Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 5, May 2015, pg.416 – 423

RESEARCH ARTICLE

Image Encryption Based Approach to Address Privacy and Security Issues in RFID Tags

S.N.Bharath[1,2], Rakshith.K.M[2], Raghavendra U.Karunakar[2], Rajendra Nayak[2], Deepashri. P[2]

Government Research Center, Sahyadri College of Engineering & Management[1]

Department of Computer Applications, Sahyadri College of Engineering & Management[2]

Mangalore – 575007

{kmrakshith12, ragstavor, rajunfsmw, deepashri2014}@gmail.com

Abstract:

Due to the exponential growth in the World Wide Web and digital media, providing the security for the data has become one of the crucial issue. This situation has made researchers to look towards developing data encryption algorithms for addressing privacy and security issues in RFID. In this article, a simple and effective data encryption model for biometric data of RFID tags are addressed. The novel proposed model is composed of two stages like data encryption and data matching. Proposed data encryption approach is critically analyzed by conducting huge set of experiments on the publicly available face and palm corpuses. A data matching technique for the proposed encryption algorithm is also designed. The result of the experiments reveals that the proposed encryption algorithm outperforms for two types of the biometric data.

Keywords: Image Encryption, Encrypted Pattern Matching, RFID Tags.

I. Introduction

A secure computing environment would not be complete without the consideration of encryption technology. The term encryption refers to the practice of hiding the meaning of a piece of information by encoding it in such a way that it can only be decoded, read and understood by people for whom the information is intended.

The exponential growth in the networking technology results with a common culture of interchanging of the data and information. Sensitive information like passports, credit cards, banking transactions and ATM pin numbers needs to be protected from the hackers. One of the solutions for this kind of problem is data encryption based techniques. Encryption is a very common yet effective tool for promoting the information security. The evolution of encryption is moving towards a future with endless possibilities. Everyday new methods of encryption techniques are discovered for addressing the data security issues.

In this paper, a novel data encryption technique for attending data security problem is proposed. It is a general tendency and also from the strong literature survey we came to a conclusion that, biometric traits like face and palm is one of the unique feature in human beings. Based on this assumption, a novel image encryption algorithm is presented in this paper. Based on the proposed encryption technique, a matching algorithm is also designed.

The rest of the paper is organized as follows. In section 2 a brief literature survey on different image encryption algorithms is presented. In section 3 we present the proposed model for the data encryption based approach for security systems. Section 4 discusses about experimentation and comparative analysis performed on the proposed models. Paper will be concluded in section 5.

II. Literature Survey

Encryption can be defined as the conversion of the data into a form another form where that cannot be understood by any people without decrypting the encrypted data. Decryption is the reverse process of encryption. In this section, we are discussing some of the existing data encryption techniques.

Dahua Xie and Jay Kuo have proposed an encryption technique with enhanced Multiple Huffman Table (MHT) by key hopping method. The previously developed Multiple Huffman Table (MHT) has good desirable properties but it was highly vulnerable to the chosen plaintext attack (CPA). Whereas this enhanced MHT encryption method faces all such limitations. As the result shown, that the algorithm is secure for the chosen plaintext attack and proved mathematically by the key hopping method.[1]

Suhaila O. Sharif, L.I. Kuncheva, S.P. Mansoor has jointly framed a manuscript for Classifying the Encryption Algorithms in accordance with the Pattern Recognition method [2]. In this article the authors focuses on the limitations of the algorithms which are used for encryption scheme and for generating the keys for encryption process. Here the pattern recognition method to identify the block ciphers in encryption process. The block cipher algorithms like AES, DES, IDEA, and RC were used to identify the good classification technique. As the result shown, that the performance of RoFo (Rotation Forest) classifier has the very good classification accuracy.

A Study on OMAP (Open Multimedia Applications Platform) Digital Fingerprint Encryption technique is proposed by Zhu Yuxi in [3]. In this study the author deals with the identification of the fingerprint and the security in transmission for the embedded systems. Here a digital fingerprint technique was used with the structure of the OMAP (Open Multimedia Applications Platform). The author designed an integrated software structure with an application platform.

Huang Jinga,b Zheng Zhen-zhuc has developed an optical encryption technique for secure real time image transmission [4]. The proposed technique is based on the fact that an image can hold a huge amount of data or information, which results in very less efficiency of the real time image encryption. The authors has proposed a new scheme for image encryption which is used in optical computing technologies that apparently focuses on images and large amounts of data simultaneously, as the result of this high speed is attained. Hence this scheme was implemented by using a stream cipher on the polarization encoder as the optical logic gates. The result of the proposed approach states that, the algorithm provides a good security for the images with histogram.

Mort Naraghi-Pour et al [5] have developed a simple encryption standard for secure detection in the wireless sensor networks. Only the authorized user or the ally fusion center (AFC) is aware of the encryption method its features, and no unauthorized or any third party fusion centers (TPFC) are not aware of such encryption features. As the result shown, the exact threshold value was found and the numerical results were evaluated for the error probabilities of the two fusion centers (AFC and TPFC).

Osamu Watanabe et al [6] have developed a scalable encryption method which comprises of backward compatibility with the JPEG2000 Images. This encryption technique tells the encrypted images to hold the multilevel encryption method also decreases the computational complexity of the encryption process. In this paper the standard JPEG 2000 decoder is used to decode the encrypted images and some parameters of JPEG 2000 were saved after the encryption process. As the result of this, the duration of the encryption process is controlled by selective encryption algorithms to promote faster processing.

Analysis on encryption techniques with JPEG Images was proposed by W. Puech, and J.M. Rodrigues [7]. This paper mainly focuses on the draw backs of both the selective encryption (SE) and the image compression. The SE (selective encryption) can be made by Advanced Encryption Standard (AES) algorithm incorporate with the Cipher Feedback (CFB) mode. And for the compression, the JPEG algorithm has been used. Here the SE was done in the stage of Huffman coding in JPEG algorithm which does not affects the size of the compressed image. The results shows the application of SE in JPEG compressed images.

Mahmood Al-khassaweneh and Selin Aviyente [8] has put forth a novel image encryption technique based on the concept of Least Square Approximation (LSA) .In this paper, the conversion of the original image into the form of encrypted one by the randomly generating vectors. And on the other hand the original image has been decrypted by using the least square approximation concept on the encrypted image and also on the randomly generating vectors. As the result of this, there is a good range of efficiency in this algorithm and also promotes good enhancement in the security aspects.

Syed Ali Naqi Gilani, M. Ajmal Bangash [9] has developed an enhanced block based image encryption Scheme with Confusion. The authors designed the Block-Based Image Encryption Algorithm (BBIE) which works together with the Blowfish Encryption algorithm. Here the digital image is decomposed into slices, after those two continuous actions that are rotating each 3D true color image slice to 90° which is then follow up by flipping row wise down were done. Also the rendered blocks were then undergo the process of scrambling into the form of converted confused image which is finally follow up by the Blowfish cryptosystem which is actually the process of encryption of the image using a secret key. The result shown that, the correlation between adjacent pixels has been reduced in the entire color component.

A real time personal identification based on Fourier transform for palm-print recognition is proposed in [10]. An auto hand gesture segmentation method is proposed first and after the segmentation, a modified Fourier transform are used for the image processing. Machine leaning based trainings are used to get the palm print training database. A spectral feature extraction algorithm is proposed for palm-print recognition, which can efficiently capture the detail spatial variations in a palm-print image in [11]. The entire image is segmented into several narrow-width bands and the task of feature extraction is carried out in each band using two dimensional Fourier transform. It was shown that the proposed dominant spectral feature selection algorithm is capable of capturing the variation within the palm image, but also a very high within-class compactness and between class separability.

III. Proposed Model

In this paper we propose a novel technique for data encryption based approach for security system. The overall theme of this article is developing an effective and efficient algorithm for providing the security to the system. For providing a good amount security to the system, we are considering encryption level matching of the input data. Our proposed model can be categorized into two stages, such as data encryption stage and the matching of the encrypted data.

Data Encryption: Since our primary objective is to provide the security to the system, we are considering the biometric data i.e., face and knuckle for data encryption. When these datas are captured using appropriate biometric data acquisition devices, they are subjected for pre-processing algorithms. Once the data is prepossessed, the RGB biometric data are converted into binary data. Once, the input data is converted to binary i.e., combination of 0’s and 1’s are given as input to run length encoding algorithm. Run Length Encoding (RLE) is a simple and effective algorithm for encoding the data. RLE accept the binary data and generate the corresponding encoded output.

Matching Stage: Once the input data is generated, they are preserved in the knowledge base for further processing. The next stage of the algorithm is to match these data at encoded level. Proposed model is algorithmically presented in the following algorithmic model.

Algorithmic Model

```
Algorithm: Data Encryption based approach for Security Systems.
Start:
        Idata : Input collection of Training Data.
        IPreProcess : Pre processing (Idata).
        Ibinary : Binary (IPreProcess)
        Iencoded : RLEncoding (Ibinary )
        KB : Iencode
        ITesting Data : Input collection of Testing Data.
        IPreProcess Testing Data : Pre processing (ITesting Data).
        ITest binary : Binary (IPreProcess Testing Data).
        ITest encoded : RLEncoding (ITest binary ). for i = 1 : Num Classes
        Result (ITesting Data) : Matching (ITest encoded ,KB (i Class))
end
```

Algorithm Ends

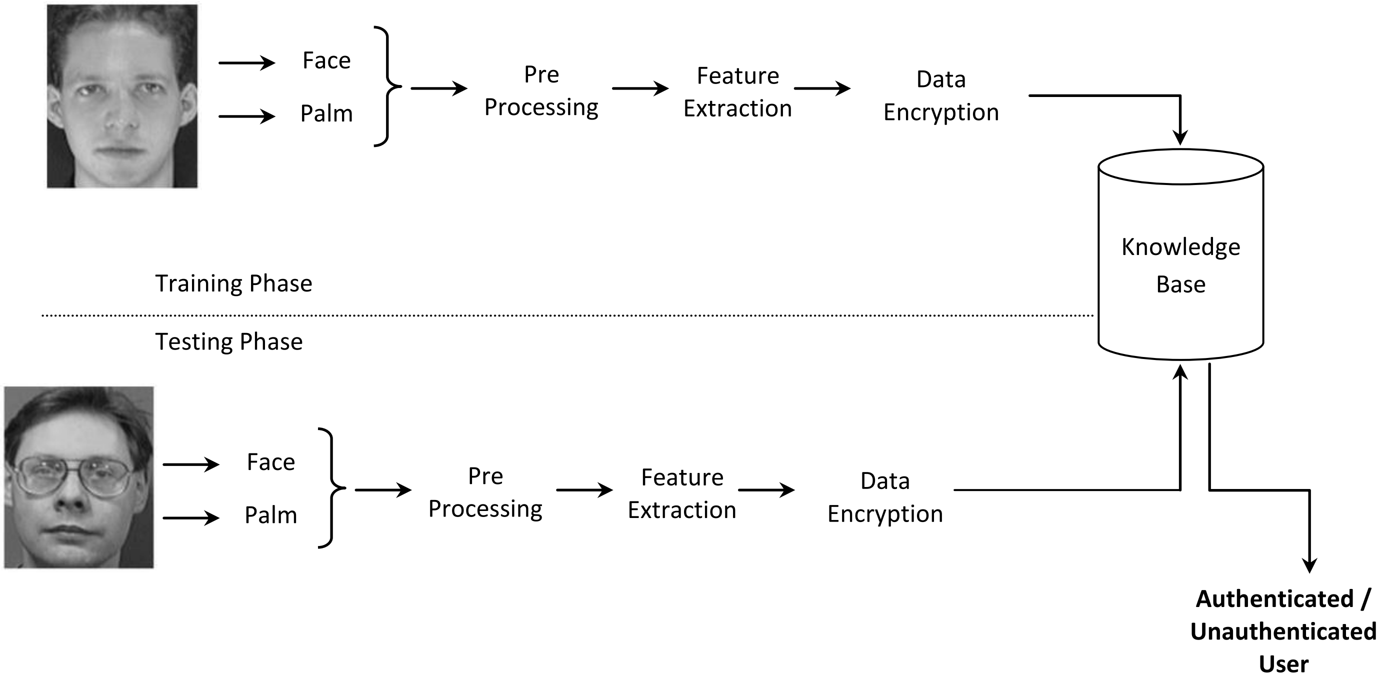


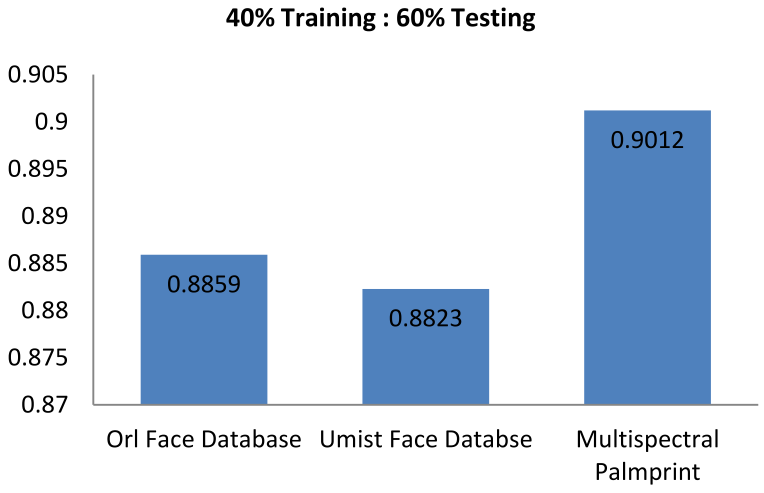
Figure 1: Block Diagram of the Proposed Approach.

In real time RFID system all these techniques can be adopted to address privacy and security issues. Since the biometric traits are preserved in encrypted format, it is very difficult for an unauthorized user to extract the information of any user data from the RFID systems. In any real time RFID application, two different traits are considered during the training stage. Once the features are extracted from the biometric traits they are subjected to data encryption and then they are preserved in knowledge base for further process. During testing stage, the same process is followed and data matching will be done at data encryption level only. Hence the processed model addresses the privacy and security issues in RFID tags.

IV. Experimental Setup

In this section, we present the details of the experiments conducted to represent the effectiveness of the proposed method on two category of biometrics viz face and palm print. The behavior of the proposed algorithm is critically analyzed on ORL face dataset, Umist face dataset and palm print database. ORL face data is a publicly available dataset consists of 400 samples from 40 different classes. Umist data is also a publicly available face dataset which consists of 1012 samples from 20 different classes and Multispectral Palm print database for palm prints.

We have conducted two sets of experiments; where each set contain three different trails. In first set of experiments, we have used 40% of the database for training and remaining 60 % is used for testing. In second set of experiments, we have used 60 % training and 40 % for testing. In each trail we have randomly selected training and testing samples. For the purpose of evaluation of the results, we have calculated precision, recall and f-measure for each trail. The details of the experiments are shown in the following graphs.



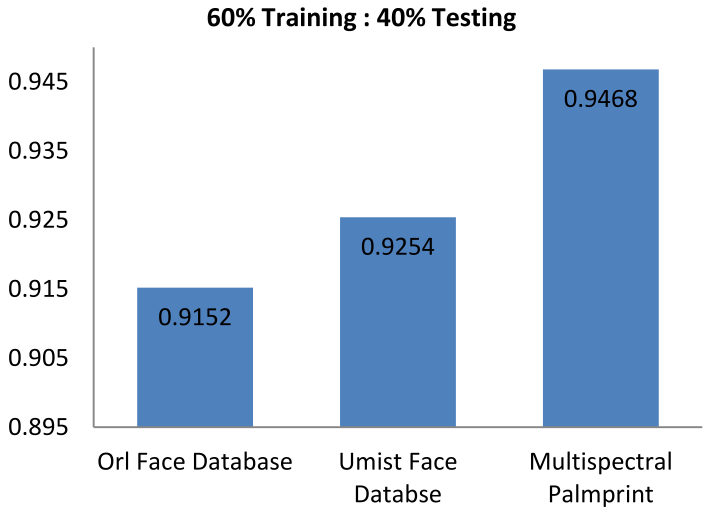


Figure : F- Measure of the results of proposed model.

V. Conclusion

A method of matching the biometric data at encrypted level for providing security for the system presented is this paper. The proposed algorithm consists of two stages like data encryption and matching of encrypted data. The algorithm is critically analyzed on two biometric data viz face and palm biometric traits. The robustness of the proposed algorithm is empirically tested by conduction of series of experiments. The results of the experiments reveals that, the novel approach perform well for providing security using biometric data. Though, the proposed approach appears to be simple, has lots of future avenues. In future, one can think of extending the same approach for different kind of biometric data.

VI. Acknowledgements

All the authors of this article acknowledge the financial support rendered by Sahyadri College of Engineering & Management, Mangalore and department of computer application under SPSS scheme.

References

1. Dahua Xie and C.-C. Jay Kuo, "Enhanced multiple Huffman table (mht) encryption scheme using key hopping" *IEEE Transactions* pp. 568-571,2004
2. Suhaila O. Sharif, L.I. Kuncheva, S.P. Mansoor ,"Classifying Encryption Algorithms Using Pattern Recognition Techniques" *IEEE Transactions* pp. 1168-1172,2010
3. Zhu Yuxi, Ruchun Cui, "*Applied Study Based on OMAP Digital Fingerprint Encryption Method*" *IEEE Transactions* pp. 1168-1172,2010
4. Huang, Jing, Zheng Zhen-zhuc, "A Method for Secure Real-Time Image Transmission Based on Optical Encryption" *International conference on the Intelligent Signal Processing and Communication Systems*, 2010

5. Mort Naraghi-Pour, Venkata Sriram Siddhardh Nadendla,” Secure Detection in Wireless Sensor Networks Using a Simple Encryption Method” *IEEE Transactions*, 2011
6. Osamu Watanabe, Akiko Nakazaki And Hitoshi Kiya,” A Scalable Encryption Method allowing Backward Compatibility with JPEG2000 Images” *IEEE Transactions* pp. 6324-6347,2005.
7. W. Puech, J.M. Rodrigues,” Analysis and Cryptanalysis of a Selective Encryption Method for JPEG Images” *IEEE Transactions on Image Analysis for Multimedia Interactive Services,*2007.
8. Mahmood Al-khassaweneh, Selin Aviyente,”Image Encryption Scheme Based on Using Least Square Approximation Techniques” *IEEE Transactions*, pp.108-111, 2008.
9. Syed Ali Naqi Gilani , M. Ajmal Bangash, “Enhanced Block Based Color Image Encryption Technique with Confusion” *IEEE Transactions* pp. 200-206,2008.
10. Shunyu Yang, “A real time personal identification based on Fourier transform of palmprint recognition”, Second International Conference on Innovations in Bio-inspired Computing and Applications, pp: 336-339, 2011.
11. Hafiz Imtiaz and Shaikh Anowarul Fattah, “A Spectral Domain Feature Extraction Scheme for Palm-print Recognition”, International Conference on Wireless Communications and Signal Processing (WCSP), Page(s): 1 – 4, 2010.q