World Academy of Science, Engineering and Technology
International Journal of Electrical and Computer Engineering
Vol:6, No:2, 2012

OFDM and Fingerprint Authentication for Efficient Airport Security

K.Amrithavarshini, S.Chandrachudeswaran

***Abstract*—**This paper presents an idea to improve the efficiency of security checks in airports through the active tracking and monitoring of passengers and staff using OFDM modulation technique and Finger print authentication. The details of the passenger are multiplexed using OFDM .To authenticate the passenger, the fingerprint along with important identification information is collected. The details of the passenger can be transmitted after necessary modulation, and received using various transceivers placed within the premises of the airport, and checked at the appropriate check points, thereby increasing the efficiency of checking. OFDM has been employed for spectral efficiency.

***Keywords*—**Orthogonal Frequency Division Multiplexing, FFT Algorithm, Fingerprint Authentication, Airport Security

I. Introduction

IN the airports, passengers are required to check –in two to three hours prior to their flight. This is because of the long procedure they have to undergo before boarding.

This paper provides an idea to improve the efficiency in the airport check-in procedures. Due to various other reasons, including emergencies, the passengers may be unable to board the flight in time. This paper also provides a means of detecting such passengers, who are in the airport premises, but not on board. Moreover to avoid fake authentication of passengers, we employ finger print (Biometric technique) authentication system[1],[2], which provides the passenger with an entry only their fingerprints are match with the patterns stored in the database.

Efficiency of this system is improved employing OFDM (orthogonal frequency division multiplexing) combined with the finger print authentication system. The carriers used in OFDM contain the user information and are transmitted using a transceiver. The fingerprint is also obtained from the passenger at the time of entry into the airport on production of their flight ticket. A number of transceivers are placed in and around the airport, and these are placed at the security checkpoints. The passenger information is received at these locations, a second fingerprint is obtained from the passenger, compared with the one stored initially, and the passenger is allowed or denied permission to move further, depending on the result of comparison of the images.

K.Amrithavarshini is with the Department of Electronics and Communication Engineering at Sri Venkateswara College of Engineering, Pennalur, Sriperumbudur-602105(e-mail: amrithakannan90@gmail.com)

S.Chandrachudeswaran is with the Department of Electronics and Communication Engineering at Sri Venkateswara College of Engineering, Pennalur, Sriperumbudur-602105(e-mail: chandrachudeswaran@gmail.com)

II. System Overview

A. OFDM Unit Design

OFDM (orthogonal frequency division and multiplexing) is a multicarrier transmission technique, which divides the available spectrum into many carriers, each one being modulated by the low rate data stream. OFDM uses the available spectrum very efficiently by spacing the channels very close together. This can be achieved by making all the carriers orthogonal to one another, thereby preventing the interference between the closely spaced carriers. The orthogonality means that each carrier has an integer number of cycles over a symbol period. Due to this the spectrum of one carrier has a null at the centre frequency of another. This results in no interference between the carriers, allowing them to be placed as closely as possible. OFDM overcomes most of the problems faced by the TDMA (Time division multiple access) and FDMA (Frequency division multiple access).Each carrier in the OFDM has a very narrow bandwidth; therefore the symbol rate is very low. This results in the signal having a high tolerance to multipath delay spread. The sinusoidal signals are placed, each differing in frequency by 1/Tu Hz where Tu is the symbol length. Cyclic prefixes are used to remove effects of Intersymbol Interference (ISI). OFDM provides good immunity to the system against Co-channel Interference and impulsive parasitic noise. Interleaving and adequate coding of data is done to recover lost symbols, due to frequency selective fading channels. Forward Error Correction (FEC) can be employed to provide frequency diversity.

B. OFDM Transmitter

In order to generate the OFDM successfully, the relationship between the carriers should be carefully controlled to maintain the orthogonality between the carriers. For this reason OFDM is generated by firstly choosing the spectrum required, based on the input data and modulation scheme used. OFDM is most efficiently implemented using FFT & IFFT algorithms [5]. Each carrier to be produced is assigned some data to transmit .The amplitude and phase of the carrier is calculated and based on this modulation scheme is chosen (usually BPSK, QPSK or QAM).The required spectrum is converted back into time domain signal by taking the IFFT (Inverse Fast Fourier Transform).The function of the IFFT is to ensure that the carriers produced are orthogonal in nature. An OFDM symbol is given by N point complex modulation sequence through IDFT as

$$x(n) = \frac{1}{\sqrt{N}} \sum_{k=0}^{n-1} X(k) e^{j2\pi \frac{nk}{N}} \quad n=0, 1, 2\ldots N\text{-}1 \quad (1)$$

The above signal consists of N subcarriers or sinusoids, which have been modulated with the complex data X. The l-th frame signal can be generated according to the above equation as

$$s_l = \sum_{k=0}^{N-1} X_{i,M-1}(k)\Psi_1(n,k) + \sum_{i=0}^{M-1}\sum_{k=0}^{N-1} X_{l,i}(k)\Psi_2(n-iN-P,k) \quad (2)$$

Where $\Psi_1(n,k)$ and $\Psi 2(n,k)$ are the two rectangular window functions defined by

$$\Psi_1(n,k) = \frac{1}{\sqrt{N}} e^{\frac{j2\pi k(N-P+n)}{N}} \qquad 0 \le n \le P-1$$

and 0 elsewhere

$$\Psi_2(n-iN-P,k) = \frac{1}{\sqrt{N}} e^{\frac{j2\pi k(n-P-iN)}{N}} \quad (3)$$

for $P \le MN + P - 1$

and 0 elsewhere

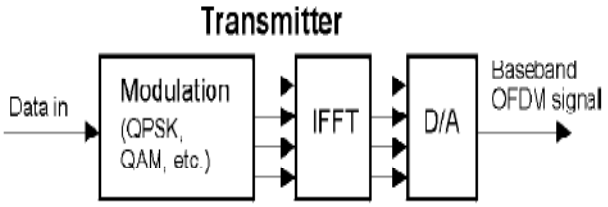

Fig. 1 Block diagram of OFDM transmitter

C.OFDM Receiver

In the receiver side, the Baseband OFDM signal is given to the FFT (Fast Fourier Transform), where the time domain signal is converted into equivalent frequency spectrum. This is done by the equivalent waveform, generated by the sum of orthogonal sinusoidal components. The amplitude and phase of the sinusoidal components represent the frequency spectrum of the time domain signal. Forward FFT takes the signal, multiplies it successively using complex exponentials, over the range of frequencies, sums each product, and plots the result as a coefficient of that frequency. These coefficients represent how much of the frequency is present in the input signal.

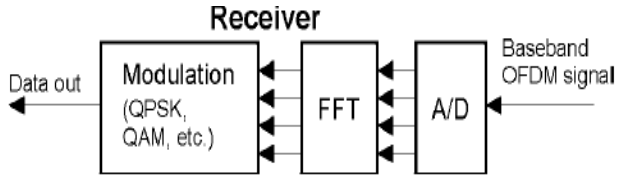

Fig. 2 Block diagram of OFDM receiver

The signal generated is a base band, thus the signal is filtered and stepped up in frequency before it is transmitted. This can be done by a process called as frequency translation.

D.Fingerprint Authentication

Biometrics is the process of automatically differentiating the people on the basis of individuality information from their biometric features such as Fingerprints, Iris pattern, Palm veins and Hand geometry etc. These techniques are used to identify the person accessing the system. Universality, uniqueness, permanence, measurability, circumvention and performance are the seven factors to be considered when assessing the suitability of any trait for a particular type of biometric authentication. Among all, fingerprint authentication [2] is the most widely used biometric device, because of its low cost and easy usability by users.

There are three basic types of fingerprints viz. arch, loop and whorl. Depending upon the variation in the characteristic of the minor details of fingerprints such as ridge endings, bifurcations and short ridges, various types of fingerprints are obtained. The Fingerprint recognition system in general has three modules:

1) Preprocessing modules that include smoothing and thinning for the refinement of the image against image acquisition sensor. Sensors used for obtaining the fingerprint can be optical, ultrasonic, or capacitance based. In these, the capacitance based sensors are preferred as there are lesser chances for duplicate fingerprints to get authenticated.

2) Extraction module that extracts the features in the fingerprint image.

3) Matching module that matches the image obtained with the template image stored earlier.

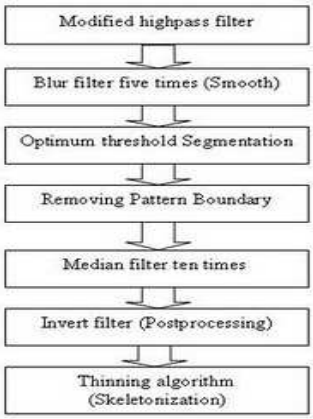

Fig. 3 Fingerprint recognition process

The Fingerprint module has two phases: enrollment and verification. In the enrollment stage ,the fingerprint images ,direction images and circular data can be obtained from

binary finger print images after image preprocessing such as low pass filter and feature extraction.In the verification module, after preprocessing of input image using displacement detection module, we find out the displacement between the enrolled direction image and the input direction image. Therefore the matching module matches the circular profile data with the input circular data according to the information of displacement.

Implementation of the fingerprint authentication Unit using Capacitive sensors improves the efficiency of the unit. Capacitance sensors use the principle of capacitance in order to form the fingerprint images. In this method of imaging, the sensor array pixels each act as one plate of a parallel plate capacitor, the dermal layer (which is electrically conductive) acts as the other plate, and the non-conducting epidermal layer acts as a dielectric. Either a passive capacitance or active capacitance.

A passive capacitance sensor uses the principle outlined above to form an image of the fingerprint patterns on the dermal layer of skin. Each sensor pixel is used to measure the capacitance at that point of the array. The capacitance varies between the ridges and valleys of the fingerprint due to the fact that the volume between the dermal layer and sensing element in valleys contains an air gap. The dielectric constant of the epidermis and the area of the sensing element are known values. The measured capacitance values are then used to distinguish between fingerprint ridges and valleys.

Active capacitance sensors use a charging cycle to apply a voltage to the skin before measurement takes place. The application of voltage charges the effective capacitor. The electric field between the finger and sensor follows the pattern of the ridges in the dermal skin layer. On the discharge cycle, the voltage across the dermal layer and sensing element is compared against a reference voltage in order to calculate the capacitance. The distance values are then calculated mathematically [3], [4], and used to form an image of the fingerprint. Active capacitance sensors measure the ridge patterns of the dermal layer like the ultrasonic method.

(a) (b)

Fig. 4 (a) Binary image from sensor (b) Image from the high pass filter

III. Working Of The System

The basic block diagram of the system consists of two modules as mentioned earlier: OFDM block and Fingerprint Authentication unit. The simplified block diagram of the fingerprint authentication unit and the overall checking system is as given below:

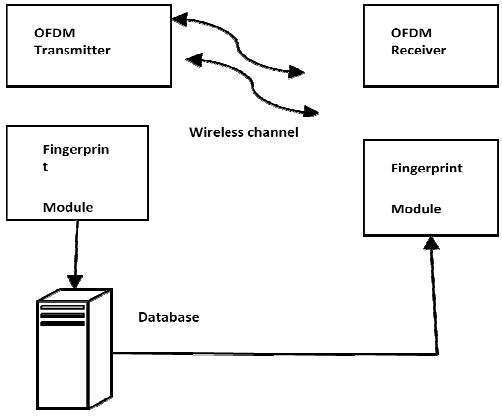

Fig. 5 Block diagram of Authentication Module

The passenger is initially checked in, with identification information, and given the boarding pass. The fingerprint is scanned and stored in the database. Active capacitance sensors are used, which eliminate the need for clean, undamaged epidermal skin and a clean sensing surface. This improves the efficiency of the system.

The use of OFDM allows us to allocate a large number of passenger information, due to the spectral efficiency. Employing OFDM using FFT/IFFT algorithms increases the efficiency further.

The boarding pass consists of OFDM transmitter, quite similar to an RFID tag, which operates in GHz range. The various passenger details like passport number, passenger name, and other details are verified initially. Modulation techniques like QPSK and QAM can be employed to use the bandwidth effectively. The passenger information is modulated, using one of these techniques, and then multiplexed using OFDM. Here using cyclic prefix codes rules out the chances of Intersymbol Interference (ISI). Walsch codes can be used to maintain simplicity. This is done automatically using a PC which already stores these predefined details. The backend of the system is wired connection using serial connection between computers, which transmits the fingerprint images to different check-in locations. The transmitter is a active component which is similar to the mobile handset, very similar to the Base station transceiver employed in the GSM (Global System for Mobile Communication) standards. The bandwidth of the OFDM is chosen in the order of GHz and the sub carriers are also in same range. This ensures that the size of transmitters and receivers are reduced, allowing easy integration of transmitter onto the boarding pass.

At the check-in locations, a receiver which is capable of receiving this GHz signal is designed. There is a computer which is connected serially to the transmitter end database, and this receives the image. A second scan of the fingerprint is taken. The two images are compared. If a match occurs, the passenger is authenticated. There is always a possibility that the passenger might get lost in the airport. We can however track this using the OFDM system.

As mentioned earlier, numerous transceivers are placed at all points in the airport which keep transmitting the user information continuously. These transceivers can be made to send out paging signals outside. If a passenger comes near a transceiver, or even within its range, the transmitter on the passengers boarding pass responds to those paging signals and the location of the passenger can be known and reported automatically to main database.Also, there is a minimum possibility that the passenger travelling might get hurt in his fingers, in order to overcome that when passenger is first checked .She/he is asked for left and right thumb fingers. By default only the right thumb is transmitted. If the person is hurt, then corresponding details of the passenger is first received and if it matches, then the passenger is asked for the left thumb impression if it also matches then the particular passenger is authenticated. This thereby avoids or completely eliminates terror attacks in the airport.

IV. Advantages

Passengers do not have to wait for long hours in the queues prior to their flights, as this system ensures quick verification of passenger information, due to the absence of human errors. The number of security checks can also be reduced in the airport, due to the usage of fingerprint authentication, which eliminates chances of fraud. Tracking a passenger is very easy using this system. Lesser man power is required as a result of implementing this system; therefore the errors occurring in the system is reduced. The usage of OFDM technique proves to be advantageous in many ways. Equalization in OFDM is very simple compared to single-carrier systems. In case of corruption of data, the information from the affected channels can be erased and recovered using Forward Error Correction codes. The cyclic prefix, apart from preserving the orthogonality, also helps the receiver in capturing multi-path energy efficiently. The bands and tones can be dynamically turned on/off for coexistence with other devices.The usage of Fingerprint Recognition is better than the other biometric authentication because of its robustness. Fingerprint scans are more reliable and stable when compared to iris, voice and face recognition methods. Moreover, its low cost and easy maintenance gives it an upper hand over the other techniques.

V. Conclusion

The OFDM is used to increase the bandwidth efficiency of the system, and hence can be used to allocate more number of passengers in the specified bandwidth. Fingerprint Authentication prevents fake identification of passengers. This reduces the number of checks required in the airport, thereby reducing the waiting as well as reporting time of passengers.

VI. Future Scope

The systems in the backend are connected using the serial connection; this can be changed by the optical fiber connection in order to reduce the transmission time and errors. This system can be integrated to the GPS system (Global Positioning System) in order to detect the passenger outside the airport premises.

References

[1] S.B.Pan, D.Moon, Y.Gil, D.Ahn and Y.Chung, “An ultra low memory fingerprint matching algorithm and its implementation on a 32-bit smart card”, IEEE Trans. Consumer Electronics, Vol 49, pp-453-459, May 2003.

[2] A.K.Jain, L.Hong, S.Pankanti and R.Bollc, “An Identity Authentication System Using Fingerprints”, Proceedingd of the IEEE, Vol 85, No.9,pp-1365-1388,Sept 1997.

[3] D.Maio and D.Maltoni, “Direct grayscale minutiae detection in fingerprints”, IEEE Trans. Pattern Analysis and Machine Intelligence, Vol 19, pp-27-40, Jan 1997.

[4] H.Lin, Yifei Wan and A.Jainm “Fingerprint image enhancement algorithm and performance evaluation”, Vol 20, pp-777-789,Aug 1998.

[5] S.B.Weinstien and P.M.Ebert, “Data transmission by frequency division multiplexing using the Discrete Fourier transforms”, IEEE Trans Communications,Vol COM-19,pp-628-634, Oct 1971.