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. 3, March 2015, pg.765 – 771

RESEARCH ARTICLE

Multimodal Biometric Approaches to Handle Privacy and Security Issues in Radio Frequency Identification Technology

[1]J V Gorabal, [2]Manjaiah D H

Department of Computer Science and Engineering, Sahyadri College of Engineering and Management, Adyar Mangalore Karnataka, India

Department of Computer Science, Mangala Gangotri, Mangalore University, Mangalore, Karnataka India

jvgorabal@gmail.com, drmdh2014@gmail.com

Abstract: In this technical era, providing a security to the data is a challenging task. This article addresses the issues related to privacy and security issues of RFID technology. RFID is radio frequency identification technology. RFID is a wireless non-contact technology uses radio wave to transfer data or track the object automatically. The tags contain electronically stored information about the object or product. In this article we are considering multimodal biometrics for user authentication. Three different biometric traits like face, finger and knuckle are considered for user authentication and verification. The fusion approach is incorporated in the proposed system. Three publically available datasets are used for evaluation of the proposed model. The result of the experiments reveals that the proposed algorithm outperforms for different types of the biometric traits.

Keywords: RFID Tag, Multimodal, Privacy, Security

1. INTRODUCTION

RFID is an acronym for radio frequency identification, uses radio wave for wireless communication to uniquely identify tagged objects or people. An RFID device frequently just called an RFID tag contains electronically stored information about the object or product. Tags are powered by RFID readers and which read at short distance through radio waves. Since these tags are associated with the objects or people, it is necessary to address the privacy and security issues associated RFID technology. In this paper we focus on the privacy and security issues of RFID technology with the help of multimodal biometrics. Though there are so many unimodal

biometric based approaches to address privacy and security issues are exiting, the core idea which made us to drop unimodal biometrics approaches. Unimodal biometric systems have to contend with a variety of problems such as noisy data, intra-class variations, restricted degrees of freedom, non-universality, spoof attacks, cloning and unacceptable error rates. Some of these limitations can be addressed by deploying multimodal biometric systems that integrate the evidence presented by multiple sources of information. This research article address the privacy and security issues related with RFID technology with the help of multimodal biometric traits like face, finger and knuckle by using fusion of the trait features.

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.

2. Literature Survey

In this section, apart from the literature survey we will also discuss about common issues associated with unimodal biometrics. These issues made us to look towards multimodal biometrics to address privacy and security issue if RFID technology.

Even though biometric systems offer several advantages over traditional token (e.g. key, PIN) or knowledge (e.g. password) based authentication schemes. These are still vulnerable to attacks.

These attacks can be grouped into eight classes.

Class I: Spoof attack: In this type of attack a fake biometric e.g. (finger made from silicon, face mask, lens including iris texture) can be presented to a sensor.

Class II: The second class of attack is called *replay attack.* In this problem biometric data is submitted to the feature extractor by passing the sensor. To detect the replay attack, the authenticator as to ensure that the data is captured through the sensor and has not been injected. But sensor noise and input variations obstructs detection, so the best method is either to build a time stamp or using challenge and response mechanism to address the replay attack.

Class III: Substitution attack: In the third type of attack the feature exactor module is replaced by a Trojan horse program that functions according to its designer specifications. Then the attacker gets an access to storage either locally or globally. He can overwrite the legitimate users template with his /her own –in essence stealing their identity

Class IV: In the fourth type of attack a genuine feature values are replaced with values (synthetic or real) selected by the attacker or an imposter

Class V: In this type of attack the matcher is replaced with a Trojan horse program. This class of attack is called *Trojan horse Attack.*

*Class VI***:** This type of attack occurs on the *template database.* The template database can be added, modified or removed. The templates can also be stolen which can be most dangerous.

Class VII: Transmission attack: A man in the middle attack is possible while the data is transmitted from one component to another. The attacker can manipulate the input data stream, send a fake template as an enrolled user, inject an artificial matching score or even generate a forged response.
Class VIII: Lastly the matured result (accept or reject) can be overridden by the attacker.

Late 90's has witnessed progress in the research work on multi modal biometrics. At initial stages face is the most common biometric used alone or in combination with other biometrics. In 1998, a bimodal approach was proposed by Hong and Jain [4] for a PCA based face and a minutiae-based fingerprint identification system with a fusion method at the decision level. In 2000, a commercial multimodal approach developed by Frischholz and Dieckmann [5], BioID. Lip motion and face images were extracted from a video sequence and the voice from an audio signal for verifying the person. Fierrez-Aguilar and Ortega-Garcia (2003) [3] proposed a multimodal approach using face and minutiae-based fingerprint verification system, and an online signature verification system. Ross and Jain (2003) [2] combined face, fingerprint and hand geometry at the matching score level. Kumar et al. (2003) presented multimodal personal verification system using hand images by combining hand geometry and palm image at the feature level and match score level. Fusion at the match score level had good performance as compared to unimodal biometric. In 2004, Toh et al. [7] developed a multimodal biometric system using hand geometry, fingerprint, and voice at match-score-level fusion. Shahin et al. (2008) [9] used hand veins, hand geometry and fingerprint to provide high security. Chandran et al. (2009) [6] combined iris and fingerprint to improve the performance. Chin et al. (2009) [11] integrated palm print and fingerprint at feature level. Kang and Park (2009) [12] presented multimodal finger veins recognition using score level fusing for finger geometry and finger veins. Poinsot et al. (2009) [8] presented palm and face multimodal biometrics for small sample size problems. They used Gabor filter to extract features of palm and face images. Tayal et al. (2009) [10] presented multimodal iris and speech authentication system using decision theory.

3. Proposed Method

This paper presents the multimodal biometric based approach to handle privacy and security issues in RFID. Proposed model can be categorized into three different levels. First level discusses the data acquisition and feature extraction. Second level discuss about the encrypted knowledge base construction. Third level discuss about processing of encrypted data for addressing privacy and security issues of RFID.

Data Acquisition and Feature Extraction Stage:

Since our primary objective is to address the security and privacy issues of RFID systems, we are considering the multimodal biometric data i.e., face, finger print and knuckle. When these data are captured in a given unit of time 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.

Construction of Encrypted Knowledge Base

After the encryption of the biometric information, all the information is preserved in the encrypted knowledge base for further processing.

Data Matching at the Encrypted Level

During the recognition time, the same biometric traits like face, finger and knuckle information of the new user is considered. Then the newly acquired data are subjected for preprocessing and encrypted using run-length encoding scheme. After the successful completion of data encryption, the data matched with knowledge base. The proposed model of the above discussed method is graphically presented in the following figure.

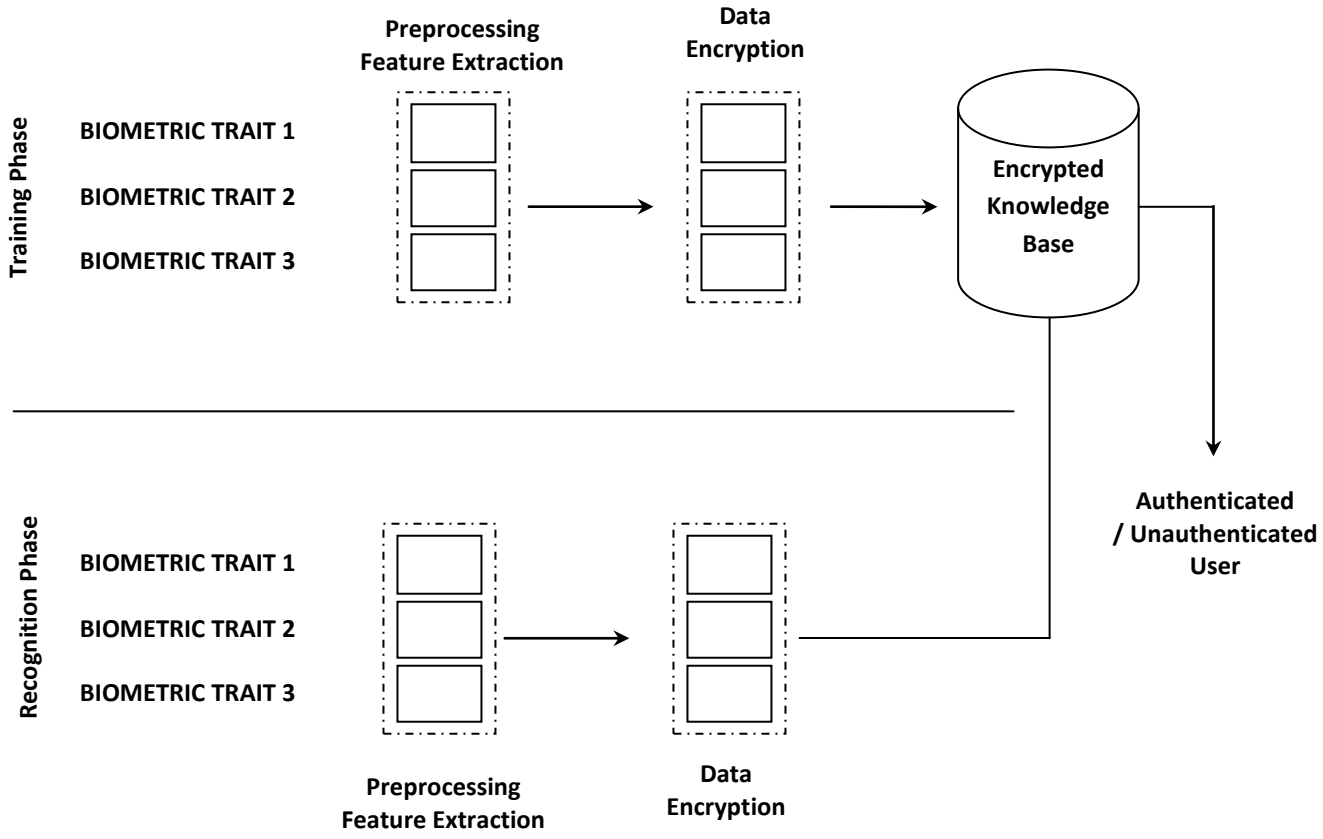


Figure 1: Block diagram of the proposed multimodal based approach

Algorithm:
Input: Three biometric traits like face, finger, knuckle
Output: Authenticated user or unauthenticated user.
Method:
CreateNode()
// Node a new data structure used to store all three biometric traits.
for i ← 1 to n // n = number of biometric traits.

for j ← 1 : m // m=database size.
Node$_{(i,j)}$←Three biometric trait like face, finger, knuckle.
end
end
Node_Preprocessing $_{(i,j)}$ ← Pre processing (**Node**$_{(i,j)}$)
Node_Binary$_{(i,j)}$← Binary (**Node**_Preprocessing $_{(i,j)}$)
Node_Encoded$_{(i,j)}$← RLEncoding (**Node**_Binary$_{(i,j)}$)
KB ← **Node**_Encoded
Testing Phase:
TestNode$_{(1,1)}$←First Biometric Trait (Face)
TestNode$_{(1,2)}$←Second Biometric Trait (Finger)
TestNode$_{(1,1)}$←Third Biometric Trait (Knuckle)

$\mathbf{P}_{\mathbf{reProcess\_TestNode}}$ ← Pre processing (**TestNode**)
$\mathbf{P}_{\mathbf{reProcess\_TestNode\ \_binary}}$ ← Binary ($\mathbf{P}_{\mathbf{reProcess\_TestNode}}$)
$\mathbf{P}_{\mathbf{reProcess\_TestNode\_encoded}}$ ← RLEncoding ($\mathbf{P}_{\mathbf{reProcess\_TestNode\_binary}}$)

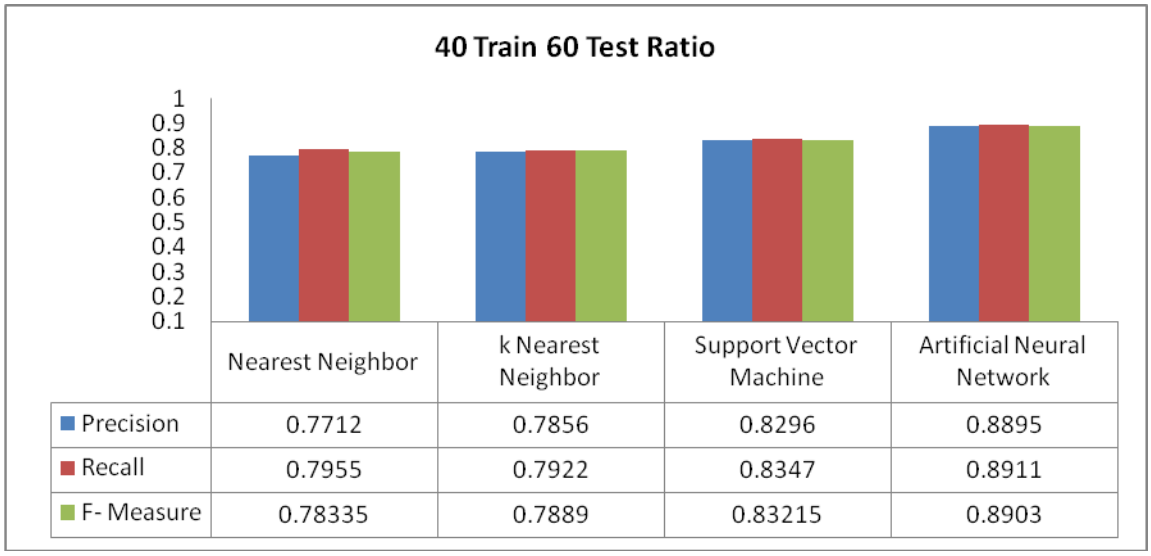
for i ← 1 : Num_Biometric_Traits
for j ← 1 : Dataset Size
Result = Matching ($\mathbf{P}_{\mathbf{reProcess\_TestNode\_encoded\ ,\ KB(i,j)}}$)
end
end
Algorithm Ends

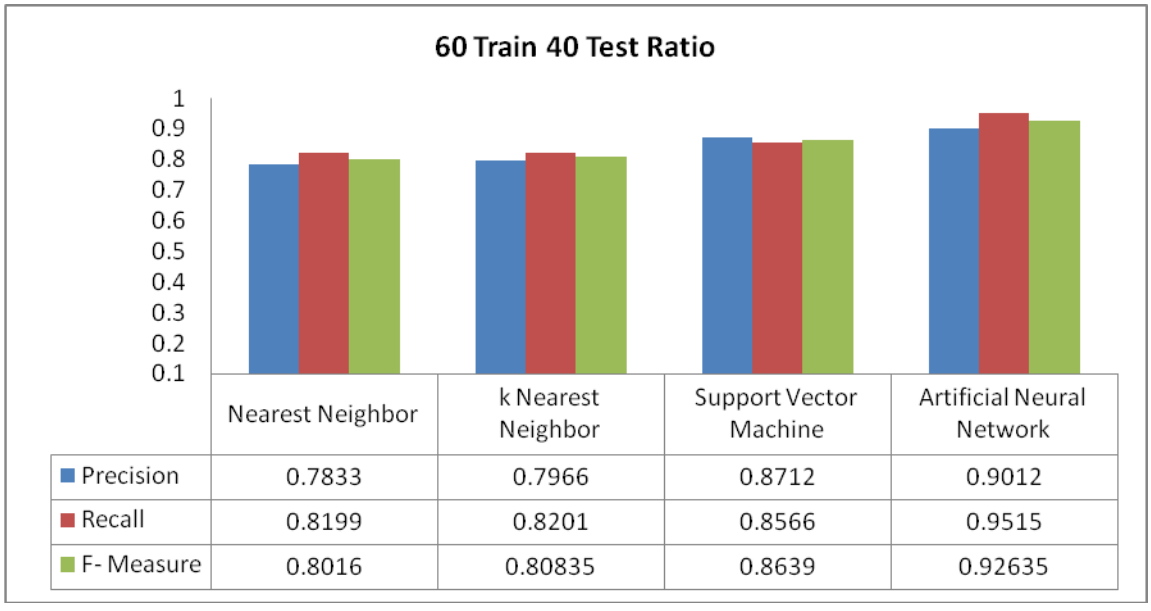
4. EXPERIMENTAL SETUP

In this section, we present the details of the experiments conducted to represent the effectiveness of the proposed method over three different biometric traits like face, finger and knuckle databases. The behavior of the proposed algorithm is critically analyzed on ORL face dataset, Umist face dataset and knuckle database. ORL face data is a publically available dataset consists of 400 samples from 40 different classes. Umist data is also a publically available face dataset which consists of 1012 samples from 20 different classes. Knuckle data set consists of 7920 samples from both right hand left hands from 660 different classes. We have conducted two sets of experiments; where each set contain three different traits. 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 trial we have randomly selected training and testing samples. Four different classifiers were considered for the evaluation of the proposed method. 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 table 1

This methodology will be incorporated to generate the UID(Unique Identification Number) for a RFID tag , that number will be used to check the authenticity of the tag, this may be used in E- Passport to validate the user.

	40: 60			60:40		
	Precision	**Recall**	**F- Measure**	**Precision**	**Recall**	**F- Measure**
Nearest Neighbor	0.7712	0.7955	0.78335	0.7833	0.8199	0.8016
k Nearest Neighbor	0.7856	0.7922	0.7889	0.7966	0.8201	0.80835
Support Vector Machine	0.8296	0.8347	0.83215	0.8712	0.8566	0.8639
Artificial Neural Network	0.8895	0.8911	0.8903	0.9012	0.9515	0.92635





5. CONCLUSIONS

This article presents the multimodal biometric based approach for handling privacy and security issues associated with RFID technology. Radio frequency identification tag is an upcoming technology, which has wide range of applications. Hence addressing the privacy and security issues of RFID technology is the need of the hour. In this paper we have considered biometric traits like face, finger and knuckle for addressing privacy and security issue. Though the biometrics provides security to a system, we cannot rely only on the biometric data. This requirement made us to look towards data encryption. The RLE encryption is applied for the biometric traits and an encrypted knowledge base is constructed and for the same users recognition is done at the data encryption level only. The proposed model evaluated by four well known different classifiers. Evaluation of result of the proposed model over four classifier reveals that the proposed model out performs with artificial neural network. The same approach can be extended to RFID based E-Passports to validate the user.

REFERENCES

1. A. Juels. RFID Security and Privacy: A Research Survey. Journal of Selected Areas in Communication (J-SAC), 24(2):381-395, February 2006 .
2. A. Ross & A. K. Jain, *Information Fusion in Biometrics*, Pattern Recognition Letters, 24 (13), pp. 2115-2125, 2003.
3. J. Fierrez-Aguilar, J. Ortega-Garcia, D. Garcia-Romero, and J. Gonzalez Rodriguez, ―A comparative evaluation of fusion strategies for multimodal biometric verification, In Proc. 4th Int, Conf,Audio-video-based Biometric PersonAuthentication , J. Kittler and M. Nixon, Eds., 2003 vol. LNCS 2688, pp. 830–837.
4. L. Hong and A. K. Jain, ―Integrating faces and fingerprints for personal identification,‖ IEEE Trans. Pattern Anal. Mach. Intell. , vol. 20, no. 12, pp. 1295– 1307, Dec. 1998
5. Frischholz and U. Dieckmann, ―BiolD: A multimodal biometric identification system,‖ Computer,vol.33,no.2, pp.64-68,Feb,2000.
6. Chandran GC, Rajesh RS (2009). Performance Analysis of Multimodal Biometric System Authentication, Int. J. Comput. Sci. Network Security, 9: 3.
7. K. A. Toh, X. D. Jiang, and W. Y. Yau, ―Exploiting global and local decisions for multi-modal biometrics verification, IEEE Trans. Signal Process., vol. 52, no. 10, pp. 3059–3072, Oct. 2004
8. Poinsot A, Yang F, Paindavoine M (2009). Small Sample Biometric Recognition Based on Palmprint and Face Fusion, Fourth International Multi-Conference on Computing in the Global Information Technology.
9. Shahin MK, Badawi AM, Rasmy ME (2008). A Multimodal Hand Vein,Hand Geometry and Fingerprint Prototype Design for High Security Biometrics, CIBEC'08.
10. Tayal A, Balasubramaniam R, Kumar A, Bhattacharjee A, Saggi M (2009). A Multimodal Biometric Authentication System Using Decision Theory, Iris and Speach Recognition, 2nd International Workshop on Nonlinear Dynamics and Synchronization.
11. Chin YJ, Ong TS, Goh MKO, Hiew BY (2009). Integrating Palmprint and Fingerprint for Identity Verification, Third International Conference on Network and System Security.
12. Kang BJ, Park K (2009). Multimodal Biometric Authentication Based on the Fusion of Finger Veins and Finger Geometry, Optical Eng., 48.

