PAPER ID: 17-04-0142

Security Enhancement of Dynamic Signature by Utilizing Local Features with Individual Threshold

Suryanti Awang[1], Nor Faradilla Mohamed Idris[1], Junaida Sulaiman[1]

[1] Soft Computing and Intelligent System (SPINT), Faculty of Computer Systems & Software Engineering, Universiti Malaysia Pahang, Lebuhraya Tun Razak, 26300, Kuantan, Pahang, Malaysia

Dynamic signature has potential to replace conventional signature in verifying an authorised person since it is legal and widely accepted by society. To date, most of the existing researches emphasise in obtaining a high performance of Genuine Acceptance Rate (GAR). However, at the same time, a high percentage of False Acceptance Rate (FAR) is achieved which indicates the verification system has a high-security vulnerability that exposes the signature being forged by an imposter. Therefore, this research aims to enhance the security level by fully utilising the advantages of all local features with the deployment of individual threshold in verifying a genuine signature. The features are based on time and strokes of the dynamic signature. The individual threshold is obtained during the training process to acquire an accurate verification setting for each signature to improve the performance of FAR. Subsequently, experiments are conducted using different classifiers including Neural Network (NN), Bayes Network and Linear Discriminant Analysis (LDA) and their outputs are measured using Genuine Acceptance Rate (GAR), False Rejection Rate (FRR) and False Acceptance Rate (FAR). The results showed that signature verification using individual threshold produced the highest GAR of 98.2%, the smallest FRR and FAR of 1.8% and 1.0% respectively, and outperformed the results with a common threshold. Thus, the proposed technique increased the security in signature verification with a lower error rate in FAR.

Keywords: Computational Intelligence, Dynamic Signature, Individual Threshold.

PAPER ID: 17-04-0147

Biometric Template Protection based on Hill Cipher Algorithm with Two Invertible keys

Emad Taha Khalaf [1], Muamer N. Mohammad [1,2], Kohbalan Moorthy[1,3] and Raed A. Hasan[1]

[1]Faculty of Computer Systems & Software Engineering, University Malaysia Pahang
[2]IBM Center of Excellence, University Malaysia Pahang, 26300Kuantan, Pahang, Malaysia
[3]Soft Computing & Intelligent System Research Group

The security of stored templates has become an important issue in biometric authentication systems this because most of the biometric attacks target the biometric database beside the difficulty of issuing the templates again. Thus, to protect the biometric templates it must be encrypted before storing in database. In this paper we proposed an efficient encryption method based on two invertible and random keys to enhance and overcome the weakness of hill cipher algorithm the keys generated using upper triangular matrices with Pseudo-Random Number Generator (PRNG) using two large and random encryption keys. The proposed encryption method provides sufficient security and protection for the biometric templates from attacks, where the experimental results showed high efficiency comparing with the traditional Hill Cipher and existing methods.

Keywords: Template Security, Hill Cipher, Modified Hill cipher, Involutory matrix, Computational Intelligence.