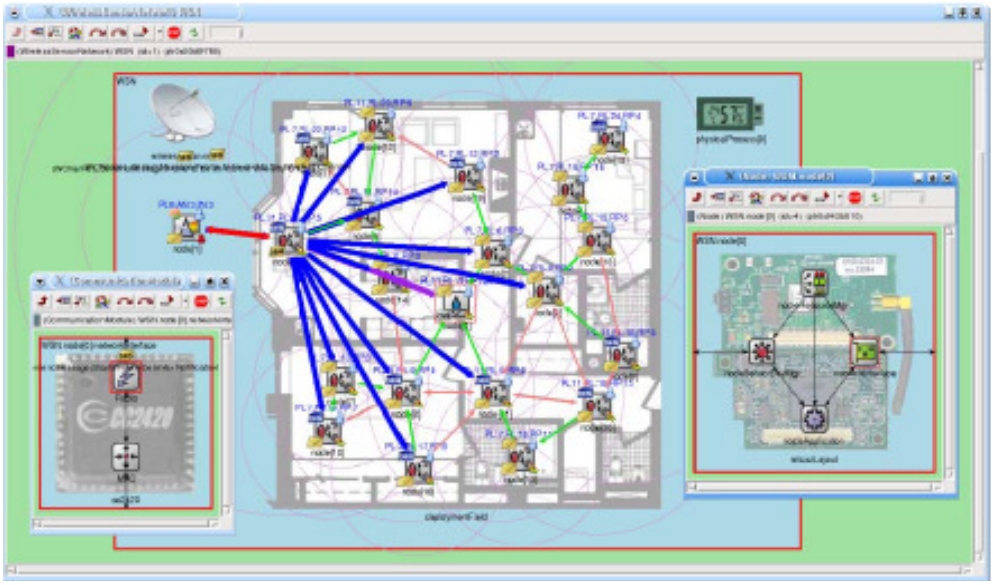

FIGURE 8: Example of Network drawing software (http://www.omnetpp.org)

4. Distribute the access points depending on the coverage of each access point, which can be determined depending on type of the access point and the diversity of its antennas, covered area and antenna types illustrated in figure 9.

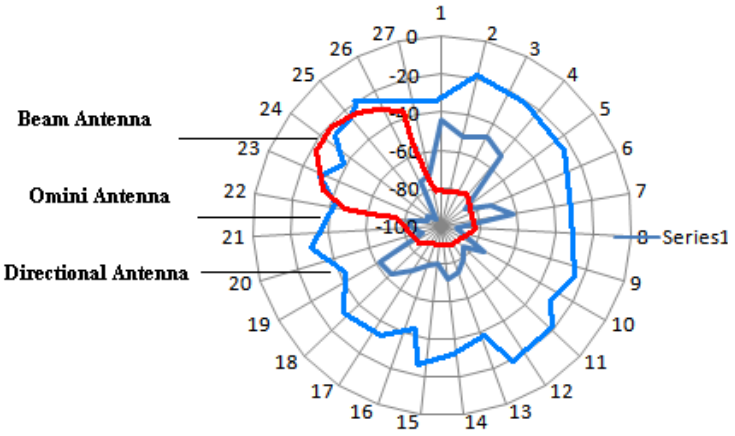

FIGURE 9: covered areas and types of antennas

5. We installed the first access point, then. For demonstration we used the following equipments:
   - CISCO Aironet 350
   - 13.5db antenna
   - Laptop with Network Stumbler software
   - TP link External card

   We got the results as shown in table 1.

Distance	Bearing	Signal	Noise	mbps
0	230	-41	-100	54
10	273	-48	-100	54
16	255	-45	-100	54
22	283	-50	-95	33
31	71	-81	-100	0
35	355	-68	-95	4
40	33	-60	-95	21

TABLE 1: Test results

6. From signal data we can generate a radar graph which can show access control covered area, Figure 10.

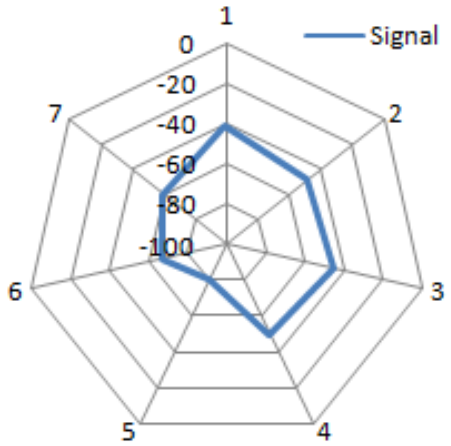

FIGURE 10: Signal data representation

7. From figure 10, we knew the covered area of the first access point, and by repeating the same procedure on the boundaries of first access point we can cover the whole area without overlapping and keeping the level of security without any affect on its level.

8. The above procedure is applied if the area which we are going to cover is open or like figure 11. But if it is a closed rooms or other facilities the type of the walls will judge our decision; since the level of the noise increases, signal will be attenuated as shown in figure.12.

FIGURE 11: offices area covered by wireless network [15]

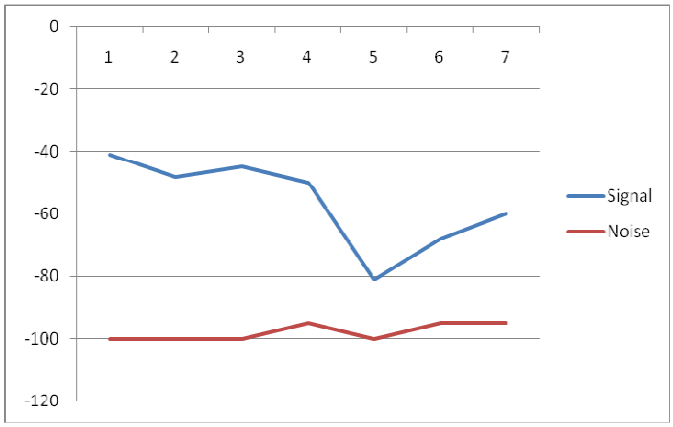

FIGURE 12: Signal / Noise

9. Also, the relation between the distance and the speed has a good role in determining the percent of overlapping between access points as in figure 13.

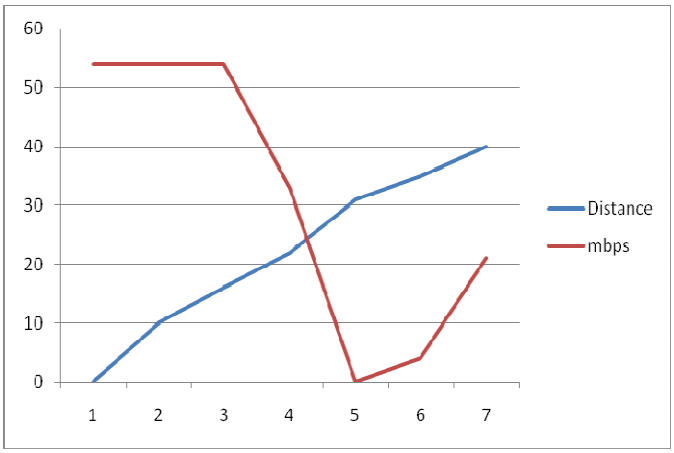

FIGURE 13: Distance / Speed

10. In addition, the rlation between the bearing and the speed, which will give us an idea about uncoverd areas, so we can cover it by other access points, as illustrated in figure 14.

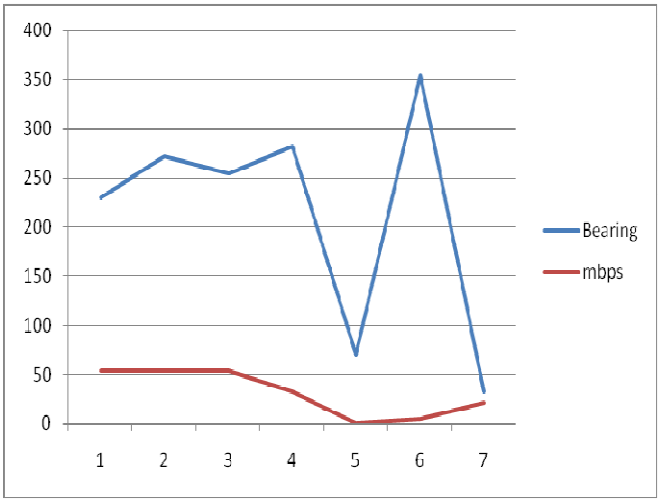

FIGURE 14: Bearing / Speead

11. Finally, the monitored area can be like figure 15.

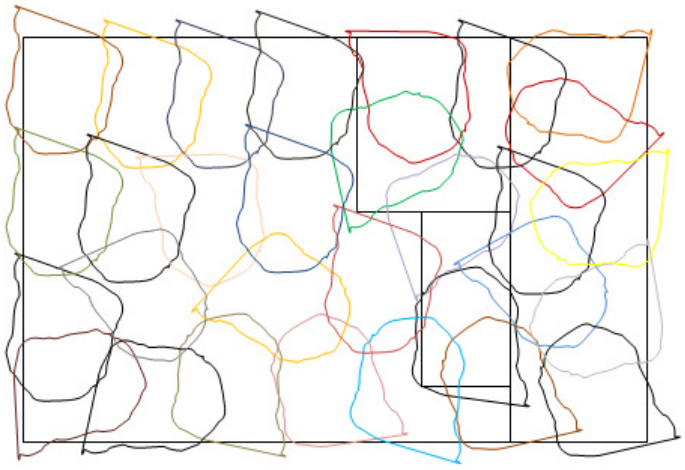

FIGURE 15: monitored area with access points locations and overlaping

4. CONCLUSION AND FUTURE WORK

Securing the network becomes a load on the network administrators; since the wireless network is wildly spread.

Signal Strength which is unique for each device as mentioned in previous works [20,21,22]; because it depends on the type and location of the device is also can be attached by some smart hackers, so the experts try to secure the network using different methods and technique to detect any kind of attack.

Choosing the optimal number of access points is a very important factor in network design; because each AP has its own coverage area, which varies from type to type of APs, therefore to illuminate overlapping problem we have to choose the optimal number, otherwise location of the intruders can't be determined. In this paper the GPS was used for accuracy issues, and as a test bed both indoor and outdoor areas were used, but in the indoor the highest floor of the building were used to overcome the coverage limitation of the GPS.

As a result three things were achieved in this paper, network service is available only for the clients on the test bed (not more); which is a result of good distribution of APs, intruder can't attack any client; because two strong techniques were merged (Puzzle [10] and signal-print [9]) and the last one is a good management for the budget; by reducing the cost into the minimum by choosing the optimal number of APs.

Finally, as a future work, merging between network security and image processing (using remote sensing) to find both the best location of access points and optimal number of them, which can be used for city plans and e-government solutions.

5. REFERENCES

1. Wireless Intrusion Detection Systems, SANS, Ken Hutchison, 2004

2. http://netsecurity.about.com/cs/hackertools/a/aa030504_2.htm

3. Swisscom.com. *"Swisscom Mobile to launch Public Wireless LAN on 2 December 2002".* 2 Jan. 2003. Available at: http://www.swisscom.com/mr/content/media/20020924_EN.html (Accessed 9 Dec. 2002)

4. Joshua Wright, Detecting Wireless LAN MAC Address Spoofing, 2003

5. Yingying Chen, Wade Trappe, Richard P. Martin, Detecting and Localizing Wireless Spoofing Attacks

6. R. A. Redner and H. F. Walker, *"Mixture densities, maximum likelihood and the EM algorithm"*. SIAM Review, 26(2):195–239, 1984

7. Iyad Aldasouqi, Walid Salameh, Detecting and Localizing Wireless Network Attacks Techniques, CSC, 2010

8. M. Ladd, K. E. Bekris, A. Rudys, L. E. Kavraki, D. S. Wallach, and G. Marceau*, "Robotics-based location sensing using wireless ethernet".* In MobiCom '02: Proceedings of the 8th Annual International Conference on Mobile Computing and Networking, Sept. 2002, pp. 227–238

9. D. B. Faria and D. R. Cheriton, *"Detecting identity-based attacks in wireless networks using singalprints".* In Proceedings of WiSe'06: ACM Workshop on Wireless Security, 2006

10. Wireless Client Puzzles in IEEE 802.11 Networks: Security by Wireless, Ivan Martinovic, Frank A. Zdarsky, Matthias Wilhelm, Christian Wegmann, and Jens B. Schmitt

11. Advancing Wireless Link Signatures for Location Distinction, by J.Z. Mohammad H. Firoozz Neal Patwariz Sneha K. Kaseray

12. PARADIS: Physical 802.11 Device Identification with Radiometric Signatures by Vladimir Brik, Suman Banerjee, Marco Gruteser, Sangho Oh

13. P. Bahl and V. N. Padmanabhan, "*Radar: An in-building rf based user location and tracking system,"* in Proceedings of the IEEE International Conference on Computer Communications (INFOCOM), March 2000

14. E. Elnahrawy, X. Li, and R. P. Martin, "*The limits of localization using signal strength: A comparative study".* In Proceedings of the First IEEE International Conference on Sensor and Ad hoc Communcations and Networks (SECON 2004), 2004.

15. Neal Patwari and Sneha Kasera, Robust Location Distinction Using Temporal Link Signatures

16. Aaron E. Earle, Wireless Security Handbook

17. P. Bahl and V. Padmanabhan." *RADAR: An in-building RF based user location and tracking system".* In Proceedings of the Conference on Computer Communications, volume 2, pages 775–784, Tel Aviv, Israel, March 2000.

18. G. M. Djuknic and R. E. Richton, \Geolocation and assisted GPS," IEEE Computer, 34(2): 123-125, 2001

19. P. Bahl and V. N. Padmanabhan, *"RADAR: an in-building RF-based user location and tracking system".* In Proc. IEEE Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'00), Tel Aviv, Israel, Mar. 2000,

20. P. Bahl and V. N. Padmanabhan, "*RADAR: an in-building RF-based user location and tracking system,"* in Proc. IEEE Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'00), Tel Aviv, Israel, Mar. 2000

21. S. Saha, K. Chaudhuri, D. Sanghi, and P. Bhagwat, "*Location determination of a mobile device using ieee 802.11b access point signals,"* in Proc. IEEE Wireless Communications and Networking Conference (WCNC'03), New Orleans, LA, Mar. 2003

22. J. Small, A. Smailagic, and D. P. Siewiorek, "*Determining user location for context aware computing through the use of a wireless lan infrastructure,"* Online, Dec. 2000. [Online]. Available At: http://www.2.cs.cmu.edu/»aura/docdir/small00.pdf

23. Krzysztof, K., Hjelm, J. (2006) LBS Applications and Services, CRC Press, ISBN: 0849333490.

24. Hazas, M., Scott, J., Krumm, J. (2004) Location-Aware Computing Comes of Age. Computer, 37 (2004) 95-97.

25. Küpper, A. (2005) Location-based services. John Wiley & Sons, Chichester.

26. P. Bahl and V. N. Padmanabhan. "*RADAR: An In-Building RF-Based User Location and Tracking System".* In Proceedings of the IEEE Conference on Computer Communications (InfoCom), volume 2, 2000.

27. P. Castro, P. Chiu, T. Kremenek, and R. Muntz. "*A Probabilistic Room Location Service for Wireless Networked Environments."* In Proceedings of the International Conference on Ubiquitous Computing (Ubicomp), volume 2201, 2001.

28. J. Hightower, G. Boriello, and R. Want. "*SpotON: An indoor 3D location sensing technology based on RF signal strength".* Technical Report 2000-02-02, University of Washington, 2000.

29. R. Want, A. Hopper, V. Falcao, and J. Gibbons. "*The Active Badge Location system."* ACM Transactions on Information Systems, 10(1), 1992.

30. S. Pandey, F. Anjum, and P. Agrawal. "*TRaVarSeL–Transmission Range Variation based Secure Localization"*, pages 215–236. 2007.

31. S. Pandey, F. Anjum, B. Kim, and P. Agrawal. "*A low-cost robust localization scheme for WLAN".* In Proceedings of the International Workshop on Wireless Internet, New York, NY, USA, 2006. ACM.

32. S. Pandey, B. Kim, F. Anjum, and P. Agrawal. "*Client assisted location data acquisition scheme for secure enterprise wireless networks"*. IEEE Wireless Communications and Networking Conference (WCNC), 2, March 2005

33. P. Tao, A. Rudys, A. M. Ladd, and D. S. Wallach. "*Wireless LAN location-sensing for security applications*.' In Proceedings of the ACM Workshop on Wireless Security (WiSe), 2003.

CALL FOR PAPERS

Information Security is an important aspect of protecting the information society from a wide variety of threats. The International Journal of Security (IJS) presents publications and research that builds on computer security and cryptography and also reaches out to other branches of the information sciences. Our aim is to provide research and development results of lasting significance in the theory, design, implementation, analysis, and application of secure computer systems.

IJS provides a platform to computer security experts, practitioners, executives, information security managers, academics, security consultants and graduate students to publish original, innovative and time-critical articles and other information describing research and good practices of important technical work in information security, whether theoretical, applicable, or related to implementation. It is also a platform for the sharing of ideas about the meaning and implications of security and privacy, particularly those with important consequences for the technical community. We welcome contributions towards the precise understanding of security policies through modeling, as well as the design and analysis of mechanisms for enforcing them, and the architectural principles of software and hardware system implementing them.

To build its International reputation, we are disseminating the publication information through Google Books, Google Scholar, Directory of Open Access Journals (DOAJ), Open J Gate, ScientificCommons, Docstoc and many more. Our International Editors are working on establishing ISI listing and a good impact factor for IJS.

IJE List of Topics:

The realm of International Journal of Security (IJS) extends, but not limited, to the following:

- Anonymity
- Attacks, security mechanisms, and security service
- Authorisation
- Cellular/wireless/mobile/satellite networks securi
- Public key cryptography and key management
- Cryptography and cryptanalysis
- Data integrity issues
- Database security
- Denial of service attacks and countermeasures
- Design or analysis of security protocols
- Anonymity and pseudonymity
- Code security, including mobile code security
- Biometrics
- Authentication
- Confidentiality, privacy, integrity, authenticatio
- Data confidentiality issues
- Data recovery
- Denial of service
- Dependability and reliability
- Distributed access control

- Distributed and parallel systems security
- Electronic commerce
- Formal security analyses
- Fraudulent usage
- Information flow
- Information hiding and watermarking
- Intellectual property protection
- Intrusion detection
- Key management
- Multicast security
- Network and Internet security
- Network forensics
- Network security performance evaluation
- Non-repudiation
- Peer-to-peer security
- Prevention of traffic analysis
- Privacy protection
- Computer forensics
- Revocation of malicious parties
- Risk assessment and management
- Secure location determination
- Secure PHY/MAC/routing protocols
- Secure routing protocols
- Security group communications
- Security in ad hoc networks
- Security in cellular networks (2G, 2.5G, 3G, B3G,
- Security in communications
- Security in content-delivery networks
- Security in distributed systems
- Security in domain name service
- Security in e-mail
- Security in high-speed networks
- Security in integrated networks
- Security in integrated wireless networks
- Security in internet and WWW
- Security in IP networks
- Security in mobile IP
- Security in optical systems and networks
- Security in peer-to-peer networks
- Security in satellite networks
- Security in sensor networks
- Security in VoIP
- Security in wired and wireless integrated networks
- Security in Wired Networks
- Security in wireless communications
- Security in wireless internet
- Security in wireless LANs (IEEE 802.11 WLAN, WiFi,
- Security in wireless MANs (IEEE 802.16 and WiMAX)
- Security in wireless PANs (Bluetooth and IEEE 802.
- Security policies
- Security specification techniques
- Security standards
- Tradeoff analysis between performance and security
- Trust establishment
- Viruses worms and other malicious code
- WLAN and Bluetooth security

IMPORTANT DATES

Volume: 4
Issue: 6
Paper Submission: November 31, 2010
Author Notification: January 01, 2011
Issue Publication: January /February 2011

CALL FOR EDITORS/REVIEWERS

CSC Journals is in process of appointing Editorial Board Members for ***International Journal of Computer Security (IJS)***. CSC Journals would like to invite interested candidates to join **IJS** network of professionals/researchers for the positions of Editor-in-Chief, Associate Editor-in-Chief, Editorial Board Members and Reviewers.

The invitation encourages interested professionals to contribute into CSC research network by joining as a part of editorial board members and reviewers for scientific peer-reviewed journals. All journals use an online, electronic submission process. The Editor is responsible for the timely and substantive output of the journal, including the solicitation of manuscripts, supervision of the peer review process and the final selection of articles for publication. Responsibilities also include implementing the journal's editorial policies, maintaining high professional standards for published content, ensuring the integrity of the journal, guiding manuscripts through the review process, overseeing revisions, and planning special issues along with the editorial team.

A complete list of journals can be found at http://www.cscjournals.org/csc/byjournal.php. Interested candidates may apply for the following positions through http://www.cscjournals.org/csc/login.php.

Please remember that it is through the effort of volunteers such as yourself that CSC Journals continues to grow and flourish. Your help with reviewing the issues written by prospective authors would be very much appreciated.

Feel free to contact us at coordinator@cscjournals.org if you have any queries.

Contact Information

Computer Science Journals Sdn BhD
M-3-19, Plaza Damas Sri Hartamas
50480, Kuala Lumpur MALAYSIA

Phone: +603 6207 1607
+603 2782 6991
Fax: +603 6207 1697

BRANCH OFFICE 1
Suite 5.04 Level 5, 365 Little Collins Street,
MELBOURNE 3000, Victoria, AUSTRALIA

Fax: +613 8677 1132

BRANCH OFFICE 2
Office no. 8, Saad Arcad, DHA Main Bulevard
Lahore, PAKISTAN

EMAIL SUPPORT
Head CSC Press: coordinator@cscjournals.org
CSC Press: cscpress@cscjournals.org
Info: info@cscjournals.org

COMPUTER SCIENCE JOURNALS SDN BHD
M-3-19, PLAZA DAMAS
SRI HARTAMAS
50480, KUALA LUMPUR
MALAYSIA