Journal of King Saud University – Computer and Information Sciences (2016) **28**, 381–394

King Saud University

Journal of King Saud University – Computer and Information Sciences

www.ksu.edu.sa
www.sciencedirect.com

New chaff point based fuzzy vault for multimodal biometric cryptosystem using particle swarm optimization

Gandhimathi Amirthalingam [a,*], **G. Radhamani** [b]

[a] *Department of Computer Science, Bharathiar University, India*
[b] *Department of Computer Science, Dr. G.R.Damodaran College of Science, India*

Received 31 January 2014; revised 1 October 2014; accepted 9 December 2014
Available online 31 October 2015

KEYWORDS

Modified Region Growing method;
Local Gabor XOR Pattern;
Chaff points;
Particle swarm optimization algorithm;
Fuzzy vault

Abstract An effective fusion method for combining information from single modality system requires Multimodal biometric crypto system. Fuzzy vault has been widely used for providing security, but the disadvantage is that the biometric data are easily visible and chaff points generated randomly can be easily found, so that there is a chance for the data to be hacked by the attackers. In order to improve the security by hiding the secret key within the biometric data, a new chaff point based fuzzy vault is proposed. For the generation of the secret key in the fuzzy vault, grouped feature vectors are generated by combining the extracted shape and texture feature vectors with the new chaff point feature vectors. With the help of the locations of the extracted feature vector points, x and y co-ordinate chaff matrixes are generated. New chaff points can be made, by picking best locations from the feature vectors. The optimal locations are found out by using particle swarm optimization (PSO) algorithm. In PSO, extracted feature locations are considered particles and from these locations, best location for generating the chaff feature point is selected based on the fitness value. The experimentation of the proposed work is done on Yale face and IIT Delhi ear databases and its performance are evaluated using the measures such as Jaccard coefficient (JC), Genuine Acceptance Rate (GAR), False Matching Rate (FMR), Dice Coefficient (DC) and False Non Matching Rate (FNMR). The results of the implementation give better recognition of person by facilitating 90% recognition result.

* Corresponding author.
E-mail address: gandhimathi0177@gmail.com (G. Amirthalingam).
Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

1. Introduction

Biometric has recently emerged as the unique function which executes an amazing task of precise identification of individual by their bodily or behavioral traits (Vandommele, 2010). Authentication is the task of substantiating or validating

http://dx.doi.org/10.1016/j.jksuci.2014.12.011

something or someone as genuine (Bhattacharyya et al., 2009). A biometric authentication mechanisms permit is validated persons by comparing a query furnished by the applicant to its biometric reference. In accordance with the outcome of this analysis, the claim is acknowledged and the system confirms that he/she owns the identity or not (Giot et al., 2012). Face (Leng et al., 2010) and ear are the modalities used in the proposed work for client identification. Facial recognition technology (FRT) has asserted itself as an eye-catching remedy to take care of several modern requirements for recognition and the authentication of identity claims. It combines the guarantees of parallel biometric mechanisms, which tend to attach an identity to independent characteristic traits of the body, and the supplementary recognizable functionality of visual supervision mechanisms (Introna and Nissenbaum, 2010). The characterizing key generation approaches regard the possibility of creating multiple keys from the same biometrics without using any external data, and the stability of the resulting cryptographic key (Rua et al., 2012). Nevertheless, it is unfortunate that no significant endeavors have been formed to explore the possibility of employing human ear for individual recognition in spite of its remarkable role in forensic science. The ear is a fairly attractive biometric candidate fundamentally because of its (i) rich and steady configuration that is conserved since birth and is reasonably distinctive in individuals, (ii) being consistent with the modifications in appearance and facial expression, and (iii) comparatively invulnerable from anxiety, privacy, and hygiene issues with various other biometric candidates. It is pertinent to note that the human ear has emerged as a catalyst for various investigations in view of its individuality and distinctiveness (Kumar and Wu, 2012).

Biometric cryptosystems and cancelable biometrics are both practical and promising schemes to enhance the security and privacy of biometric systems (Leng and Zhang, 2011). In the event of a person's biometric getting compromised, his distinctiveness will be lost. Unlike passwords, biometric cannot be revoked. Hence, furnishing safety to the saved biometric template is extremely critical. The multi-biometric cryptosystems concurrently defend the two different templates of a user using a single secure sketch (Nagar et al., 2012). Crypto biometric systems are validation techniques which combine the concepts of cryptography and biometrics. Quantization Index Modulation (QIM) has to bind biometric characteristics with binary keys (Bui et al., 2010), providing an increased flexibility in managing the templates' intraclass variability. Fuzzy vault is a well-established crypto biometric construct, which is credited to the quality of safeguarding the biometric templates (Meenakshi and Padmavathi, 2009). Moreover, due to the difficulties in managing the intraclass variability of biometric data, the recognition performances of such schemes are typically significantly lower than those of their unprotected counterparts (Sutcu et al., 2009). Usually, for the fuzzy vault creation, joint feature vector is primarily created with the assistance of characteristic features (Sowkarthika and Radha, 2012). To create this collective feature vector, supplementary feature point named 'chaff points' is required. A non-organized group of points $R = X \cup C$ furnishes joint feature vector points, where X the unique feature point of the modalities and the points in C are called chaff points that are arbitrarily chosen from the characteristic feature points (Chang et al., 2006). This chaff point creation module is employed to create arbitrary noise points to conceal the biometric features that are gathered from the clients' biometric template. The extraction of a repeatable binary string from biometrics opens new possible applications, where a strong binding is required between a person and cryptographic operations (Hao et al., 2006). The blend of genuine and chaff points is called the secure fuzzy vault template which safeguards the biometric data as well as the crypto key. For a concurrent accomplishment of the bio-cryptosystem, which is a vital necessity for modern data safety mechanisms, the current technique of chaff generation is grossly insufficient (Khalil-Hani and Bakhteri, 2010). The relevant hassles in chaff point created are successfully tackled by giving shape to a new chaff point generation method, which employs an optimizing algorithm for the choice of the new chaff feature points.

The name of the optimization algorithm used in the proposed investigation is the unique PSO (Egrioglu and Ozdemir, 2014) algorithm. It is a heuristic comprehensive optimization technique introduced by Doctor Kennedy and Eberhart in 1995 (Meenakshi and Padmavathi, 2009). The algorithm imitates the social characters shown by swarms of animals. In the PSO algorithm, a point in the search space, which is a possible solution, is called a particle. The group of particles in a specific iteration is called 'swarm' (Onwunalu and Durlofsky, 2010). In the case of particle swam optimization algorithm, solution swam is linked to the bird swarm, the travel of birds from one location to another is parallel to the growth of the solution swarm and excellent data correspond to the most idealist remedy, and the food resource is akin to the most desirable solution during the entire track (Bai, 2010).

Thus, by means of similar algorithm, chaff feature points get optimized and developed new chaff points with highly protected fuzzy vault fusion. The rest of the paper is organized as follows: a brief review of some of the literature works in the multimodal biometric recognition is presented in Section 2. Section 3 explains the brief notes for the proposed methodology. The experimental results and performance analysis discussions are provided in Section 4. Finally, the conclusion is summed up in Section 5.

2. Literature review

A critical problem in the design of a cryptographic system is the vexed issue of key administration. A high-tech remedy to this hassle is to make use of bio-cryptosystems, wherein cryptography is blended with biometrics. In this remedy, the client biometrics are employed to safeguard the cryptographic key. A well-liked method to the blueprint of parallel bio-cryptosystems is the relevance of a fuzzy vault scheme. This self-styled vault is a safe treasure house in which the key is concealed within the biometric data jumbled with illogical chaff points. The utmost crucial function in the fuzzy vault scheme is a creation of the chaff points. A concise assessment of a parallel technique with face and ear biometrics is furnished below:

Multimodal biometric recognition of face and ear traits is analyzed initially. The habitual exclusion of local 3D features (L3DF) from ear and face biometrics and their arrangement at the feature and score levels for healthy recognition has been skillfully offered by Islam et al. (2013). The bouquet rightly reaches them for their relentless effort to introduce feature level fusion of 3D features extracted from ear and frontal face