ISSN: 0976-3104
SPECIAL ISSUE
Gorabal et al.

THE IIOAB JOURNAL

ARTICLE OPEN ACCESS

NOVEL IMPLEMENTATION OF MULTIMODAL BIOMETRIC APPROACHES TO HANDLE PRIVACY AND SECURITY ISSUES OF RFID TAG

J. V. Gorabal*, Manjaiah D. H., and S. N. Bharath Bhushan

Department of Computer Science & Engineering SCEM, Mangalore, KA, INDIA
Department of Computer Science, Mangalore University, Mangalore, KA, INDIA

ABSTRACT

In the present scenario there is huge technology revolution in all dimension of life, in this context one such promising technology is Radio frequency Identification technology which is a very strong substitute for Barcode in automatic identification systems. As the technology is growing in the same speed issues like eavesdropping, cloning, spoofing etc are becoming nig threat for the development of this smart technology. Since research is ongoing process, it is the constructive process to contribute some novel approaches in the field of automatic identification technology. Since in coming days RFID tag based applications may make big revolutions to make the life of the people more smart. In this direction as a part of my research work this article contributes in designing a security system to handle critical issues in RFID enabled applications. At present Biometric security is gaining lot of importance in providing security for many applications. Since Biometric traits are unique in its nature obviously this technology stands most promising in place password or token based mechanism. Here we proposed a multimodal biometric based security systems to handle critical issues. The proposed work uses feature level fusion approach, the same is experimented with F-Measure, Precision and Recall. The results are very comprehensive, robust and promising in its nature.

Received on: 10th -Apr-2016
Revised on: 29th-Apr-2016
Accepted on: 5th-May-2016
Published on: 10th-May-2016

KEY WORDS

Radio frequency, Privacy, Security, Multimodal, Biometric.

***Corresponding author:** Email: jvgorabal@gmail.com

INTRODUCTION

Radio frequency recognizable proof (RFID) empowers the ID of various RFID tags. The distinguishing proof procedure is performed over a remote system without the assistance of observable pathway or physical touch between the RFID tags and the RFID reader [1]. These better optimal properties like low installation costs, convenient to use, easy to manage and less computational hassles, etc., are making the RFID technology to be most suitable to replace conventional strategies. It is the most suitable candidate to replace technology like Barcode systems. In the present situation many RFID systems are massively installed across the globe, which are useful for object tracking, manufacturing, supply chain management, tiny goods management, retailing and for different applications, for example in defense and admission management. The RFID research has the enormous force of gathering data about an object and variables [1, 2]. There are so many issues in RFID management system, since it is cutting edge technology, the term confidentiality, competence, heterogeneity, dependability have lots of roles to play in the coming days.

Since RFID technology is gaining lot importance in the market [3], intruders are also hyperactive in killing the technology by disclosing confidential information, denial of service attack, data corruption, which are the biggest threat to the growth of the technology, but as we know no technology is free from issues and hurdles. Being researchers, engineers, it is an opportunity to handle the hurdles to make this technology a promising technology for the mankind of this modern digital world.

The present research focuses on handling privacy and security issues and proposed many solutions to protect the system and make the technology as popular as possible, but still there are some issues left unanswered. Many researchers in their proposed solutions like hazing, cryptographic approaches, pseudo names, secret-words etc, but these are not enough to withstand the attacks. Hence it made us to focus on a typical and unique methodology to deploy.

THE IIOAB JOURNAL
ISSN: 0976-3104

As we know biometric a trait are the one gaining lot of importance in providing security to the stakeholders. Biometric features are permanent and unique which are concrete during pregnancy, even twins will have different biometric print, may be retina, finger and face. Taking this into consideration RFID enabled applications like E-Passport, where stakeholder data is very precious, challenge to protect from intruders. This situation made us to think to act upon privacy and security issues and a made us to design a solution to enable the technology for the intended functionality which certainly will make the RFID system trustworthy and dependable [4].

RELATED WORK

At present there is lot of research is in progress to protect the privacy of consumer. In this process there are several techniques and approaches are contributed by many researchers to handle the various issues associated with RF ID technology. Following are the techniques which will be considered for handling above mentioned critical issues. Those techniques includes blocker tag, password approach, hashing approach, tag killing approach and encryption approach. But non of these approaches can handle the issues effectively. As a solution to this issue, in this article we proposed a novel and effective yet efficient methodology which incorporate multimodal biometric approach to handle privacy and security issues associated with RFID technology.

PROPOSED MODEL

Picture encryption for privacy and security issues of RFID

This section exhibits a picture encryption based model to handle protection and security issue of RFID innovation. The goal of this work is to build up a solid and ideal calculation for giving the security to the RFID labels [5]. This specific methodology guarantees to give a superior security to the framework. This model capacities two stages, for example, information encryption stage and the contrasting of the encoded information.

Information encryption stage

Since the indispensable target of the proposed procedure is to give security to the RFID systems, biometric properties like face and knuckle are considered. Precisely when this information are put away by using honest to goodness biometric information by electronic devices, they are subjected for pre-planning computations. Once the information is preprocessed, the RGB biometric information is changed over into double information. Right when, the information is changed over to parallel, i.e., blend of 0's and 1's are given as data RLE data encryption computations an immediate and persuading figuring for encoding the information. RLE computation counts perceive the two fold information and make the relating encoded yield.

Coordinating data at encrypted level

Once the information is produced, they are put away in the knowledge base for next computation. The following diagram of the calculation is to think about this information at scrambled level [6].

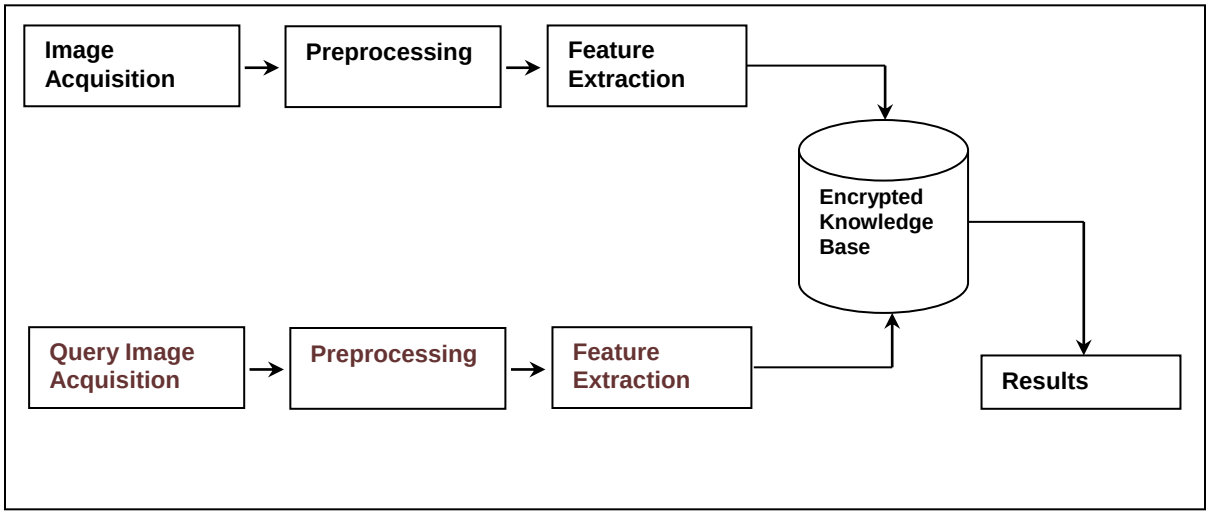

Fig: 1. Block Diagram of the Anticipated Model

THE IIOAB JOURNAL
ISSN: 0976-3104

ALGORITHM

Algorithm: Image Data Encryption Mechanism
Start:
I_{data} (Input collection of Training Data

$I_{PreProcess}$ (Pre processing (I_{data})

Twofold ←Twofold ($I_{PreProcess}$)

I encoded (RLEncoding (I twofold)

KB ←I encoded

$I_{Testing\_Data}$ (Input collection of Testing Data

$I_{PreProcess\_Testing\_Data}$ (Pre processing ($I_{Testing\_Data}$)

$I_{Test\_twofold}$ ←Twofold ($I_{PreProcess\_Testing\_Data}$)

$I_{Test\_encoded}$ (RLEncoding ($I_{Test\_twofold}$)

For me (1: Num_Classes

Result ($I_{Testing\_Data}$) (Compareing ($I_{Test\_encoded}$, KB ($i_{\_Class}$))

End

Multimodal biometrics for privacy and security issues of RFID

This strategy addresses the privacy and security issues in RFID technology. With the help of multimodal biometric traits like “face and knuckle by using a fusion of the biometric trait features [7, 8]. The proposed model can be categorized into three various levels. First level discusses the data acquisition and feature extraction. Second level discuss about the encrypted knowledge base construction. Third level discusses processing of encrypted data for addressing privacy and security issues of RFID [9].

Data acquisition and feature extraction stage

Since the essential target of this work is to address the security and privacy issues of RFID systems, we are considering the multimodal biometric information i.e., face, and knuckle[10]. At the point when this information is captured in a given unit of time by using proper biometric information securing gadgets, they are subjected for pre-processing computations. Once the information is stored, the RGB biometric information is changed over into twofold information. When, the information is changed over to twofold, i.e., combination of 0's and 1's are given as data to run length encoding algorithm.

Construction of encrypted knowledge base

Once the data acquisition and feature extraction is accomplished, construction of encrypted knowledge base is the next step. Run Length Encoding (RLE) is the lucid and impressive encoding technique which accepts the twofold data and generates the corresponding encoded output. After the encryption of the biometric traits are completed, all the individual traits encrypted information are fused and then stored in the knowledge base for further computation. Working principle of Run Length Encoding is as shown in the following.
Input: 1111001110
Encoded Output: 41203110.

Data compression at the encrypted level

“Once the encrypted knowledge base is constructed, supervised learning algorithms like” nearest neighbor, k nearest neighbor, support vector machine and artificial neural network classifiers are designed for identification of the authorized stakeholders.” Once the all the training is completed with biometric traits like face, knuckle next phase is the recognition phase. During the recognition time, the same biometric traits like face knuckle information of the new user is considered. Then the newly obtained data are subjected for preprocessing and encrypted using run-length encoding scheme. After the successful completion of data encryption, the data compared with knowledge base. The proposed model of the above discussed method is graphically presented in the following figure.”

Algorithmic model

Algorithm:

Input: Two biometric traits like face and, knuckle
Output: Authenticated user or unauthenticated user.
Method:
CreateNode()

THE IIOAB JOURNAL
ISSN: 0976-3104

// Node a new data structure used to store all three biometric traits.
For me (1 to n // n = number of biometric traits.
for j ← 1 : m // m=database size.
Node$_{(i,j)}$←Three biometric trait like face, 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$_{(1,1)}$←Seond Biometric Trait (Knuckle)
$\mathbf{P}_{\text{reProcess\_TestNode}}$←Pre processing (**TestNode**)
$\mathbf{P}_{\text{reProcess\_TestNode\_twofold}}$ ←Twofold ($\mathbf{P}_{\text{reProcess\_TestNode}}$)
$\mathbf{P}_{\text{reProcess\_TestNode\_encoded}}$← RLEncoding ($\mathbf{P}_{\text{reProcess\_TestNode\_twofold}}$)
for i ← 1 : Num_Biometric_Traits
for j ← 1 : Dataset Size
Result = Compareing ($\mathbf{P}_{\text{reProcess\_TestNode\_encoded , KB(i,j)}}$)
end
end
Algorithm Ends

RESULTS AND DISCUSSION

This section shows the sufficiency of the proposed framework on two arrangements of biometric qualities data and knuckle dataset [11]. With the deciding objective of evaluation of the results, three most basic measures like precision, recall and f-measures are considered for each trial. The results of the experiments are presented in **Table–1**.

Table: 1. Result of Data matching at encrypted level

	"ORL Face Dataset "		"UmistFace Dataset"		"Knuckle Dataset "	
	40 / 60	**60/ 40**	**40 / 60**	**60/40**	**40/ 60**	**60/40"**
Precision	.88500	.88833	.88400	.98000	.88050	.88333
Recall	.88600	.88949	.88564	.99089	.88000	.88596
F- Measure	.88549	.88890	.88481	.99044	.88024	.88462
CA	.88500	.88830	.88400	.90000	.88000	.88333

Table: 2. Result Multimodal Biometric Approach

	40/ 60			60/40		
	Precision	Recall	F- Measure	Precision	Recal l	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

THE IIOAB JOURNAL
ISSN: 0976-3104

How proposed model works in RFID applications

With RFID technology enabled applications like passport stakeholders E-Passport (RFID Tag) is uniquely identified by UID unique identification No which is scanned by an RFID scanner with proper database and middleware. To check the authenticity of the user, the user has to submit his biometrci traits, these biometric traits are used to compute and generate UID. If this UID and scanned UID are same then scanned the RFID tag belongs to legitimate user is fake. Like this our proposed methodology protects the users' information and validates the same for further press [12].

Here we proposed multimodal approaches and conceived calculations for feature extraction and the development of knowledge base with the assistance of more than three distinctive biometric characteristics like face and knuckle databases are viewed as Accuracy can be seen as a measure of exactness or consistency, however the audit is a measure of zenith. Four unique classifiers were considered for the assessment of the proposed strategy. At the end we have figured accuracy, review and f-measure. The results of the tests are mentioned in the **Table–2**.

CONCLUSION AND FUTURE WORK

The proposed mechanism comprises of two stages like information encryption and coordinating of encoded information. The algorithm is fundamentally broke down on two biometric information viz face and knuckle. In the proposed approach we used RLE encryption for the biometric attributes and with the help of the encoded knowledge base is developed. During authentication process user has to submit the above mentioned two traits to validate. Our experiments proved that this method can be deployed to protect the user's private information in RFID technology based applications. In future the same technology may be used for more than four to five biometric traits to provide a robust security measures for RFID enabled applications.

ACKNOWLEDGEMENT
None
.

CONFLICT OF INTEREST
Authors declare no conflict of interest.

FINANCIAL DISCLOSURE
No financial support was received to carry out this project

REFERENCES

[1] A Juels. [2006] RFID security and privacy: a research survey. *Journal of Selected Areas in Communication (J-SAC)* 24(2): 381–394.
[2] V Daniel Hunt Albert, Puglia, Mike Puglia.[2007] RFID a Guide to Radio frequency Identification Technology.
[3] Yanjun and Zuo.[2010] Survivable RFID Systems: Issues, Challenges, and Techniques, *IEEE Transactions* 40(4):406–418.
[4] Ari Juels.[2010] RFID Security and Privacy A Research Survey*: IEEE Journal on selected areas in communications*. 24 (2).
[5] JV Gorabal, Manjaiah DH,[2014] Image data encryption approach for security issues International, *Journal of Information Technology Management Information System (IJITMIS)*, 5(2):59–64.
[6] A Ross and A.K Jain. [2003] Information Fusion in Biometrics, *Pattern Recognition Letters*, 24(13),2115–2125.
[7] J Fierrez-Aguilar. [2003] A comparative evaluation of fusion strategies for multimodal biometric verification,in Proc. 4th Int, *Conf,Audio-video-based Biometric Person Authentication* , 26(88):830–837.
[8] L Hong and AK Jain. [1998] Integrating Faces and Fingerprints for Personal Identification, *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 20 (2):1295–1307.
[9] Maher K Mahmood and Jinan N Shehab.[2014] Image Encryption and Compression Based on Compressive Sensing and Chaos, *International Journal of Computer Engineering & Technology (IJCET)*, 5(1): 68 – 84.
[10] Mahmood Al-khassaweneh, Selin Aviyente. [2008]Image Encryption Scheme Based on Using Least Square Approximation Techniques, *IEEE Transactions*, 108–111.
[11] Suhaila O. Sharif, LI Kuncheva, SP Mansoor. [2010] Classifying Encryption Algorithms Using Pattern Recognition Techniques, *IEEE Transactions*, 168–1172.
[12] JV Gorabal, Manjaiah DH,[2015] Multimodal Biometic Approaches to handle privacy and security issues in radio frequency identification technology, *International Journal of Computer Science and Mobile Computing*, 4(3):765–771.