

Study of Face Detection for Wireless Secure Data Transmission

Sudhir C.tembhare, Ketan B.Suley

Abstract—Security of data is main goal for to days communication purposes. This paper presents an idea about an efficient system that provides a sound security for data transfer from one user to another user in an efficient way using Radio Frequency Identification Technology along with Face Detection technique. This two way security approach will guarantee both the parties which are sender and receiver about their confidential data while maintaining a flexible communication approach.

Keywords—Sender, Receiver, Face Detection, Radio Frequency Identification, Wireless Communication,.

1 INTRODUCTION

The security of data while transmission is very essential. There are Two Way Security System which is being proposed, which comprises of wireless data transmission and face detection, to enhanced the security of the system. The risks are associated with wireless data transmission due to the unauthorized access. This security system can be used at places where the data is highly confidential. This paper relates to the security of data communication in wireless system and particularly to a system where encryption key is used by a transmitter and receiver to provide a secure system. Data transmission is done using the technology called as RFID. RFID is used for identification of the automated objects and other creatures by using the short range radio technology for the communication of digital data in between a non-movable location and a movable creature. RFID has come up with various applications along with numerous risks. Now a days the RFID technology systems are seen almost everywhere for example product tracking, inventory control, access control etc. A wireless network is vulnerable to all exploits targeted at wired networks with a weakness of their own that makes them to susceptible to many other attack. Breaking into a network which is wireless requires no physical break since you are broadcasting from a signal your network is simply up for grasp, waiting for anyone to cash on and the other part of vulnerability is at receiver end if an unauthorized person gets access of your information it may be at risk. Data is transmitted through wireless technology which ensures improved convenience and efficiently which leads to fastly growth in the segment of communication industry. The person who is good in hacking even though your receiver is protected with password or with security code but what if your receiver side is protected by a biometric system retina recognition finger prints recognition or face recognition keeping in mind the high level of security of data and to provide secure transmission. Here we used RFID technique to communicate. Here the data is 12 bit password which is protected. RFID technology is being used for data transmission which involves Radio Frequency Transmitter and Radio Frequency Receiver. Facial Recognition System is an useful application basically which has been used for the verification & identification of a person implicitly from an

video frame or an image. The face detection technology has some of the algorithms which help in identifying the facial features, i.e. by extracting the features from an appropriate image of a particular face. Once the data is transmitted and send to the receiver, the receiver cannot retrieve the information till the time face recognition is approved. The process of Face recognition thus gives the full proof security. Usage of MATLAB will be there be for the face detection technique. The algorithms had been developed through sophisticated mathematical computing matching process for the recognition of the face of any individual. The algorithms thus play a very important role in the case of face detection using MATLAB technique. The communication that involves internet or any external network needs security. In the case of virtual attacks the data encryption provide us security data encryption will help to save and protect any important data, whether it is stored on a laptop or desktop, computer, removable storage media, a PDA an email server or corporate network, moreover it will make it possible to securely access your files from any place –at the work place or at residence or while travelling on road in case if the device is stolen or lost, the data will any way be impossible to read as it is encoded by the mechanism of the data encryption it is no matter how many security measures you have applied to protect your network. They all are inefficient until your important data will not be protected itself. This means that only an authorized receiver can read the information (the receiver must have the appropriate decryption key). Therefore the variable key is quiet important. The proposed two way enhanced secure data transmission may necessarily use for commercial organizations. If company losses all important information for no matter what the reason is ,the consequences may be unpredictable and even degrade the whole business. It is important to understand that any data is vulnerable and may be compromised in two ways.

2 LITERATURE REVIEW

The 802.11 standard for wireless networks includes a Wired Equivalent Privacy (WEP) protocol, used to protect link-layer communications from eavesdropping and other attacks. We have discovered several serious security flaws in the protocol,

stemming from misapplication of cryptographic primitives. The flaws lead to a number of practical attacks that demonstrate that WEP fails to achieve its security goals. In recent years, the proliferation of laptop computers and PDA'S caused an increase in the range of places people perform computing. At the same time, network connectivity is becoming an increasingly integral part of computing environments. As a result, wireless networks of various kinds have gained much popularity. But with the added convenience of wireless access come new problems, not the least of which are heightened security concerns. When transmissions are broadcast over radio waves, interception and masquerading becomes trivial to anyone with a radio, and so there is a need to employ additional mechanisms to protect the communications.

3 PROPOSED SYSTEM

Encryption and decryption are done using a variable called key. A key is long sequence of bits used in cryptography algorithms. During encryption the algorithm changes the original data based on the key's bits to create a new encrypted message and when the data reaches to its destination, the same symmetric or asymmetric key is used to decode the encrypted message turn into its original form. With the help of RF technology wireless communication is added with 12 bit password protected data transmission. The data is reached to the receiver whose address is matched by the transmitter address. In

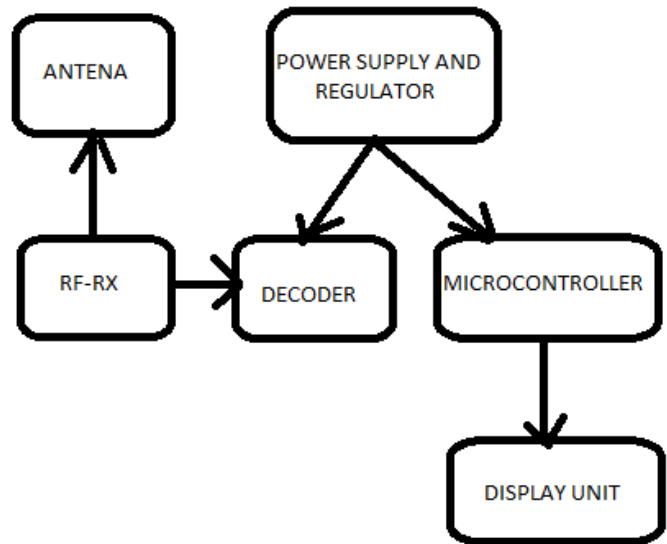


Fig2- Figure For Reciever

the system provides full security and along with this now the face detection technique is being merged which ensures ththe data is not received until and unless the face detection is done successfully. At the receiver side the data is not retrieved even if the password is matched until the face detection is done. If the image is matched with the previously defined data base the detection is valid & justified which further allows displaying the information.

4 IN WIRELESS SECURE DATA TRANSMISSION

This paper gives information about the security of data communication in a wireless system and particularly to a system where encryption key used by a transmitter and receiver may be reprogrammed explicitly in order to provide a secured and a full proof system. Data is transmitted through wireless technology which ensures exact and improved efficiency which leads to large growth in the segment of communication industry. RFID technology is being used for data transmission which involves Radio Frequency Transmitter and Radio Frequency Receiver. RFID does not have more range as compared to a centrally located trans receiver, and therefore it is less prone to hacking from any illegal source. The transmitter sends the encoded signals and the receiver receives the signals which has been encoded. In the transmitter a unique code is created that is used to detect the RF signal. The identification code is the 12 bit password. In order to convert the data into an encrypted data that is to be transmitted over RF channels, encoder is being used. Encoder thus translates the RF data that is entered from the keypad. This encrypted data is converted in the form of RF frequency. Power supply is to be provided in order to drive the transmitter and encoder. RF receiver decodes the data and displays it on the desktop.

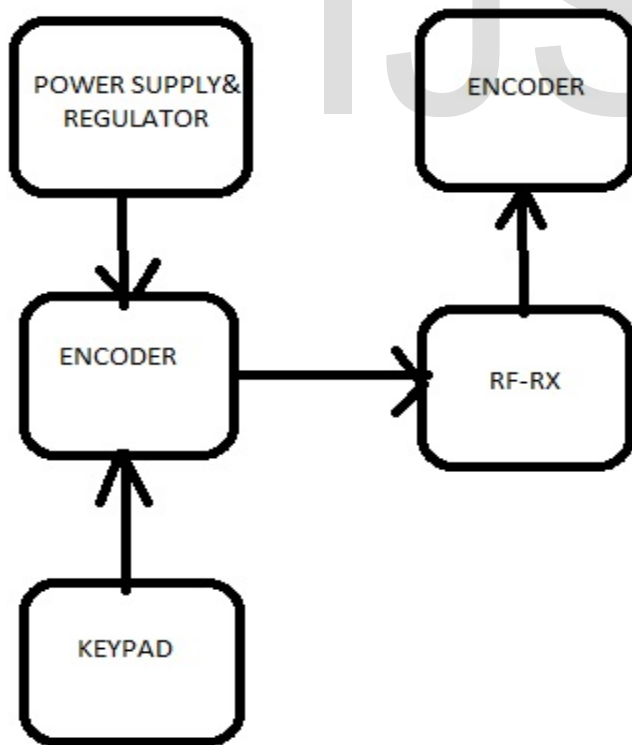


Fig1- Figure For Sender

case the user wants to display the same message on both receiver then the same address can be set for each receiver. Thus

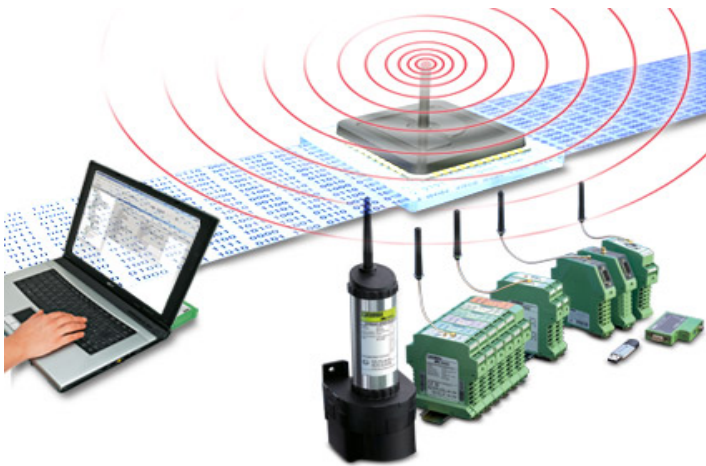


Fig3- Wireless Transmission

At the receiving side decoder is used to decrypt the data and then provided it to the microcontroller. This technique of wireless data transmission system is conveniently useful in every way. And for better security as per keeping the transmission safe from intrusion we are using the technique of RFID.

5 TECHNIQUE OF FACE DETECTION

The Facial Recognition System is application typically used for the identification and verification of a person automatically from an image or a video frames. The face detection technique uses some of algorithms which helpfull in identifying the facial features i.e. by extracting the features from an appropriate image of a specific face. Once the data is transmitted and send to the receiver, the receiver cannot retrieve the information till the time face recognition is justified. The process of Face recognition thus gives total security. The face recognition stage typically uses an intensity representation of the image by the 2D-DCT. This system serves for the crime detecting purpose because the pre-recorded images can be afterward used for the identification of a person. The face recognition process includes some important steps to be followed up:

5.1 Detection Method: The computer by itself decides which portion of the pixel to be taken and others to discard.

5.2 Normalization: This means that the image must be accepted in terms of dimensions, posture, etc related to the images in the reference database.

5.3 Face extraction and recognition: In feature extraction, a mathematical representation called a biometric template is to

be generated, which is stored in the database and forms the basis of any recognition step.

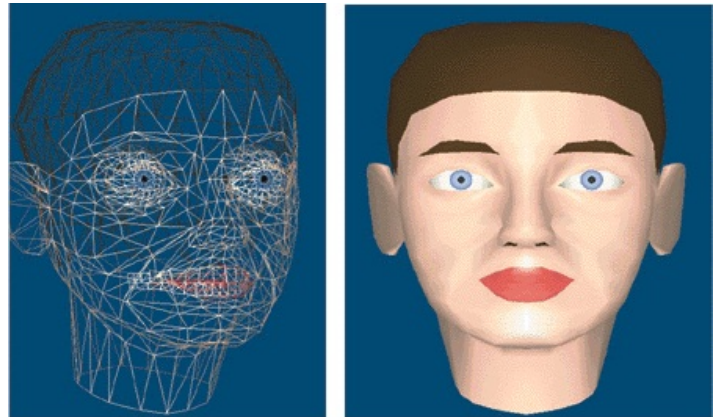


Fig 4- Face Recognition Technique

MATLAB will be used for the face detection technique. The algorithms had been developed through sophisticated mathematical computing matching process for the recognition of the face of any person. The algorithms thus play a very important role in the case of face detection using MATLAB technique. The communication that involves internet or any external network needs security. Encryption of any algorithm has many purposes like:

- 1-Security and Proprietary
- 2-Integrity
- 3-Legal Activities.

We even have different kind of algorithms which can be used in the face recognition process, for e.g. Symmetric Algorithms, Asymmetric Algorithms, Hash Algorithms, etc. The face recognition algorithm are highly depend on the detection of the facial features but in the different approach that is being used here, face is treated as a general pattern and is recognized by its photometric characteristics. To implement this approach algorithms are to be implemented.

PRINCIPLE COMPONENT ANALYSIS (PCA):

The PCA technique converts each 2D image into a 1D vector. This vector is then decomposed into geometric principal component in other words, the technique selects the feature of the image (or face) which vary most from the rest of the image.

LINEAR DISCRIMINATE ALGORITHM (LDA):

LDA is a statistical approach based on the same statistical principals as PCA. LDA classifies faces of unknown individuals based on a set of training images of known individuals. The technique finds the underlying vectors in the facial feature that would maximize the variance between individuals and minimize the variance within a number of samples of the same person.



Fig5: Figure for Procedure

6 APPLICATION

EFFECTIVE TRANSMISSION: The system which includes the FRS can well provide the purposes for law enforcement, national defense and handle terrorism. The system can be used for authentication and verification purposes including the entry and exits of security areas. There can be wide use of the system from highly prohibited areas to your own PC's. The proposed two things enhanced secure data transmission may necessarily use for commercial firms.

SAVE VALUABLE DATA AT ANY COST: Situation such as virtual attacks the data encryption provide security data encryption it will help to save and protect any precious data, whether it is stored on a laptop or desktop, computer, removable storage media, email server, moreover it will make it possible to securely access your files from any place at the office at home or on the street in case if the device is stolen or lost. This means that only an legal receiver can read the information or data therefore the variable key is very important.

7 CONCLUSION

Thus wireless data transmission by using RFID technology along with face detection in MATLAB. By combining the two systems it will be beneficial to obtain good security in any geographical area and location. The valuable data when send across the network will be secured by the use of radio frequency security mechanism and can only be access at the other end by using face detection method. As the system have pre-recorded images to scan from the given database the probability of error is minimize to a large extent thus giving us value of security and protection.

REFERENCES

- [1] A. Abdallah, M. Abou EI-Nasr, and A.Lynn Abbott, "A New Face Detection Technique using 2D-DCT and self organizing Feature Map" vol. 21, May 2007, pp. 15-19.
- [2] Anil K. Jain and Stan Z. Li, "Handbook of Face Recognition", Springer, 2nd edition.
- [3] SamerAbdo, Rolf Ambuehl, and Olivier Bodenmann, "Wireless Secure Device ", Retrieved May 29, 2007.
- [4] Louis A. Stilp "RFID Based Security Network", Retrived March 28, 2012.
- [5] Dan Linh Nguyen, "Security Between client and server in a computer network", Retrieved December 31, 2012.
- [6] Phillip Dunkelberger, "The Future Of Encryption", Retrieved November 12, 2011.
- [7] Helen Fouche Gaines, "Cryptanalysis", 1939, Dover ISBN 0-486-200973.
- [8] Dr. DuanHaselman and Bruce R. Littlefield, "MasteringMatlab 2012 Edition", Retrieved 3 June, 2012.
- [9] Francis C. Marino, Dixc Hills, and Thomas P. Schmit, Huntington, "Secure Communication in a Wireless System", Retrieved February 15, 2012.