ABSTRACT

Biometrics are widely accepted as the most reliable proof of identity, entitlement to services, and for crime-related forensics. Using biometrics for remote authentication is becoming an essential requirement for the development of knowledge-based economy in the digital age. Ensuring security and integrity of the biometric data or templates is critical to the success of deployment especially because once the data compromised the whole authentication system is compromised with serious consequences for identity theft, fraud as well as loss of privacy. Protecting biometric data whether stored in databases or transmitted over an open network channel is a serious challenge and cryptography may not be the answer. The main premise of this thesis is that Digital Steganography can provide an alternative security solutions that can be exploited to deal with the biometric transmission problem.

The main objective of the thesis is to design, develop and test steganographic tools to support remote biometric authentication. We focus on investigating the selection of biometrics feature representations suitable for hiding in natural cover images and designing steganography systems that are specific for hiding such biometric data rather than being suitable for general purpose. The embedding schemes are expected to have high security characteristics resistant to several types of steganalysis tools and maintain accuracy of recognition post embedding. We shall limit our investigations to embedding face biometrics, but the same challenges and approaches should help in developing similar embedding schemes for other biometrics. To achieve this our investigations and proposals are done in different directions which explain in the rest of this section.

Reviewing the literature on the state-of-art in steganography has revealed a rich source of theoretical work and creative approaches that have helped generate a variety of embedding schemes as well as steganalysis tools but almost all focused on embedding random looking secrets. The review greatly helped in identifying the main challenges in the field and the main criteria for success in terms of difficult to reconcile requirements on embedding capacity, efficiency of embedding, robustness against steganalysis attacks, and stego image quality. On the biometrics front the review revealed another rich source of different face biometric feature vectors. The review helped shaping our primary objectives as (1) identifying a binarised face feature factor

with high discriminating power that is susceptible to embedding in images, (2) develop a special purpose content-based steganography schemes that can benefit from the well-defined structure of the face biometric data in the embedding procedure while preserving accuracy without leaking information about the source biometric data, and (3) conduct sufficient sets of experiments to test the performance of the developed schemes, highlight the advantages as well as limitations, if any, of the developed system with regards to the above mentioned criteria.

We argue that the well-known LBP histogram face biometric scheme satisfies the desired properties and we demonstrate that our new more efficient wavelet based versions called LBPH patterns is much more compact and has improved accuracy. In fact the wavelet version schemes reduce the number of features by 22% to 72% of the original version of LBP scheme guaranteeing better invisibility post embedding.

We shall then develop 2 steganographic schemes. The first is the LSB-witness is a general purpose scheme that avoids changing the LSB-plane guaranteeing robustness against targeted steganalysis tools, but establish the viability of using steganography for remote biometric-based recognition. However, it may modify the 2nd LSB of cover pixels as a witness for the presence of the secret bits in the 1st LSB and thereby has some disadvantages with regards to the stego image quality.

Our search for a new scheme that exploits the structure of the secret face LBPH patterns for improved stego image quality has led to the development of the first *content-based* steganography scheme. Embedding is guided by searching for similarities between the LBPH patterns and the structure of the cover image LSB bit-planes partitioned into 8-bit or 4-bit patterns. We shall demonstrate the excellent benefits of using content-based embedding scheme in terms of improved stego image quality, greatly reduced payload, reduced lower bound on optimal embedding efficiency, robustness against all targeted steganalysis tools. Unfortunately our scheme was not robust against the blind or universal SRM steganalysis tool. However we demonstrated robustness against SRM at low payload when our scheme was modified by restricting embedding to edge and textured pixels. The low payload in this case is sufficient to embed a secret full face LBPH patterns.

Our work opens new exciting opportunities to build successful real applications of content-based steganography and presents plenty of research challenges.