International Academic Institute for Science and Technology

International Academic Journal of Science and Engineering
Vol. 2, No. 2, 2015, pp. 95-108.
ISSN 2454-3896

International Academic Journal of Science and Engineering

www.iaiest.com

A modify fingerprint watermarking to improve Security in Wireless Networks

Alireza Farhang [a] , Hassan Rashidi [b]

[a] *Faculty of Computer and Information Technology Engineering, Qazvin Branch, Islamic Azad University, Qazvin, Iran*.

[b] *Department of Mathematics and Computer Science, Allameh Tabataba'i University, Tehran, Iran*.

Abstract

This paper has aimed to explore a biometric method to secured wireless communications. Briefly, the system is built upon a complete challenge/response methodology in order to obtain a high level of security on the basis of user identification by fingerprint. First is the enrolment phase by which the database of watermarked is created and sending it to the server through wireless medium. Later is the verification stage at which claimed users are verified against the database, and it includes of five steps.In order to implement fingerprint watermarking, i.e. incorporating the memorable term as a watermark message into the fingerprint image, an algorithm of five phases has been developed. The first three novel phases having to do with the fingerprint image enhancement have been followed with further two steps for embedding phase, and extracting the watermark into the enhanced fingerprint image utilizing Discrete Wavelet Transform (DWT).

Keywords: Fingerprint, Watermark, Biometric ,Discrete Wavelet Transform(DWT)

Introduction:

Enhancing the security in various scenarios such as used for national identification, network access and border pass, has resulted in an unprecedented growth in the use of biometrics. The ever-increasing application of biometrics extends also to wireless world for the obvious reason of important role security plays in this field. An example can be found in authorized mobile devices where an authorization based on biometric identification allows the user to gain access to data such as needed for bank transactions. In addition, the recent upgrading of the E-Health and E-Commerce to M-Health and M-Commerce [1] increased the contribution of biometric authentication in disparate wireless applications [2] and this is expected to increase even more in the near future. Wireless networks have significant advantages over wired networks such as elimination of cables and freedom of mobility. Whereas the disadvantages are lower channel capacity (i.e. limited spectrum available, power restrictions, noise levels), Denial of Service (DoS), eavesdropping (signal is in the open air and data is not encrypted unless the protocol is encrypted), theft or loss of device (due to size and portability) and Masquerading (i.e. rogue clients pretend to be legitimate endpoint), etc. Currently the use of wireless networking is expanding way faster than before by the introduction of new technologies such as 4G, WiMAX. These networks regardless of whether they use WiMAX or Wi-Fi LANs as defined in the IEEE 802.11 standard are inherently less secure than wired counterparts due to the lack of physical infrastructure [3]. The main issue here is making sure to have a control measure in place prior to establishing a connection, so that access is restricted to the authorized users only. Biometrics can deliver outstandingly here as compared to the traditional solutions for access control, taking into account the rare chances of data being lost or stolen. Unimodal biometrics in the context of security raises several design limitations such as noise in input data, intra-class variation, interoperability, vulnerability against spoof attacks and inter-class similarities [4]. Some of these restrictions can be alleviated through multimodal biometric approaches by providing multiple evidences of the same identity [5]. The purpose of this paper is to develop a simple and accurate method to obtain high level of confidence fingerprint identification and watermarking technique through a simulated investigation. Therefore, based on the proposed methodology, embedding the watermark message into the fingerprint image has been design and developed. This scheme encompasses three step procedure, fingerprint image enhancement, embedding the watermark message into the enhanced fingerprint image and verify the integrity of the claimed user by extracting this watermark from the watermarked fingerprint image. The reminder of this paper is organized as following:

Section 2 describes the role of fingerprint sensor in wireless communication. Section 3 enhancement fingerprint and describes algorithms in fingerprint biometric. Section 4 present watermarking algorithms and finally in section 5 we present result of simulates a projected model and conclusion.

2. Biometric Traits over Wireless Communication

Fingerprinting is one of the more mature technologies used in criminal investigations. A fingerprint image is made of a spatial map of the friction ridges of the skin and the valleys between them. In order to find out if two images are a matching pair, an algorithm of identification is needed to compare two fingerprints by examining the "landmarks" of ridges and valleys. In the majority of the current fingerprint matching systems, the features employed in the matching process are the fingerprint minutiae. Minutiae based fingerprint matching transforms fingerprint image into a minutiae map and generally involves preprocessing, ridge width and ridge direction, enhancement, and minutiae detection [6-8]. Using

fingerprints as an identification system is very popular today and has almost become a synonym for biometric systems. Fingerprint sensors are one of the most accepted and developed biometric techniques in wireless. In addition, it is an appropriate technique for a large number of recognition applications. This technique is recognized by various mobile and handheld companies as an authentication method in their devices such as personal digital assistant or mobile phone that offers biometric security through a built-in fingerprint scanner to restrict access to the devices. In addition, various wireless devices include fixed and mobile equipment with fingerprint recognition sensor such as Lock Secure, and Corporate Access Control Locks. The major problem in utilizing fingerprints in mobile device is the varying image quality due to population characteristics and environmental factors [9]. Therefore, providing the software to deal with the alignment and quality of the image is an issue of concern when employing fingerprints in wireless devices.

3. Fingerprint Enhancement

Once the fingerprint image is captured, its quality is usually improved by enhancement techniques. This is particularly necessary if the image is damaged or not acquired very well. Fingerprint-matching techniques can be classified in three main groups namely; correlation-based, minutiae-based and ridge feature-based matching [10]. In minutiae-based matching technique, minutiae (ridge terminations and ridge bifurcations) are chosen as features. The position of minutiae are extracted from the fingerprint image and stored as sets of points in a plane. The two sets of points, one from the template and the other from the input image, are examined based on their alignment and the number of pairings is used for matching. Typically, in one fingerprint, endpoints and bifurcations combine to form up to 30 minutiae points on average. In minutiae based matching, the attempt has been made to align two sets of minutiae points and make a decision based on the total number of matched minutiae [11-14]. The focus of this section is on the minutiae-based matching and starts from the second step of fingerprint authentication (Enhancement) before embedding the watermark data. This is for the reasons that fingerprint image consist of worthless image area without valuable ridges and furrows which must be excluded before matching a pair of fingers. The valuable remaining area is sometimes known as ROI (Region of Interest). There are many publications in scientific literature on watermark schemes that are based on the enhancement of the fingerprint image [15, 16]. For instance, Hsieh et al. [16] proposed a method based on the fingerprint image enhancement, discrete wavelet transform, and secret sharing scheme. They experimentally have shown that the retrieved enhanced fingerprint images are more recognizable than without enhancement.

3.1 Fingerprint Images Enhancement Algorithms

The performance of feature extraction algorithms depend on the input fingerprint images and usually, fingerprint image enhancement is applied to obtain an enhanced output image through a set of intermediate steps. Various techniques, which are used to enhance the gray level of the fingerprint images, have been published in the scientific literature [17-19]. The majority are based on the information about the local ridge structure in term of estimation of the local ridge orientation from input fingerprint images. However, such algorithms, which perform very well for good quality images suffer a drastic decrease of performance when low quality images are used, due to noise (creases, smudges, and holes). This section presents a novel enhancement algorithm.

3.1.1 Spatial and Fourier Domain Filtering

In [18] enhanced the fingerprint image in the Fourier domain, based on convoluting each image with pre-computed filters of the same size as the processed image. Their algorithms do not use the full contextual information provided by the fingerprint image because of the assumptions that the ridge frequency is constant throughout the image, and decreases the number of pre-computed filters. Another approach has been proposed by enhancing the fingerprint image completely in the Fourier domain. This algorithm is based on dividing the fingerprint into overlapping blocks, and in each block:

$$(x\ y) \qquad \{\ (\quad v)|F(u\ v)|^{k}\} \tag{3-1}$$

This approach does not require the computation of intrinsic images for this operation, which has the effect of increasing the dominant spectral components while attenuating the weak components. According to equation 3.1, a two dimensional Inverse Fast Fourier Transform (IFFT) is applied as a second step, and computing the IFFT of each dimension of the input matrix is equivalent to calculating the two-dimensional inverse discrete Fourier transform (IDFT), defined by the following equation:

$$f(x\ y) \quad —\sum \quad \sum \quad F(m\ n)e^{\overline{\quad}\ \overline{\quad}} \tag{3-2}$$

This technique was proposed by [20] and [21] to perform a sort of contextual filtering without requiring explicitly computing local ridge orientation and frequency. In their algorithm block size of was found to be best and using a fast radix-2 FFT when the block size is a power of two, the FFT speed is optimum. Although , as it is considered by Willis et al. [21] requirements of patching in holes and smoothing, as well as separating incorrectly joined ridges is met in their algorithm, applying this technique raise two issues. The first is discontinuities at the edges of adjacent blocks and the second is at the edges and background of the image. In their algorithm, the former has been compensated by overlapping blocks and later by summing the gray level pixels in each block and assigning the block to the background if this sum exceeds a threshold. However, a large amount of overlap between the neighboring blocks (e.g., overlap of 24 pixels) is necessary which can significantly increases the enhancement time [20]. After analyzing various solutions used a combination of filters in both domains, spatial and Fourier to obtain an appropriate enhanced image. Their algorithm is based on algebraic sum of two enhanced images in which the resulting pixel will be white, if both images are white. As it is considered in their algorithm, Gabor filters have important signal properties such as optimal joint space frequency resolution. The even symmetric form of the Gabor function in their algorithm is given by:

$$G(x\ y) \quad exp\left\{--\left[—\quad —\right]\right\}\cos(2\pi f x) \tag{3-3}$$

3.2.2 Fingerprint Image Binarization

The fingerprint binarization is an algorithm that produces a 1-bit type image from 8-bit grayscale image. However, the adaptive binarization method is based on a threshold t, with gray-level pixels lower than t assigned to 0 and the others to 1. It is known that dissimilar fingerprint images have special contrast and intensity, and therefore, a unique threshold t is not the appropriate value for a general fingerprint image analysis. The local threshold technique changes t, by adapting its value to the average local intensity. In very poor quality fingerprint images, the local threshold mode cannot guarantee acceptable results and a special threshold value, which has sufficient effect, is required. A wide range of evaluation study of locally adaptive binarization has been conducted by [22]. They have shown experimentally that [23] method with post processing step appears to be the best. However, some improvement to this binarization method has been made by [24] and [25] later. The fingerprint binarization based on the adaptive thresholding is a common image-processing tool [26].

4. Proposed Watermarking Algorithm

Different methods in the public domain for fingerprint image enhancement have been reviewed, and a new methodology allowing superior performances is proposed. In order to avoid specific shortfalls of this process, the procedure follows first the application of CLAHE with Clip Limit in order to enhance the contrast of small tiles, to eliminate the artificially induced boundaries and to avoid over-saturation of the image specifically in homogeneous areas. In addition, a combination of filters in both domains, spatial and Fourier is used to obtain an appropriate enhanced image. Embedding the watermark in the transform domain is more robust as compared with spatial domain. Therefore, DWT, which is of latter type, is utilized to embed the watermark into the fingerprint image. This section focuses on the study of watermarking the fingerprint image as used in the proposed biometric cryptosystem. The proposed algorithm is divided into two parts, watermark embedding and watermark extraction. In the watermark embedding stage, firstly, presented memorable word by the user is converted to the image. In a second step, a single-level two-dimensional wavelet (DWT2) is applied to the enhanced fingerprint image and transformed image of the text from prior step. This is to decompose both images into low-pass subband and high-pass subbands. Finally, after embedding watermark coefficients to the most significant coefficients at the low and high frequency bands of the discrete wavelet transform of an fingerprint image, watermarked fingerprint image has been reconstructed by using single-level inverse discrete two-dimensional wavelet transform (IDWT2). In the watermark extraction stage, the memorable word has been used to verify the integrity of the watermarked fingerprint image by the process of detection. Figures 1 and 2 illustrate the flowcharts of embedding and extraction.

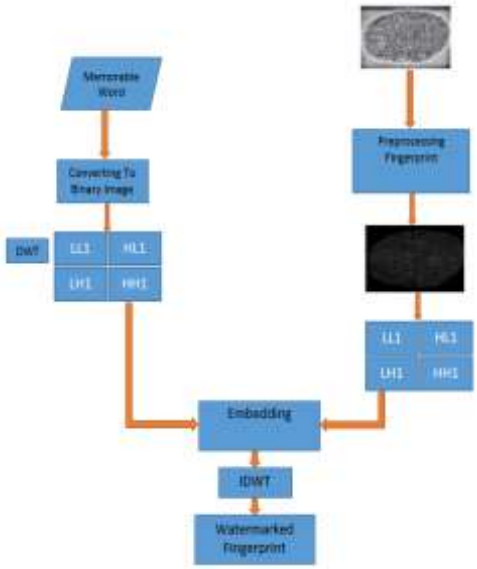

Figure 1: Watermark Embeddi

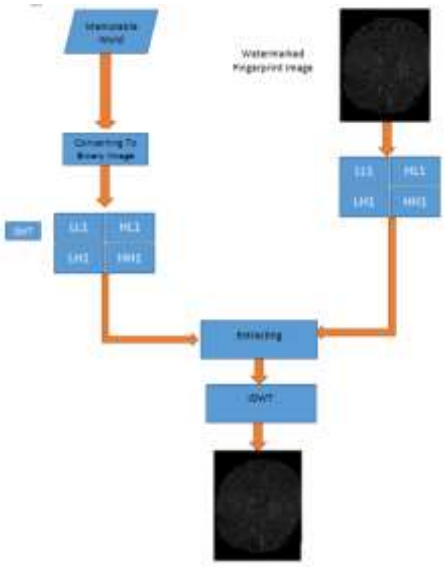

Figure 2: Watermark Extraction Process

The above approach is explained in more detail as follows:

A. Decomposition

As detailed in previous Chapter, watermark can be embedded in either the spatial domain or frequency. The watermark embedded in the frequency domain is more robust than in the spatial domain. A wavelet transform can be interpreted as decomposition into a set of frequency bands having the same bandwidth on a logarithmic scale. It comes with superior advantages and hence, discrete wavelet transform (DWT) is preferred in this work at decomposition stage. As is shown in Figure 3, firstly, input signal is computed by a successive low-pass decomposition (Lo_D) and high-pass (Hi_D). Two-dimensional DWT leads to a decomposition of approximation coefficients at level j in four components. This encompasses the approximation at level j + 1, which is produced from pure low-pass together with the decompositions produced from high-pass in three orientations (horizontal, vertical, and diagonal). The following chart describes the basic decomposition steps for fingerprint and watermark images: Where downsample columns and rows keep the even indexed columns, and even indexed rows respectively. In addition, Lo_D and Hi_D convolve at rows with filter X, the rows of the entry, which is set to "Harr" filter in this experiment, and at columns, with filter x, the columns of the entry. Computing the approximation coefficient (cA) of the watermarked fingerprint image is mathematically shown below:

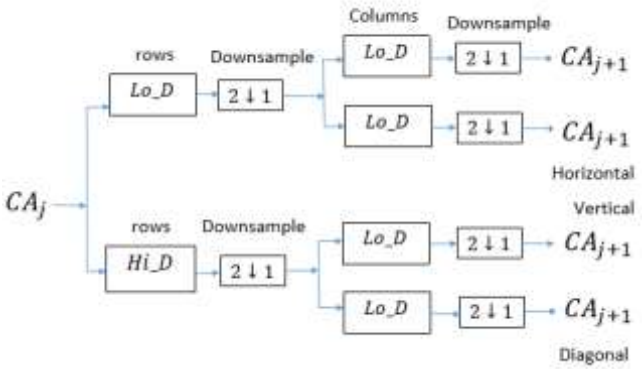

Figure 3: Decomposition steps of two-dimensional DWT [9]

(1) (3 4)

Where represent the of the watermarked fingerprint image I, I_W is the approximation coefficient (cA) of the fingerprint image and the (cA) of the watermark W. As explained above these two coefficient (W and I_W) can be produced by using the low-pass decomposition. In addition, there are three detailed information coefficients (cH cD) of

(3 5)

the watermarked fingerprint image that are embedded in the higher frequency components of the image. Computing these coefficients is based on the following equation:

Where I_W is the coefficient (cH, cD) of the fingerprint image I and W_W is the corresponding coefficient of the watermarked image W. As explained previously, these three coefficients can be

produced from the DWT high-pass decompositions in three orientations (horizontal, vertical, and diagonal). Human eyes are very sensitive to changes from low-pass decomposition but not sensitive to small changes in the edges and the textures which are embedded in the higher frequency components of the image. This is due to sensitivity of human eyes to small changes in smooth part of the image that is represented by low-resolution representation in which most of the information in image is located. Therefore, invisibility of the watermark is kept by selecting a smaller value of α, and a larger value of β.

B. Embedding a Watermark Image into the Fingerprint Image

Once these coefficients are obtained for both fingerprint and watermark images, the watermark image ones can be embedded into those of fingerprint. Firstly, fingerprint wavelet coefficients (I_W) and those from watermarked are generated by a single-level two-dimensional wavelet transformation. Secondly, in order to obtain the approximation coefficient (cA) and three coefficients (cH cD) for the watermarked fingerprint image, the equation 3-4 and 3-5 are being applied. Furthermore, in order to reconstruct the watermarked fingerprint image, inverse Discrete Wavelet Transformation (IDWT) is applied to these coefficients, as is being discussed below.

C. Image Reconstruction

In this step, after embedding the watermark image coefficients, IDWT is applied to the watermarked fingerprint coefficients in order to achieve the final secure watermarked fingerprint image. Those decomposed components can then be assembled back into the original fingerprint image. This process is called reconstruction, or synthesis, and mathematical manipulation that affects synthesis is called the inverse discrete wavelet transform. Therefore, to reconstruct the watermarked fingerprint from the wavelet coefficients, IDWT2 has been performed. Figure 4 illustrates above, where up sample columns and rows insert zeros at odd indexed Columns and rows respectively. In addition, Lo_R and Hi_R at rows convolve with filter X, the rows of the entry, which is set to "Harr" filter in this experiment, while at columns; convolve with filter x the columns of the entry.

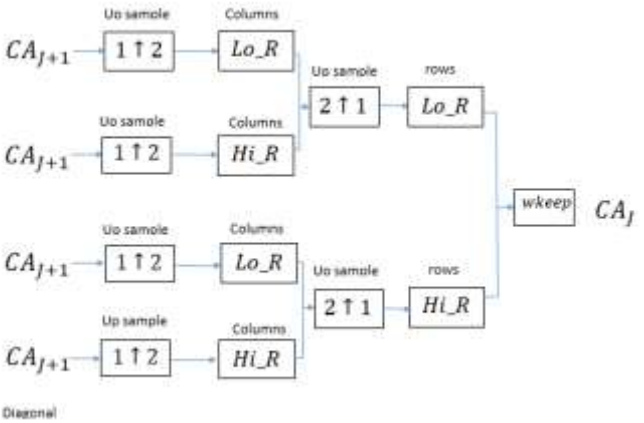

Figure 4: Reconstruction step of Two-Dimensional IDWT [9]

D. Retrieving an Embedded Watermark

In the previous steps, the discrete wavelet transform has been used to decompose images and then watermark image coefficients are embedded into the fingerprint image coefficients and assembled back into the original image by inverse discrete wavelet transform. Generally, the task of decoding the watermarked image is to verify the presence of the watermark image. However, because of using fingerprint image as host image, the fingerprint image should be unique; otherwise, it will cause the false acceptance for the imposter. This is due to the fact that fingerprint technology is unable to obtain the identical image and feature, each and every time scanning and analysis is done. Therefore, in order to address the problem of indistinctness in a fingerprint image when presented at different times, watermark image has been used to extract the fingerprint image. Finally, this extracted fingerprint image can be matched against the one that is stored in the database to verify the integrity of the claimed user. In addition, presence of the memorable word can be verified during this process.

5. Results

This section simulates a projected model over three wireless technologies, WiMAX, Wi-Fi and 3G. After such a model is being simulated, the results will be presented to check the effect of these networks upon the performance of the proposed system in terms of speed, reliability, and the quality of service. Therefore, the five-step challenge/response process will be accomplished over WiMAX, Wi-Fi and 3G, and the most important parameters including corresponding delay, throughput, and jitter will be analyzed. In order to measure QoS (delay, throughput, and jitter), the Wireshark software has been used which is a network packet analyzer. Wireshark will try to capture network packets and display packet data as detailed as possible. The delay (D) was monitored for every single packet and different sizes of watermarked fingerprints were tested using the PING utility tool based on the following equation:

$$\underline{[(Rc-Ts)+(Rc-Tc)]} \qquad (5\ 1)$$

Where is the time at which the packet was sent from the server. The time at which the packet was received by the client on the other hand is . Similarly, is the time at which the packet was sent from the client and the time at which the packet was received by the server is . In addition, in order to experience the worst case of voice features in terms of size, maximum packet size of this feature has been utilized . The tests for every packet size were performed four times, in different periods of a day. Every single packet size was tested 20 times in a single period of a day, and its average was calculated. The second parameter, jitter was monitored automatically on both client and server sides based on the following equations:

$$^1/_2\ \Sigma \quad _____ \quad _____ \qquad (5\ 2)$$

Where and are total number of packets and the time at which the packet (n) is received at the server respectively. In spite of the fact that TCP can address the packet loss issue by retransmitting the missing packets, it can decrease the throughput of the connection. Therefore, these throughputs were measured automatically using Wireshark. The throughput at the client (uplink throughput) was measured when the server was sending and similarly, the throughput at the server (downlink throughput) was measured when the client was sending. The test was carried out around four to five times in order to calculate the average

throughput for every individual file size. Simulation begins by sending the eight various sizes of fingerprint as phase one of proposed system in which the smallest, medium, and the largest sizes of data have been selected. The packets then are delivered through the three selected wireless technologies (WiMAX, Wi-Fi, and 3G) in order to measure QoS (delay, throughput, and jitter). The same process is carried out for the largest voice packet size. The Matlab codes employed in voice feature (cepstral coefficients) extraction have been provided for public use [61]. After the simulation, the results can be extracted from the measured parameters (delay, throughput, and jitter). The parameters here can be varied over the different wireless technologies. Finally, with the parameters being varied and under different technologies, the results can be evaluated. The experiment was carried out by connecting the system to a hub and configuring its respective IPs. The substation was connected to a computer and was treated as a client. The base station was connected to another system and treated as a server. The readings for delay were noted initially at 5% bandwidth. To enable monitoring of delay over small packet sizes, the bandwidth was reduced to 1%. Ping application did not react to 1% bandwidth since the packets were damaged and hence the bandwidth was set to 3%. In addition, the Wi-Fi network at Brunel University and T-Mobile 3Gnetwork card has been used for this simulation. The computer connected with the network card was treated as the server and another as client. Tables 5-1, 5-2, and 5-3 depict the average delay, throughput and jitter for every corresponding fingerprint packet respectively in WiMAX, Wi-Fi and 3G networks. The delay for every single network varies which shows the speed, external interference, and performances of every single network. As is shown in these three tables, the maximum delay, throughput, and jitter are 18.19, 507and 1.84 respectively in WiMAX, 82.44, 445 and 3.79 in Wi-Fi and 284.29, 129 and 12.64 in 3G networks.

Table 5.1: Delay, Throughput, and Jitter for WiMAX

	WiMAX							
FILE SIZE (KB)	54	59	72	150	256	364	482	570
Delay(ms)	14.4	14.52	18.12	16.11	17.19	12.56	18.19	17.54
Throughput(kbps)	502	502	501	507	504	501	502	504
Jitter(ms)	1.76	0.89	1.84	1.92	1.21	0.94	1.14	1.17

Table 5.2: Delay, Throughput, and Jitter for Wi-Fi

	Wi-Fi							
FILE SIZE (KB)	54	59	72	150	256	364	482	570
Delay(ms)	80.24	81.39	80.91	81.27	80.63	82.44	81.42	81.18
Throughput(kbps)	346	354	402	296	336	445	339	375
Jitter(ms)	2.17	3.79	3.25	2.36	2.76	1.92	1.21	2.25

Table 5.3: Delay, Throughput, and Jitter for 3G

	3G							
FILE SIZE (KB)	54	59	72	150	256	364	482	570
Delay(ms)	161.32	162.26	164.42	166.17	216.2	227.37	238.47	284.29
Throughput(kbps)	114	119	121	113	129	134	116	118
Jitter(ms)	10.54	9.65	10.37	12.64	10.31	11.54	12.52	11.86

WiMAX technology proved to be the quickest with high performance to transfer biometric data over the network due to the shortest delay as compared to the other networks (Wi-Fi and 3G). In addition, though different sizes of packets have been sent, the network delay always remains just about constant in WiMAX and Wi-Fi. However, the measured throughput varies for each technology and this is due to the experiments being carried out in different times, i.e. peak and off-peak. The jitters of all the three technologies did vary drastically from one another. Obviously, specific requirements for any biometric system depend on the scenario and its requirements. To the best of our knowledge, there is no set standard for applying biometrics over internet or wireless communication, unless for voice and video. Latter addressed by ITU (International Telecommunication Union), Cisco[38] measures standard requirement for QoS parameter (150 ms is defined as acceptable delay, higher than 400ms is unacceptable and between these values user should be aware of quality issues, acceptable jitter is 30ms, and the guaranteed bandwidth for the video should be at least 1.2 times the actual throughput). Therefore, if guaranteed bandwidth is accepted for the voice and video, it is accepted in this algorithm (fingerprint) due to the less throughput requirement. There is however no restrictions on the proposed challenge/response algorithm in terms of delay, jitter, and throughput except in cases that requires verifying identities in real-time or near real-time delivery (no appreciable time delay). The Figures 5, 6 and 7 show the delay, throughput and jitter comparison of different technologies with watermarked fingerprints differing sizably for WiMAX, Wi-Fi and 3G.

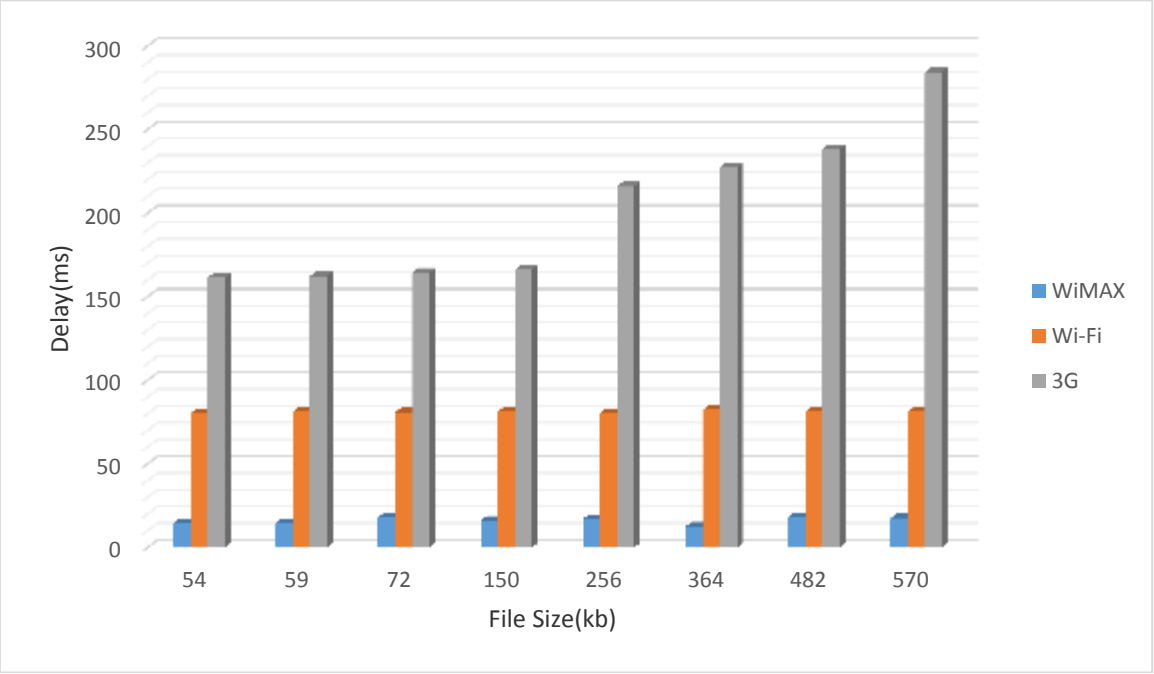

Figure 5: Delay Comparison for Different Size of Watermarked Fingerprint over Different Technologies

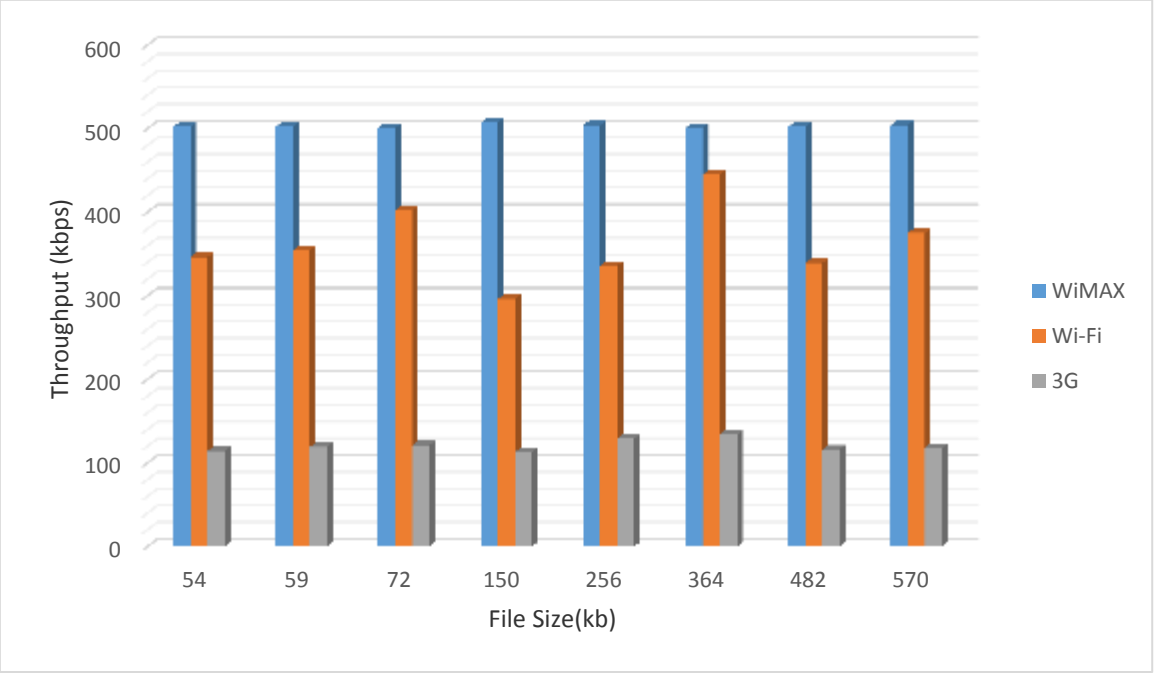

Figure 6: Throughput Comparison for Different Size of Watermarked Fingerprint over Different Technologies

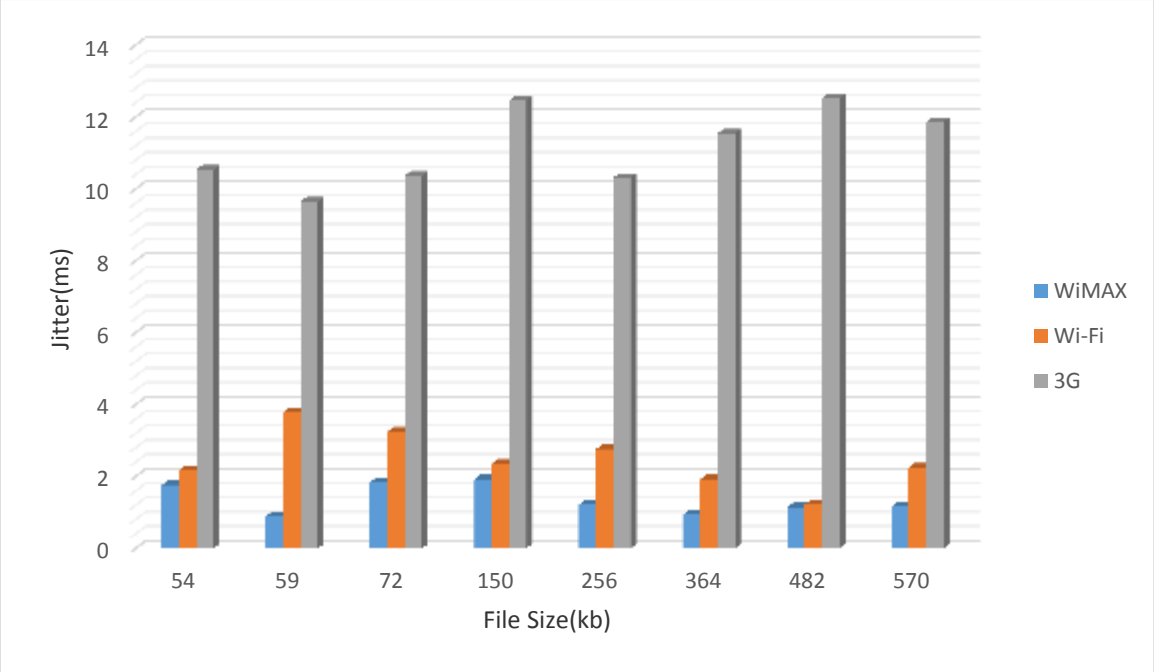

Figure 7: Jitter Comparison for Different Size of Watermarked Fingerprint over Different Technologies

6. Conclusions

The main concentration of this paper has been designated to having a control measure in place prior to establishing a wireless network connection, so that access is restricted to the authorized users only. , restriction of access to authorized users only is provided by a technique referred to hereafter as biometric cryptosystem. Briefly, the system is built upon a complete challenge/response methodology in order to obtain a high level of security on the basis of user identification by fingerprint. First is the enrolment phase by which the database of watermarked is created and sending it to the server through wireless medium. Later is the verification stage at which claimed users are verified against the database, and it includes of five steps. Firstly faced by the identification section, one is asked to first present one's fingerprint and a memorable term, former is watermarked into latter, in order for system to confirm the fingerprint and verify the validity of it by retrieving the challenge for accepted user. In order to implement fingerprint watermarking, i.e. incorporating the memorable term as a watermark message into the fingerprint image, an algorithm of five phases has been developed. The first three novel phases having to do with the fingerprint image enhancement have been followed with further two steps for embedding, and extracting the watermark into the enhanced fingerprint image utilizing Discrete Wavelet Transform (DWT).

References:

C. Gabriel and et al, "A Perspective of State-of-the-Art Wireless Technologies for E-Health Applications", IEEE International Symposium on IT in Medicine & Education, pp. 76 – 81, 2009.

C. Li, C. C. Lee, "A novel user authentication and privacy preserving scheme with smart cards for wireless communications", Mathematical and Computer Modelling, Vol. 55, pp. 35-44, 2012.

C. T. Huang, J. M. Chang, "Responding to security issues in WiMAX networks", IEEE Comp. Society IT Professional Magazine, Volume 10, Issue 5, pp. 15–21, 2008.

D. Fan and et al, "A Novel Probabilistic Model Based Fingerprint Recognition Algorithm", Procedia Engineering, Vol. 29, pp. 201-206, 2012.

D. Miller, B. Fauve, "Mobile e-commerce to drive voice-based authentication", Biometric Technology Today, Volume 2012, pp. 5-8, 2012.

D.S. Guru, H.N. Prakash, "Fingerprint template protection with minutiae-based bit-string for security and privacy preserving", Expert Systems with Applications, Vol. 39, 2012, pp. 6157-6167.

H. M. Sim and et al, "Multimodal biometrics: Weighted score level fusion based on non-ideal iris and face images", Expert System with Applications, Volume 41, pp. 5390-5404, 2014.

K. Cao and et al, "A novel ant colony optimization algorithm for large-distorted fingerprint matching", Pattern Recognition, Vol. 45, pp. 151-161, 2012.

K. Zebbiche, F. Khelifi, "Region-Based Watermarking of Biometric Images: Case Study in Fingerprint Images", International Journal of Digital Multimedia Broadcasting, Vol. 2008, Article, 2008.

M. Heenaye, M. Khan, "A Multimodal Hand Vein Biometric based on Score Level Fusion", Procedia Engineering, Vol. 41, pp. 897-903, 2012.

M. Khitrov, "Talking passwords: voice biometrics for data access and security", Biometrics Technology Today, Vol. 2013, pp. 9-11, 2013.

N. Nagamalleswara Rao and et al, "An efficient copyright protection scheme for digital images using Biometrics and Watermarking", IEEE International Conference on Computer Science and Information Technology, pp. 69 – 74, 2009.

R. Giot and et al, "Fast computation of the performance evaluation of biometric systems: Application to multibiometrics", Vol. 29, pp. 788-799, 2013.

R. Giot, C. Rosenberger, "Genetic programming for multibiometrics", Expert Systems with Applications, Vol. 39, pp. 1837-1847, 2012.

W. J. Wong and et al" Enhanced multi-line code for minutiae-based fingerprint template protection ", Pattern Recognition Letters, Vol. 34, pp. 1221-1229, 2013.

Y. Ding, A .Ross, "A comparison of imputation methods for handling missing scores in biometric fusion", Pattern Recognition, Vol. 45, pp. 919-933, 2012.