European Journal of Academic Essays 1(1): 6-10, 2014
ISSN: 2183-1904
www.euroessays.org

Multi Modal Biometrics using Cryptographic Algorithm

B.Kiran Bala[1], J.Lourdu Joanna[2]

[1]K.Ramakrishnan college of Engineering
Trichy, Tamil Nadu
India
Email: kiranit2010@gmail.com

[2]Care School Of Engineering
Trichy,Tamil Nadu
India
Email: lourdujo@gmail.com

Abstract: Security is a major issue in all recent developing technologies, for that system deals with palm-vein and Iris (Biometrics inputs) from the user and then extract the features like edge, texture using the feature extraction algorithm from both palm vein and iris captured images simultaneously and then apply cryptographic algorithm (Blow fish) to that extracted features. Finally cipher text will be generated and stored in the database. Matching algorithm is also a major issue for the multimodal biometrics to avoid the time delay the proposed system matching algorithm avoid the time delay and also the system avoid the false acceptance rate as well as false rejection rate is very low compare to the existing system has been justify by the system results.

Keywords: Data Encryption Standard, Advanced Encryption Standard, Blow fish, Key-Dependent Advanced Encryption Standard, Cipher Text

1. Introduction

The increasing reliance on electronic information, which needs to be exchanged across the internet or stored on open networks, cryptography is becoming an increasingly important feature of computer security. A biometric key dependent cryptosystem is proposed, to ensure the security of the whole system by using fingerprint features as a key in a cryptosystem, like, key-dependent Advanced Encryption Standard (KAES). KAES is used to ensure that no trapdoor is present in cipher and to expand the key-space to slow down attacks [1]. Biometric template protection is one of the important issues in deploying a practical biometric system. To tackle this problem, many algorithms have been reported in recent years, most of them being applicable to fingerprint biometric. Since the content and representation of fingerprint template is different from templates of other modalities such as face, the fingerprint template protection algorithms cannot be directly applied to face template. Moreover, we believe that no single template protection method is capable of satisfying the diversity, revocability, security and performance requirements. We propose a three-step cancelable framework which is a hybrid approach for face template protection. This hybrid algorithm is based on the random projection, class distribution preserving transform and hash function. Two publicly available face databases, namely FERET and CMU-PIE, are used for evaluating the template protection scheme. Experimental results show that the proposed method maintains good template discriminability, resulting in good recognition performance. A comparison with the recently developed random multispace quantization

Corresponding Author: B.Kiran Bala, Email: kiranit2010@gmail.com

(RMQ) bio hashing algorithm shows that our method outperforms the RMQ algorithm [2]. The user Authentication methods based on hash functions like MD5, NT / NTLM and SHA-1 can be easily Compromise. We used methods that utilize cryptanalytic tables based on time memory tradeoff procedures (TMTO) and we analyzed certain limitations on this approach. With those modifications a new concept for TMTO procedures is created. We also describe vulnerabilities based on physical access to a segment of a computer network infrastructure that can compromise almost any quasi secure system. Regarding those vulnerabilities we present a number of biometric authentication methods that can minimize or nullify this security risks [3]. Since fingerprint data are no secrets but of public nature, the verification data transmitted to a smartcard for on card matching need protection by appropriate means in order to assure data origin in the biometric sensor and to prevent bypassing the sensor. For this purpose, the verification data to be transferred to the user smartcard is protected with a cryptographic checksum that is calculated within a separate security module controlled by a tamper resistant car terminal with integrated biometric sensor [4]. Uni modal 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, 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 paper discusses the various scenarios that are possible in multimodal biometric systems, the levels of fusion that are plausible and the integration strategies that can be adopted to consolidate information. We also present several examples of multimodal systems that have been described in the literature [5]. Multimodal biometric system utilizes two or more individual modalities, e.g., face, gait, and fingerprint, to improve the recognition accuracy of conventional unimodal methods. However, existing multimodal biometric methods neglect interactions of different modalities during the subspace selection procedure, i.e., the underlying assumption is the independence of different modalities. In this paper, by breaking this assumption, we propose a Geometry Preserving Projections (GPP) approach for subspace selection, which is capable of discriminating different classes and preserving the intra-modal geometry of samples within an identical class. With GPP, we can project all raw biometric data from different identities and modalities onto a unified subspace, on which classification can be performed. Furthermore, the training stage is carried out once and we have a unified transformation matrix to project different modalities. Unlike existing multimodal biometric systems, the new system works well when some modalities are not available. Experimental results demonstrate the effectiveness of the proposed GPP for individual recognition tasks [6].

2. Proposed System

In this proposed system biometrics like palm vein and iris taken initially extract the feature from this inputs and then apply cryptographic algorithm to the extracted features figure. 1. Shows the basic block diagram of this proposed system.

2.1 Input as palm vein and iris

This is an initially stage of this system, palm vein and iris both the images are capture and used for this proposed system.

2.2 Extract the feature for palm vein and iris image

This is an important stage available for this proposed system to extract the features for both the palm vein and iris image separately by following ways Initially acquired the palm vein image then find out the smoothing and edge of the palm vein to be enhanced, then find the threshold value for the palm vein finally post process the value. locate the IRIS from the image using the transform convert the values and find the iris code.

2.3 Integrate the image

Adaptive Multimodal Biometric Fusion Algorithm"(AMBF), which is a combination of Bayesian decision fusion and particle swarm optimization. A Bayesian framework is implemented to fuse decisions received from multiple biometric sensors. The system's accuracy improves for a subset of decision fusion rules. The optimal rule is a function of the error cost and a priori probability of an intruder. This Bayesian framework formalizes the design of a system that can adaptively increase or reduce the security level. Particle swarm optimization searches the decision and sensor operating points (i.e. thresholds) space to achieve the desired security level. The optimization function aims to minimize the cost in a Bayesian decision fusion. The particle swarm optimization algorithm results in the fusion rule and the operating points of sensors at which the system can work. This algorithm is important to systems designed with varying security needs and user access requirements. The adaptive algorithm is

found to achieve desired security level and switch between different rules and sensor operating points for varying needs. A Bayesian framework formalizes the design of a personal identification system that can adaptively increase or reduce the security level as well as adapt to each user's physical characteristics. The key is to use multiple biometric modes, adapt the error costs, and vary the sensor operating points giving the system robustness and adaptability. The extracted feature can be integrated with AMBF.

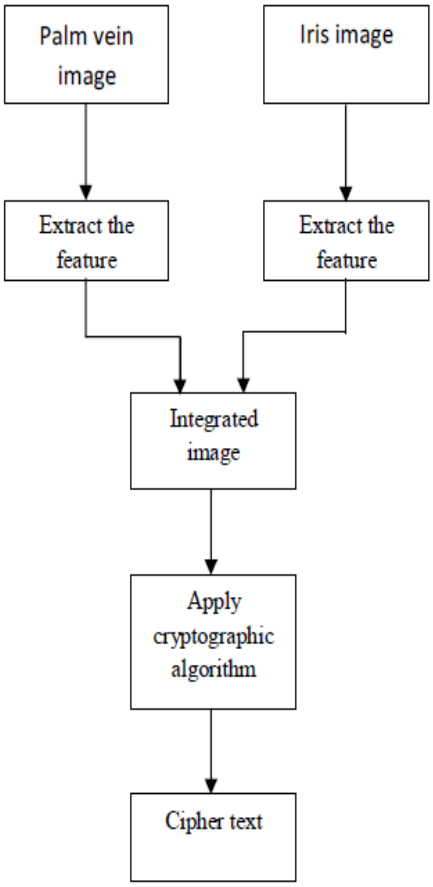

Figure. 1: Basic diagram for the proposed system

2.4 Apply cryptographic algorithm

Cryptography is the science of encrypting and decrypting written communication. It comes from the Greek word kryptos, meaning hidden, and graphia, meaning writing. Cryptanalysis is the process of trying to decrypt encrypted data without the key. Plain text: This is the original message or data that is fed into the algorithm as input.
Encryption algorithm: This algorithm performs various substitutions and transformations on the plain text. Secret key: the secret key is also input the algorithm. The exact substitutions and transformations performed by the algorithm depend on the key. Cipher text: this is the scrambled message produced as output. It depends on the plain text and the secret key. Decryption algorithm: this is essentially the encryption algorithm run in reverse. It takes cipher text and the same secret key and produces original plain text.

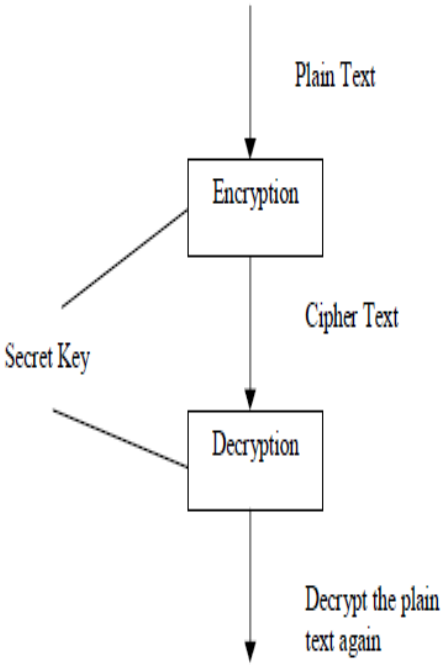

Figure. 2: Symmetric key cryptography

The basic block diagram for the symmetric key cryptography is shown Blowfish is a symmetric encryption algorithm, meaning that it uses the same secret key to both encrypt and decrypt messages. In the following two sections we would explain in details the two parts of the blowfish algorithm which they are: data encryption & key expansion
Data encryption: The input is a 64-bit data element, x. Divide x into two 32-bit halves: xL, and xR. Key expansion: Key expansion converts a variable-length key of at most 56 bytes (448 bits) into several sub key arrays totaling 4168 bytes. Blowfish has 16 rounds. Each round consists of a key-dependent permutation, and a key- and data-dependent substitution. All operations are XORs and additions on 32-bit words. Blowfish has 16 rounds .Blowfish is also a block cipher, meaning that it divides a message up into fixed length blocks during encryption and

decryption [21]. The block length for Blowfish is 64 bits; messages that aren't a multiple of eight bytes in size must be padded. Blowfish is public domain.

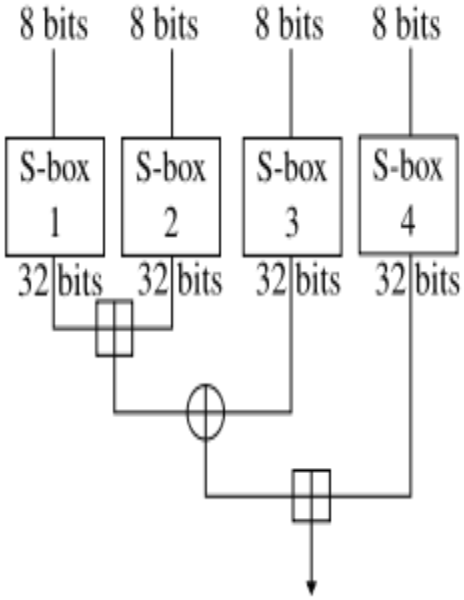

Figure 3:. Graphical representation of blow fish

This proposed system deals with blow fish algorithm for encrypt the palm vein and iris image

2.5 Cipher text

Finally after applying cryptographic algorithm to the integrated image of both iris and palm vein there will be the conversation of plain text into unknown format is called cipher text.

3. Experimental Results

The database provided good segmentation, since those eye images had been taken specifically for iris recognition research and boundaries of iris pupil and sclera were clearly distinguished. For the database, the segmentation technique managed to correctly segment the iris region from 624 out of 756 eye images, which corresponds to a success rate of around 83%. The LEI images proved problematic and the segmentation process correctly identified iris and pupil boundaries for only 75 out of 120 eye images, which corresponds to a success rate of around 62%.The problem images had small intensity differences between the iris region and the pupil One problem faced with the implementation was that it required different parameters to be set for each database. These parameters were the radius of iris and pupil to search for, and threshold values for creating edge maps. However, for installations of iris recognition systems, these parameters would only need to be set once, since the camera hardware, imaging distance, and lighting conditions would usually remain the same. The proposed palm vein recognition is carried out on 5 samples of 50 users. Palm vein reader based on NIR imaging technique obtains the palm vein images. The following steps do the palm vein recognition. In this paper image de-noising and enhancement is performed by GSZ shock filter. The real part of the GSZ shock filter provides the de-noised and enhanced image.

Table 1: Fusion algorithm performance

Algorithm	*Complete Database*		*Low quality Image*		*High quality image*	
	A	B	A	B	A	B
Adaptive Multimodal Biometric Fusion Algorithm	97.2	16.3	95.5	17.6	99.01	17.26

In **Table 1** A denotes the verification accuracy in (%), B denotes the Time in seconds.

Table 2: Comparison Of cryptographic algorithm

Algorithms	*Data (MB)*	*Time (sec)*	*Average (MB/SEC)*	*performance*
DES	256	10.2-11.4	21-23.1	LOW
3 DES	256	12.5	11.7	LOW
AES	256	5.7	51.6	MEDIUM
Blow fish	256	3.4-3.9	63.9	HIGH

4. Conclusion

Security issues of multimodal biometrics of existing system has been overcome in the proposed system and give more security in the biometrics using the mulit model biometrics by applying the cryptographic algorithm the existing algorithm performance is medium compare to the proposed system methodology as well as algorithm by the experimental results and tabulations justify the results. In future try to implement for different recognition like gait, heart beat etc and cryptographic algorithm like elliptic cure, MD5 etc like that algorithm can be implement and matching algorithm time taken should be minimize and try to avoid the false acceptance rate and false rejection rate in the system.

List of Abbreviations

S.No	Abbreviations	Expansion
1.	AES	Advanced Encryption Standard
2.	DES	Data Encryption Standard
3.	3DES	Triple Data Encryption Standard
4.	GPP	Geometry Preserving Projections
5.	AMBF	Adaptive Multimodal Biometric Fusion Algorithm
6.	KAES	key-dependent Advanced Encryption Standard

References

[1] A Proposal for a Biometric Key Dependent Cryptosystem by K. Hassanain1 ,M. Shaarawy, E. Hesham2, P a g e 42 Vol. 10 Issue 11 (Ver. 1.0) October 2010 Global Journal of Computer Science and Technology.

[2] A Hybrid Approach for Face Template Protection by Y C Feng, Pong C Yuen and Anil K: JainDepartment of Computer Science , Hong Kong Baptist University.

[3] Improving computer authentication systems with biometric technologies by Tonimir Kišasondi, Miroslav Bača, Ph. D., Senior Lecturer, Markus Schatten, BSc: University of Zagreb, Faculty of Organization and Informatics, Pavlinska 2, 42000 Varaždin, Croatia.

[4] Protected Transmission of Biometric User Authentication Data for OncardMatching by Ulrich Waldmann Fraunhofer-Institute Secure Telecooperation SIT Rheinstr. 7564295 Darmstadt, Germany.

[5] multimodal biometrics: an overview, Arun Ross and Anil K. Jain, Appeared in Proc. of 12th European Signal Processing Conference (EUSIPCO), (Vienna, Austria), pp. 1221-1224, September 2004.

[6] Multimodal biometrics using geometry preserving projections, Tianhao Zhanga,c, Xuelong Lib, Dacheng Taoc,∗ , JieYanga, 2007 Pattern Recognition Society. Published by Elsevier Ltd. All rights reserved

Authors Profile

Mr.B.Kiran Bala has Completed his B.Tech (inf ormation Technology) and then completed his M.E (Computer and communication Engineering) concurrently he also completed his MBA (human Resource Management) and he is very much interest in cryptographic, image processing and networks

Mrs.J.Lourdu Joanna has Completed her B.E (Compute Science and Engg) and then Completed her M.E (Compute Science and Engg) and she is very much interested in Data structure, operating system