World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(Research Article)

Face recognition based physical layer security system for next-generation wireless communication

Md. Ariful Islam [1, *], Md. Tofail Ahmed [2], Md. Imran Hossain [3], Md. Humaun Kabir [4] and Sujit Roy [4]

[1] *Department of Electrical and Electronic Engineering, Pabna University of Science and Technology, Pabna-6600, Bangladesh.*
[2] *Department of Information and Communication Engineering, Pabna University of Science and Technology, Pabna-6600, Bangladesh.*
[3] *Department of Electrical, Electronic and Communication Engineering, Pabna University of Science and Technology, Pabna-6600, Bangladesh.*
[4] *Department of Computer Science & Engineering, Bangamata Sheikh Fojilatunnesa Mujib Science & Technology University, Jamalpur-2012, Bangladesh*

World Journal of Advanced Research and Reviews, 2023, 18(03), 524–532

Publication history: Received on 01 May 2023; revised on 11 June 2023; accepted on 13 June 2023

Article DOI: https://doi.org/10.30574/wjarr.2023.18.3.1099

Abstract

Security system in every sector all over the world is a most demandable and crucial issue to protect the fake user especially in wireless communication system. The most common feature in current wireless communication system is only transmitted users' information; consequently, it is difficult to identify the actual sender to attain the desired security. Face recognition is one of the most popular security systems in biometric authentication, which can detect intruders to restricted or high-security areas in wireless communication sector, and help in minimizing the face user. In this paper, we proposed a system that is the senders will transmit message information with their image to confirm the original senders. A face-recognition algorithm will be implemented at the receiver end. When a senders' transmitted information enters to the receiver section, the image of sender will be separated from original message signal and sent to the face-recognition algorithm to be analysed and compared with an existing database of trusted user. An alarm goes off if the user is not recognized.

Keywords: AWGN; BPSK; Face Recognition; PSK; QAM; Wireless Communication

1. Introduction

In recent years, security is the first demand to protect personal or official information in every sector of commutation system. It is more important to identify who is the original sender of information over the channel to fulfil the requirement of security system. There have been many choices in conventional technology and biometric technology to ensure the security demands of every communication system. The conventional security systems such as using cryptic keys, passwords, and other methods will be defective if objects for access are lost [1]. Those security systems have many disadvantages when someone forgets their keys or password. The development of technology in the security system presently offers more convenient systems to users in various parts of life. One of them currently trending is automatically recognizing a user when they are trying to access any system. Biometrics is one of the best solutions to recognize unauthorized access to any system that has the ability for a computer to recognize a human through a unique physical attribute [2]. Biometric systems are increasing very speedily, particularly in security technology to access data because they can fulfil two functions, users' identification as authentication, and verification. The biometrics security systems have physical characteristics that cannot be missing, cannot be forgotten, and cannot be counterfeited because

[*] Corresponding author: Md. Ariful Islam

the inherent properties of humans will differ between humans and other humans so that their individuality is fixed [3]. The face has a physiological feature to identify the user as authentication is very convenient, fast, and highly secure because that is easiest to distinguish between individuals. So, face recognition is one of the best biometrics technologies that have been used in a few sectors, studied, and developed for increasing quality and accuracy [4]. Face recognition is a technique that takes an image or a video of a person's face by using a camera or saved image from an image stored device and compares it to another image faces of that person image is stored in a database. For implementing a facial recognition technique, several pictures of a person need to be taken at different angles and with diverse facial expressions for storing in the database to identify that person next time [5]. At the time of authorization and identification the taken image of a person is compared to those images that have been previously recorded in the database. Recently, facial recognition is most demandable biometric security system because it can be worked from a faraway distance even without the person being conscious that he/she is being scanned [5]. The face recognition system is better than other biometric techniques for the purpose of facial authentication and identification because it is easy to alter someone's face and store it in a database. When the facial recognition technology is applied in combination with other systems such as wireless communication, wired communication, mobile communication and so on it can be increased dramatically of verification and identification to meet the demand for security system.

In this work, we present how an automated security communication system can be implemented with the help of the face recognition technique. At transmitter, a person transmits his/her information along with his/ her image over wireless communication channel. At receiver, the transmitted image of person feed into facial recognition algorithms to authenticate and identify who actually send the information which can be accomplish the security of data transmission.

2. Literature review

Face recognition is an automatic biometric method to recognize the identity of a people with the help of his/her physiological characteristics [6]. Biometrics word means ''life measurements'' is the combination of two Greece words one is (Bio) and another (Metrics) [7]. It is a very much demandable user authentication system compare with other safety system in computer security world [8]. Automatically identification or verification of a user is first purpose of a biometric system. It works in a process that the input data (pictures, fingerprints, or voice) of user is given to the system and it will compare the given input to a previously stored database to identify the user [9]. Physiological biometric user identification system is most popular between physiological and behavioural biometric system. Physical features of a user such as iris scans, fingerprints, and face recognition are used in physiological biometric. Behaviour patterns such as hand-writing, voice and key-stroke are used to identify a person because of human inherent properties of those behaviour are vary from person to person [10]. Among physiological biometric systems face recognition is normally used to identify for authentication of a person from his/her input image. Generally, face recognition is a three-step procedure. Firstly, a camera takes an image of a person or it can be a stored image. Secondly, a computer faces recognition algorithm is use to normalize the taken image of that person so that it is in the same format (size, resolution, view, etc.) as the image on the system's database. The normalization of the image gives us a normalized image of the individual. Finally, a matcher compares the normalized image with the set (or sub-set) of normalized images on the system's database and provides a similarity score that compares the individual's normalized image with each image in the database set (or sub-set). Face detection and recognition security system is suitable for home automation security system based on using Internet of Things (IoT). The face of a person compares with the stored database to give access to the home and restrict to access any unregistered person [11]. Face recognition-based attendance system is a procedure of recognizing students by using face biostatistics with the help of an efficient and robust device for taking attendance in a classroom without any time consumption and manual work [12]. It is suitable for industries, offices and even air-ports for identifying unauthorized people. The face recognition system has an advantage which is user friendly method [13]. Face recognition can be used in mobile devices because of their flexibility but it has constraints on processing power, limited storage, limited bandwidth, privacy, and security issues [14-15]. Face recognition method is generally used in the security, username identification, password application, and marketing applications (based on identity) [16-22]. It is clear that face recognition system is used in application. There are several methods are used in face recognition such as (Principal Component Analysis, Linear Discriminant Analysis, Independent Component Analysis, Local Binary Pattern etc.) [23]. Among all face recognition method, the Independent Component Analysis (ICA) algorithm achieves a result of 86.7% to recognize faces which is considered a good result, as it compares with Principal Component Analysis (PCA) algorithm on the same sample, where the result is 76.7% [24]. In this paper we proposed a security system using PCA face recognition method for next generation wireless mobile communication system.

3. Methods of face recognition

Face recognition systems are already implemented in almost every security system sector all over the world despite that it is an interesting topic for researchers on how to use it effectively and how to make it more robust. The current face recognition system performs well in comparatively static and controlled environments. Still, it does not show expected performance due to variations of different features such as pose, facial expressions, time, and the illumination of light change when the images are taken [25]. The research needs to eliminate the effect of these features to create an accurate and more authentic face recognition system. Different face recognition algorithms work by using different methods but their system models are almost similar. Figure 1 shows the block diagram of the face recognition system [26].

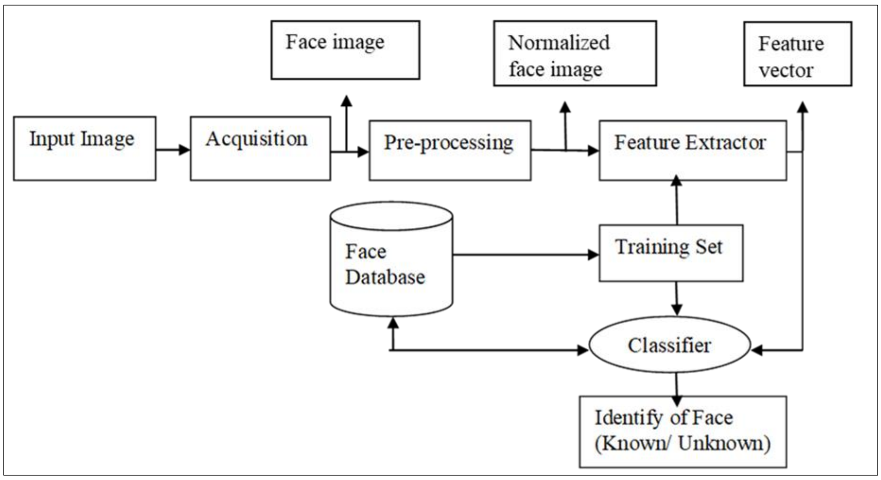

Figure 1 Block Diagram of the Face Recognition System

The steps of face recognition process to identify a known/ unknown person can be divided into three main phases. These are face detection, facial feature extraction and face recognition [27]. In the face detection phase, it represents a face using the successive algorithms of detection and identification to determine whether or not the given image represents a face and the detected image is transformed into scaled and rotated image as like the images from the database. In the second phase, the facial feature extraction works to extract the unique properties of the face image for comparing with the images from the database. Finally, the classification phase use to identity of a known/ unknown person from the database with the smallest differences compared to the input face image. It may use threshold value if the differences are very small. After all, the person will be known if the input face is in the database otherwise the person will be unknown.

4. Function of Transmitter

A power-domain based model with a single transmitter is illustrated in Figure 2. Transmitter is represented as the base station (BS) where two different signals namely UE-image (image of the user) and UE-data (information of the user) are generated and power is allocated at the BS before the transmission, considering the procedure of the signal digital modulation at the transmitter side. Then the image is passed to image to bits conversion model to convert image into bits. After that, modulator is adopted to process the converted bits for bits transmission. The superposition coding (SC) are applied on the modulated signals of user at the BS after modulation. IFFT is used to convert real and imaginary frequency space images (produced by IFFT) into a normal image. The addition of the cyclic prefix (CP) adds robustness to the OFDM signal. Let consider $X_{1,i}$ and $X_{2,i}$ that are denote as modulated signals at the transmitter corresponding to UE-image and UE-data, respectively and i denotes the $i-th$ modulated symbol. SC signals of UE-image and UE-data are given as $S_1 = \sqrt{\sigma}\ X_{1,i}$ and $S_2 = \sqrt{1-\sigma}\ X_{2,i}$ respectively at the transmitter side.

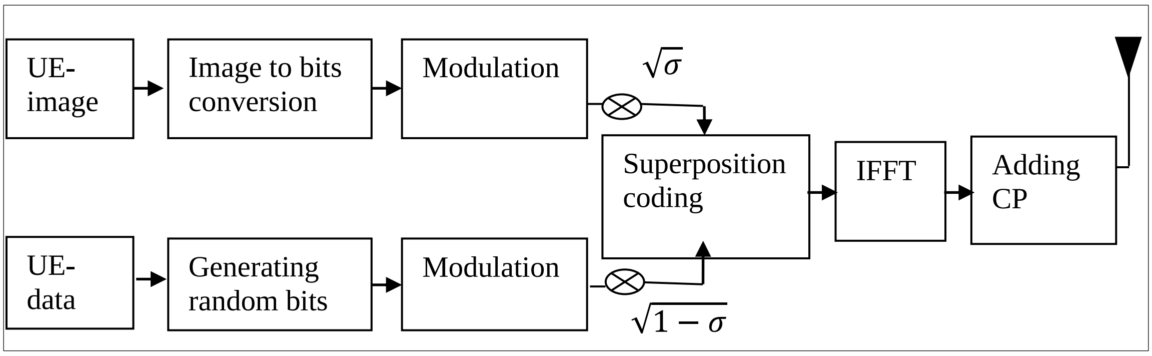

Figure 2 Block Diagram of Power Domain Based Transmitter

Where, σ denotes the power assignment factor for power-domain non-orthogonal multiple access technique and adding cyclic prefix (CP) before beginning the transmission [28]. The power assignments for UE-image denotes as $(\sqrt{\sigma})$ is more than the power of UE-data denotes as $\sqrt{1-\sigma}$ that represents as $\sqrt{\sigma} > \sqrt{1-\sigma}$ and the sum of transmit power allocation factor is restricted to σ. So, the transmit signal x at BS is superposed as:

$$x = S_1 + S_2 = \sqrt{\sigma}\ X_{1,i} + \sqrt{1-\sigma}\ X_{2,i} \qquad \text{(i)}$$

5. Method of Receiver

The working principle of receiver is to assign different power coefficients for different signals of user namely UE-image and UE-data at downlink system and employed Successive Interference Cancelation (SIC) operation to separate the transmitted signals. The receiver block diagram is shown in Figure 3; the received user equipment (UE) time-domain signals can be represented as:

$$y = h_1 x + \delta \qquad \text{(ii)}$$

where h_1 denotes as the complex channel coefficient between the user and the BS. The Additive White Gaussian Noise (AWGN) at the receiver's is denoted as δ which is including inter-cell interference. The power density of AWGN noise δ represents as $\delta_{0,1}$. The decoding operation to the downlink system is in the order of the increasing channel gain which is normalized by the noise and inter-cell interference power that denotes as $[h_1]^2/\delta_{0,2}$. For transmitted data recovery case which is shown in Figure 3. At first CP removed processed bits are passed into FFT and then UE-data decodes UE-image and deletes its component by using SIC scheme from received signal y. UE-image decodes from received signal y directly without interference cancellation, because it has the first decoding order. After that, the decoded signal is passed to demodulation process before receiving the bits at the receiver. Finally, the received bits are allowed to bits to image conversion algorithm to convert transmitted bits received at the receiver into image. In this way we can transmit signal including distinct image without providing additional information regarding the signal.

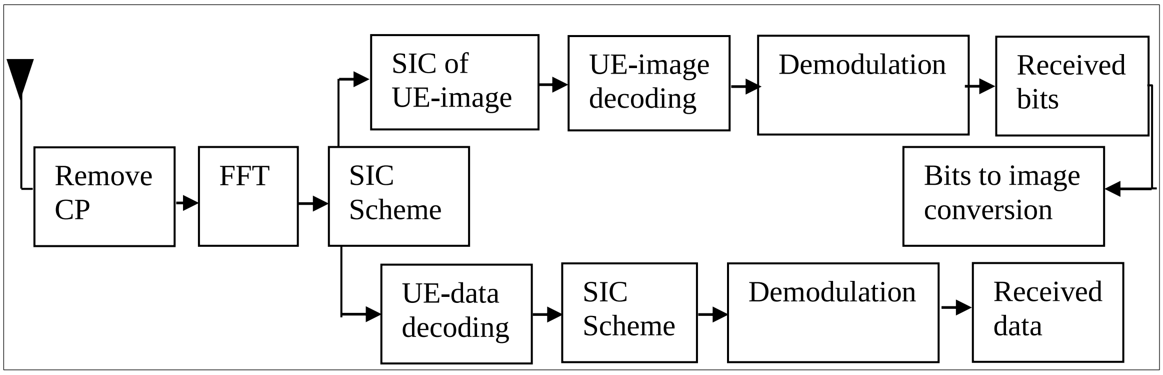

Figure 3 Block Diagram of Power Domain Based Receiver

6. System Model

The face recognition-based security model in wireless communication system shows in Figure 4. In this system, two different types of signal are used for transmitting as well as receiving between them one type is image that is used to recognize to user and other type is synthetic data that is represented as user's information. A user's grey image select from dataset of identical size (height: 112 pixels and width: 92 pixels) and synthetic message signal generate for that user. The pixel integer values of user's grey image are converted into 8 bits binary form which total bit number will be 112*92*8. On the contrary, the user's message signal receives directly as synthetic data (random binary bit which size is 112*92*8). The transmitted information of user's image and message signal are used the most common channel encoded system named convolutional scheme, interleaved and subsequently using the most familiar digital modulation technique like BPSK, 4-QAM, 8-QAM and 16-QAM [29] converted the message binary bits into digitally modulated complex symbols. The digital form of modulated symbols is allotted given power and then feed this power assigned signals into spatial multiplexing encoder section for multiplexing between two different signals and finally the generated signal transmitted from the appropriate transmitting allocated antenna. The original propagated signal which is transmitted from antenna is changed because of the wireless noisy channel. For this reason, AWGN wireless noisy channel are considered to adulterate the transmitted signal with noise. With the help of SIC technique, the ML decoding based QR channel decomposition system is used to separate the message signal bits and user's image from the noise adulterated signal. The retrieve signals are given into spatial multiplexing decoder for decoding the signals. After that the digital demodulation technique use to demodulate the signals, henceforward the two different schemes deinterleaved and channel decoded are used to original regain the transmitted binary bit stream. Finally, the received binary data of user's image descrambled and converted into pixel integers and filtered to recover the transmitted grey image as well as retrieve binary data of user's no need to convert because the transmitted was random binary data. Now the received grey image of user sends into face representation and feature extraction system which are face recognition part in our system to ensure the security. The extract features of given image are used to compare with image dataset. If the given image and any image of image dataset are matched then the system will show a message that the user is "found" otherwise show "not found". After seeing this message, we will confirm the user is authentic or not.

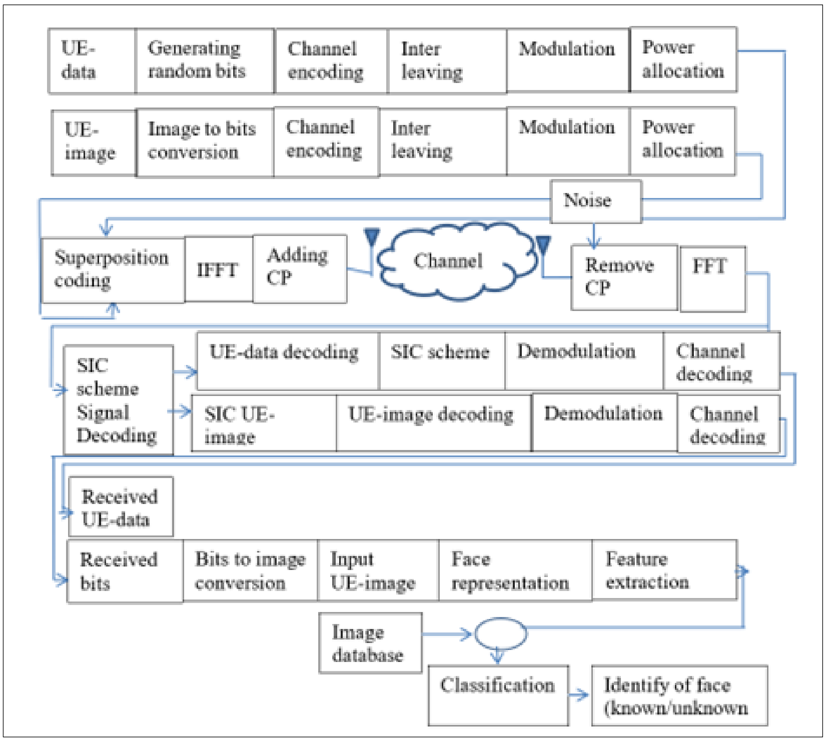

Figure 4 Block diagram of Face Recognition for Wireless Communication System

7. Result and Discussion

The system performance evaluation of multiuser with different data types downlink MIMO NOMA wireless communication is shown in this section. The simulation results have presented using MATLAB R2014a to clarify the significant change of various types of channel coding and digital modulation techniques on system performance in terms of bit error rate (BER). In the whole processing work, it is considered that at the receiver end the channel state information (CSI) of fading channel is available with unchanged fading. Which parameters are used in our system to evaluate the system performance is shown in Table 1.

Table 1 Summary of the simulated system parameters

Sl	Parameters	Types
1	Data type	Grey Image
2	Image Size	112 x 92 Pixels / (112 x 92 x 8 bits)
3	Binary bits	112 x 92 x 8
4	No. of user	1
5	Antenna configuration	2 x 2 MIMO Channel
6	Channel coding	½-rated Convolutional
7	Digital modulation	BPSK, QPSK, PSK, 4-QAM, and 16-QAM
8	Signal detection technique	ML decoding based QR channel factorization aided SIC scheme
9	SNR	0 to16 dB
10	Channel	AWGN
11	Noise Type	Gaussian

The figure 5 shows that the User's transmitted image is received at the receiver end using face recognition of user over AWGN channel with PSK modulation scheme. The original image is affected with small noise due to channel quality but it is almost clear to identify the User. After sending the received image into the above-mentioned face recognition system, it is seen that the recognition system identifies the user with comparing with dataset image and did not found any image after bits image conversion process.

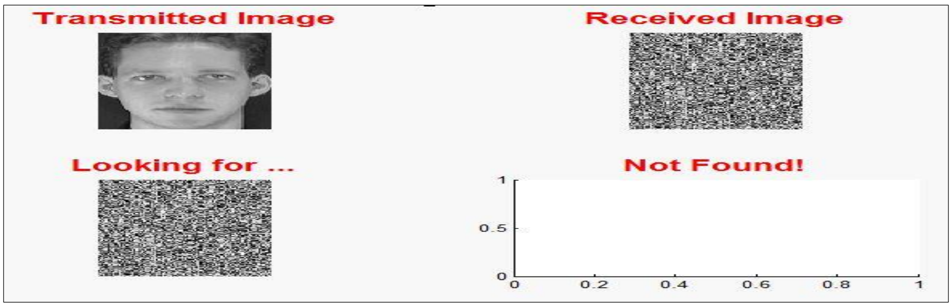

Figure 5 Face Recognition of User over AWGN channel with PSK modulation scheme

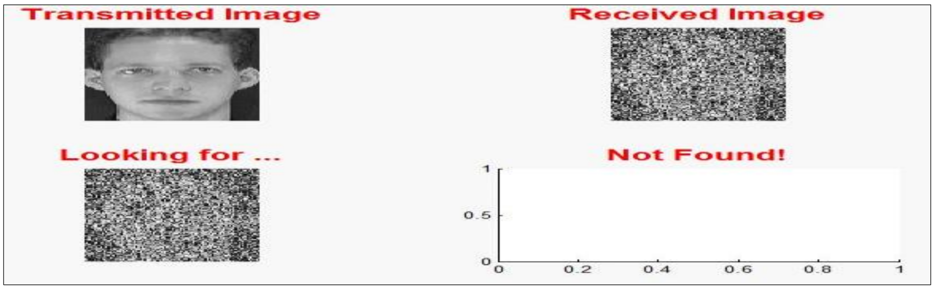

Figure 6 Face Recognition of User over AWGN channel with DPSK modulation scheme

After sending the received image into the face recognition system of User over AWGN channel with DPSK modulation scheme. It is seen that the recognition system identifies the User with comparing with dataset image. The synthetic binary data of User information received which is shown in figure 6 and did not found any image after bits image conversion technique as like as the above figure 5.

Face Recognition of User over AWGN channel with BPSK modulation scheme is depicted by figure 7 and found image after bits image conversion process.

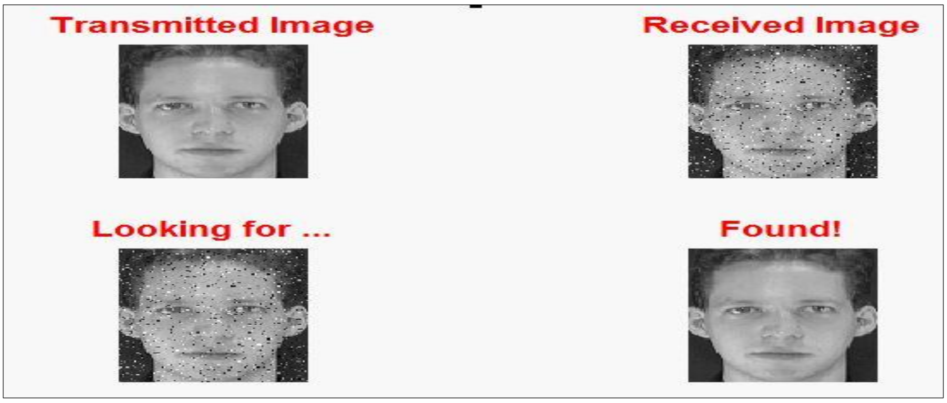

Figure 7 Face Recognition of User over AWGN channel with BPSK modulation scheme

Another face recognition of User over AWGN channel with 16-QAM modulation scheme is shown in below figure 8 and found image after bits image conversion technique.

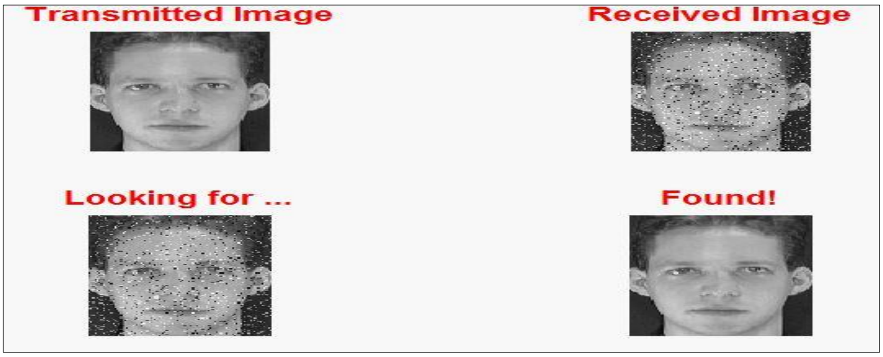

Figure 8 Face Recognition of User over AWGN channel with 16-QAM modulation scheme

Instead of 16-QAM modulation scheme, 4-QAM modulation scheme gives image after bits image conversion process. Face recognition of User over AWGN channel with 4-QAM modulation scheme is depicted in figure 9.

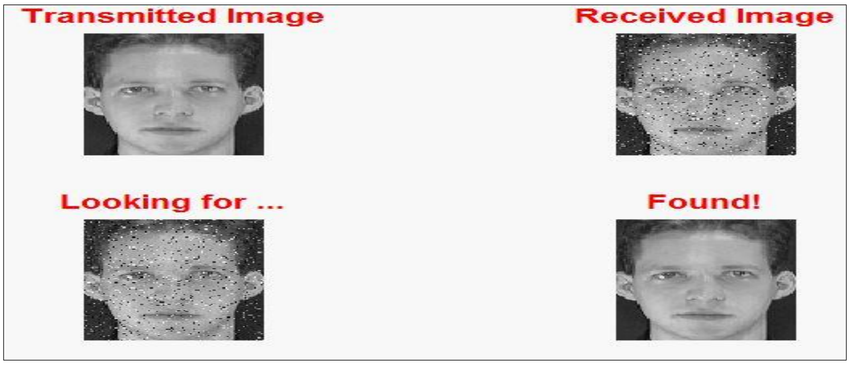

Figure 9 Face Recognition of User over AWGN channel with 4-QAM modulation scheme

It is seen from the figure 10 that the plot of BER values for user's digital data are almost constant in PSK, DPSK, 16-QAM modulation with convolutional channel. Under assumption of SNR value of 10 dB for the user, the estimated BER values are near 0.5026 for all modulation technique in convolutional channel coding schemes. On the other hand, in case of BPSK and 4-QAM modulation with convolutional coding the BER is 0.02 and 0.14 respectively considering 4dB SNR and for identical 10dB SNR value, the estimated BER value is also constant value with zero BER.

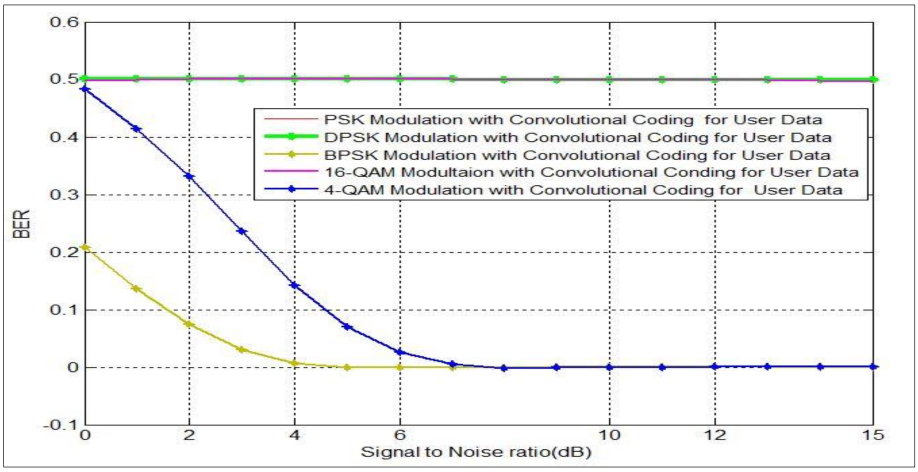

Figure 10 BER performance of User data transmission with BPSK, QPSK, PSK, 4-QAM and 16-QAM digital modulation scheme

8. Conclusion

In this paper, face recognition signal transfer technique with image is introduced for ensuring proper security system in wireless communication system instead of mixing additional information file regarding the transmitted signal. Considering the assumption of SNR value of 10 dB for the user, the estimated BER values are near 0.5026 for all modulation technique in convolutional channel coding schemes. On the other hand, in case of BPSK and 4-QAM modulation with convolutional coding the BER is 0.02 and 0.14 respectively considering 4dB SNR and for identical 10dB SNR value. BPSK shows constant zero BER under the assumption of SNR among all the techniques used in this study.

Compliance with ethical standards

Disclosure of conflict of interest

There is no conflict of interest in connection with this paper.

References

[1] F. Faisal and S. A. Hossain, "Smart security system using face recognition on raspberry Pi," 2019 13th Int. Conf. Software, Knowledge, Inf. Manag. Appl. Ski. 2019, no. August, 2019.

[2] Michel Owayjan, Amer Dergham, Gerges Haber, Nidal Fakih, Ahmad Hamoush, Elie Abdo, "Real-time Face Recognition Under Different Environment," International Joint Conferences on Computer, Information, and Systems Sciences, and Engineering, University of Bridgeport, December 2013.

[3] R. Singh, M. Singh, and L. Ragha, "Real-time Face Recognition Under Different Environment," SSRN Electron. J., 2019.

[4] Soe Sandar | Saw Aung Nyein Oo, "Development of a Secured Door Lock System Based on Face Recognition using Raspberry Pi and GSM Module," Int. J. Trend Sci. Res. Dev., vol. 3, no. 5, pp. 357–361, 2019.

[5] Find Biometrics, Faceial recognition, [Online], Available at: http://findbiometrics.com/solutions/ facial-recognition/.

[6] A. S. Tolba, A.H. El-Baz, and A.A. El-Harby, "Face Recognition: A Literature Review", International Journal of Signal Processing Volume 2 Number 2, January 2005.

[7] Parusheva, S..," A comparative study on the application of biometric technologies for authentication in online banking", Egyptian Computer Science Journal, 39(4), 115126, 2015.

[8] Joseph Lewis, "Biometric for secure Identity Verification: Trends and developments", University of Maryland, Bowie State University, January 2002.

[9] Buciu, I., &Gacsadi, A.,"Biometrics systems and technologies: a survey", International Journal of Computers Communications & Control, 11(3), 315-330,2016.

[10] Alzubaidi, A., &Kalita, J.," Authentication of smartphone users using behavioral biometrics", IEEE Communications Surveys & Tutorials, 18(3), 1998-2026, 2016.

[11] Sana Ghafoor, Khan Bahadar Khan, Muhammad Rizwan Tahir, and Maryoum Mustafa, "Home Automation Security System Based on Face Detection and Recognition Using IoT", Springer Nature Singapore Pte Ltd. 2020 I. S. Bajwa et al. (Eds.): INTAP 2019, CCIS 1198, pp. 67–78, 2020.

[12] Samridhi Dev, Tushar Patnaik, "Student Attendance System using Face Recognition", roceedings of the International Conference on Smart Electronics and Communication (ICOSEC 2020) IEEE Xplore Part Number: CFP20V90-ART; ISBN: 978-1-7281-5461-9.

[13] Prashanth Balraj Balla, Prof.K.T.Jadhao, "IoT Based Facial Recognition Security System", 2018 International Conference on Smart City and Emerging Technology (ICSCET), DOI: 10.1109/ICSCET.2018.8537344, November 2018.

[14] Hassan Soliman, "Face Recognition in Mobile Devices", International Journal of Computer Applications (IJCA), pp.13-20, jul.2013.

[15] Aesha shan, kavin shav,"Bult-in Face Recognition on Smart Phone Devices", International Journal of Engineering and Technology (IRJET), Vol.4, pp.1472-1474, Jan.2017.

[16] Dandashi, Amal and Walid Karam, "Biometrics security and experiments on face recognition algorithms", Computational Intelligence for Security and Defence Applications (CISDA), 2012 IEEE Symposium on. IEEE, 2012.

[17] Peter, K.J.,Nagarajan, G.,Glory,G.,Devi, V.V.S., Arguman, S.,&Kannan, K. S., "Improving ATM security via face recognition", In Electronics Computer Technology (ICECT), 2011 3rd International Conference on (Vol.6, pp.373-376).IEEE.

[18] Holat, Recep, and Selman Kulac, "ID identification by using face detection and recognition systems", Signal Processing and Communication Applications Conference (SIU), 2014 22nd. IEEE,2014.

[19] Nakano, Miyoko, F. Yasukata, and Minoru Fukumi, "Marketing data collection from face images using neural networks", Nonlinear Signal and Image Processing, 2005. NSIP 2005. Abstracts.IEEE-Eurasip. IEEE, 2005.

[20] Kresimir Delac, Mislav Grgic,"Asurvey of biometric recognition methods", 2004.

[21] sulochana sonkamble, 2dr.ravindra thool, 3balwant sonkamble, "Survey of biometric recognition systems and their Applications", Journal of theoretical and Applied Information Technology, 2010.

[22] Anil K.Jain, Ajay 2010 Kumar, "Biometrics of Next Generation:An Overview". Gizem, Aksahya & Ayese, Ozcan (2009) Coomunications & Networks, Network Books, ABC Publishers.

[23] Ramandeep Kaur, Er. Himanshi, "Face Recognition Using Principal Component Analysis", 2015 IEEE International Advance Computing Conference (IACC), DOI: 10.1109/IADCC.2015.7154774, July 2015.

[24] Aisha Bazama , Fawzia Mansur* , Nura Alsharef, "Security System by Face Recognition", Bazamaet al. Alq J Med App Sci. 2021;4(2):58-67, June 2021.

[25] W. Zhao, R. Chellappa, P. J. Phillips, and A. Rosenfeld, "Face recognition: A literature survey" ACM Computing Surveys (CSUR), 35(4):399{458, 2003.

[26] J. Nagi, "Design of an Efficient High-speed Face Recognition System", Department of Electrical and Electronics Engineering, College of Engineering, Universiti Tenaga Nasional, March 2007.

[27] Nisha Soni, Mahendra Kumar, and Garima Mathur, "Face Recognition using SOM Neural Network with Different Facial Feature Extraction Techniques", International Journal of Computer Applications (0975 – 8887) Volume 76– No.3, August 2013.

[28] Joana Angjo, Mehmet Basaran, Lutfiye Durak Ata, "On the Channel Estimation Performance of NOMA Systems: Experimental Implementation of Real-Time Downlink NOMA-OFDM", IEEE International Black Sea Conference on Communications and Networking, DOI: 10.1109/BlackSeaCom48709.2020.9234965, May 2020.

[29] Pavan Kumar, Amita Kumari, "BER Analysis of BPSK, QPSK, 16-QAM & 64-QAM Based OFDM System over Rayleigh Fading Channel", OSR Journal of Electronics and Communication Engineering (IOSR-JECE), p- ISSN: 2278-8735.Volume 11, Issue 4, Ver. III, Jul -Aug 2016.