Hiding Fingerprint in Face using Scattered LSB Embedding Steganographic Technique for Smart card based Authentication system

S.Brindha
Senior Lecturer, Computer Networking, PSG Polytechnic College, Coimbatore, India

Ila.Vennila
Associate Professor, Electrical & Electronics Department, PSG College of Technology, Coimbatore, India

ABSTRACT
Smart card technology is currently recognized as the most appropriate technology for identity applications that must meet critical security requirements. Smart cards provide the secure, convenient and cost-effective ID technology that stores the enrolled biometric template and compares it to the "live" biometric template. In order to protect biometric data, Steganography using scattered *Least Significant Bit (LSB)* embedding algorithm is suggested, which embeds bits in the LSB position in a *non linear fashion* inside an image. As an improvement, prior to embedding, the *bits are encrypted and then embedded*. Steganography and Cryptography coined together will aid to protect the biometric data and thereby provide secrecy and avoid loss of privacy.

General Terms
Biometrics, Security, Smart card, Steganography

Keywords
Hiding Fingerprint, LSB Steganography, Authentication

1. INTRODUCTION
In view of the recent increase of incidents over the Internet and other networks, the role of authentication techniques to prevent unauthorized access by malicious users becomes more significant. Due to the growing importance of security technology and the necessity of the protection and access restriction, reliable personal identification and authentication is necessary.

The emergence of Biometric authentication systems has proven to be a viable practical alternative to address the problems in conventional methods. Biometrics refers to the automatic identification (or verification) of an individual (or a claimed identity) by using certain physiological or behavioral traits associated with the person. Biometric systems make use of fingerprints, hand geometry, iris, retina, face, hand vein, facial thermograms, signature, voiceprint, gait, palm print, etc. to establish a person's identity.

Biometrics relies on who you are—on one of any number of unique characteristics that you can't lose or forget. A biometric system authenticates its users in conjunction with a smart card, username or ID number. The biometric template captured is compared with that stored against the registered user either on a smart card (Fig. 1) or database for verification.

Fig. 1 Smart card for driving license

2. SMART CARD TECHNOLOGY
Smart card has gone several development phases during the years. Today it is a credit-card-sized card equipped with microprocessor and memory. It is a portable and an intelligent device capable of manipulating and storing data. It is inserted into a reader as part of the authentication process. They often contain a digital certificate and they are usually presented in a combination with a knowledge factor such as password or a personal identification number (PIN). In biometric process, there are three types of smart card based on their typical technical features and type of authentication they support. The three types of smart card as in literature [2] are :

- Template-on-card (TOC)
- Match-on-card (MOC)
- System-on-card (SOC)

In TOC, original identifying biometric template is stored on a smart card. Data acquisition, feature extraction and matching are done on the reader side. During the authentication process, the reading device requests the identifying template from the smart card and matches it on the reader side with newly scanned template.

In MOC, original template is stored on a smart card. During the authentication process, data acquisition and feature extraction are done at the reader side and the matching is done inside the smart card. The final matching result is computed inside the smart card itself.

In SOC version, smart card incorporates original template, the entire biometric sensor, processor and algorithm. All authentication procedures are done inside the smart card itself. Adding individuals' unique characteristics into smart card chip, smart card becomes more secure medium, suitable for use in a wide range of applications that support biometric methods of identification.

There are numerous ID systems implemented worldwide based on biometric smart card and biometric technology. For example: US Department of Defense Common Access Card, Malaysia's national ID multipurpose card, UK's Asylum Seekers Card – contain photo for visual recognition and fingerprint template stored on smartcard chip for biometric identification [2].

Fig. 2 Biometric Smart card Application

As shown in Figure 2, smart card systems embedded with biometric data such as fingerprint have enabled more reliable applications such as home entertainment, personal identification and prepayment service. Smart cards can be used as a single, portable identity token for a wide range of personalized security services within business and government organizations. They support contact and contact-less communication interfaces and multiple identification, authentication and authorization methods, including single key, one time passwords (OTP), digital certificates (PKI), and biometrics. Applications include visual identification, physical access control, computer logon, remote network access, email and data encryption, digital signature, and canteen and vending machine payments. In addition to strengthening security throughout the organization, smart cards provide convenience to users and administrators with significant cost savings through consolidation of security services using a single identity credential.

3. FINGERPRINT BIOMETRICS

Biometric authentication uses data taken from measurements of a person's body, such as fingerprints, faces, irises, retinal patterns, palm prints, voice prints, hand-written signatures and so on, to identify individuals by means of image processing [3]. Such data is unique to the individual and remains throughout one's life. It is important to have reliable personal identification due to growing importance of information technology. Of all the biometric techniques being used today, fingerprint-based identification is the oldest method, which has been successfully used in numerous applications. Everyone is known to possess a unique fingerprint and it does not change throughout his lifetime and so the fingerprint matching is considered one of the most reliable techniques of people identification.

Fingerprint recognition derives a unique template from the attributes of the fingerprint without storing the image itself or even allowing for its reconstruction. Fingerprints basically consist of ridges (raised skin) and furrows (lowered skin) that twist to form a distinct pattern. When an inked imprint of a finger is made, the impression created is of the ridges while the furrows are the uninked areas between the ridges. [4] Although the manner in which the ridges flow is distinctive, other characteristics of the fingerprint called *'minutiae'* are what is most unique to the individual (See Fig.3 for minutiae representation). These features are particular patterns consisting of terminations or bifurcations of the ridges.

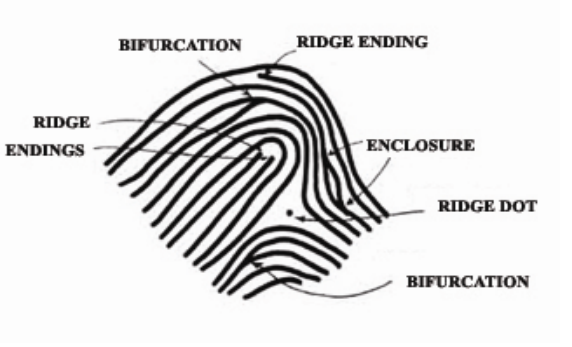


Fig. 3 Minutiae

Fingerprint is chosen as it is more mature in terms of the algorithm availability while other biometrics such as face recognition may not be well suited to an ordinary smart card processor. Fingerprint identification is suitable as a method to authenticate users to use a smart card. This can elaborate by using two factors: space complexity and time complexity. A common available smart card has approximately 8K to 16K of non-volatile memory. The current state-of-art fingerprint technology shows that the minimum size of a fingerprint template adequate for comparison can be as small as several hundreds of bytes. So space complexity is not a major problem as the smart card can store the entire fingerprint template. For time complexity, it refers to whether the in-card processor is capable to accomplish the entire fingerprint matching calculation in real time.

4. STEGANOGRAPHY

Steganography is the art of hiding a message signal in a host signal, such as audio, video, still images and text document without any imperceptible distortion of the host signal. While cryptography is about protecting the content of messages, steganography is about concealing their very existence. By using steganography, you can embed a secret message inside a piece of unsuspicious information and send it without noticing the existence of the secret message.

In image steganography [5], the information is hidden exclusively in an image which is called the cover image. After embedding the secret message, the cover image is called the stego-image. To be a useful steganography system, it must

provide a method to embed data imperceptibly, and the secret message must be able to convey the meaning after extraction. The basic idea of image data hiding is to hide the secret image under the camouflage of the cover-image. There are, in general, two approaches that can be used for image data hiding.

One approach is the spatial domain techniques and the second approach is the transform domain techniques. Spatial domain techniques usually embed the bits of the message directly into the least significant bits (LSBs) of the pixels of the cover image. LSB encoding is the simplest steganographic techniques, but the stego-image is sensitive, and not robust to operations such as blurring, cropping, lossy compression, and addition of noise.

The second type of method, the frequency domain method, is based on the embedding in the coefficient in the frequency domain (i.e., Discrete Cosine Transformation (DCT), Discrete Wavelet Transformation (DWT)). This type of technique is more robust with regard to common image processing operations and lossy compression. Another type of method is that of adaptive Steganography which adapts the message embedding technique to the actual content and features of the image.

4.1 Data Hiding and Encryption

In this paper we propose a biometric application which stores and verifies users' fingerprint information directly on the smart card for added security. The fingerprint information never leaves the card and is never stored in a database, thus protecting users' digital identities. Privacy issues and security risks associated with other biometric authentication methods are mitigated because the fingerprint credentials are stored and validated on the smart card which is constantly in the user's possession.

Each steganographic communication system consists of an embedding algorithm [6] and an extraction algorithm. To accommodate a secret message, the original image, also called the cover-image, is slightly modified by the embedding algorithm. As a result, the stego-image is obtained.

In order to illustrate how image embedding works, a very simple method, known as least significant bit (LSB) substitution is used. It consists of the extraction of the LSB and its replacement by the information that you want to hide. It is interesting to observe the noisy aspect of the lower bits, and their small contribution to the final luminance. For gray-scale images encoded at 8 bits per pixel, the luminance (I), of each pixel can be represented in terms of bits (b) as in Eqn.(1) :

$$I = b_7 * 2^7 + b_6 * 2^6 + b_5 * 2^5 + b_4 * 2^4 + b_3 * 2^3 + b_2 * 2^2 + b_1 * 2^1 + b_0 \quad (1)$$

and the LSB 'b_0' can be replaced without altering significantly the image quality. The difference between the new values and the old ones is very small, so it is difficult, if not impossible, for the human eye to identify any difference from the original picture.

The classic LSB steganography embeds message into cover medium by using message bit stream to replace the cover medium's least-significant bit (LSB) sequentially. A major goal in image steganography is to preserve the statistical properties of the host image to thwart statistical based steganalysis. However, LSB steganography methods [7] introduce some distortions into the host signal's statistical properties that have been used, as a certain indication of manipulation of the signal, by steganalysis algorithms. In order to overcome such a methodical vulnerability, in this paper we propose a technique which performs scattered LSB embedding to preserve histogram of the host signal.

4.2 Embedding Process

1. Read image file
2. Get fingerprint image to be hidden
3. Obtain password from user
4. Encrypt the fingerprint image
5. Generate pseudo random number based on password to calculate the LSB's to hide image.
6. Hide the fingerprint in the cover image
7. Resulting image is the stego image.

4.3 Retrieving Process

1. Read stego image
2. Obtain password from user
3. Generate pseudo random number based on password to calculate the LSB's where fingerprint is hidden.
4. Retrieve the fingerprint image
5. Decrypt the fingerprint image
6. Resulting image is the original image.

The above process is illustrated in Fig. 4.

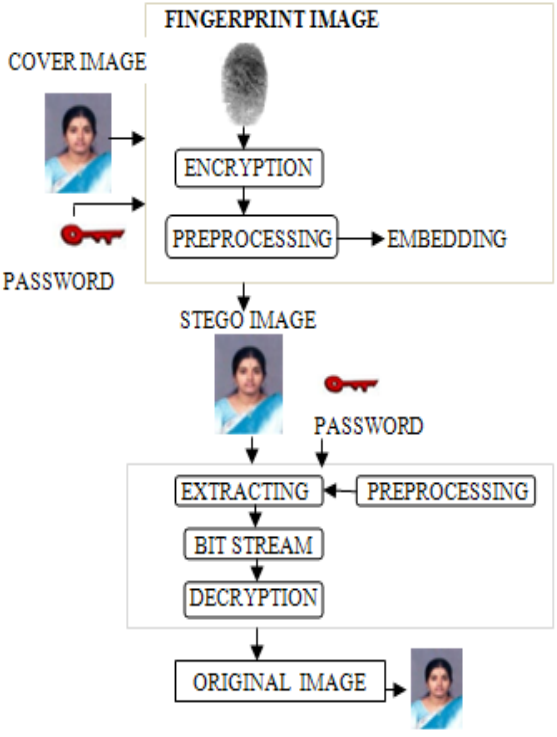


Fig. 4 Steganography process

5. IMPLEMENTATION

The cover images used are 24 bit colour images .The fingerprint images to be hidden are taken from FVC2004database. The header (containing information for the hidden file, such as its size and filename) and the fingerprint image to be hidden are *encrypted with an encryption algorithm* , using the password given, before being written in the picture. . The fingerprint image bits are not written in a linear fashion; instead, a *pseudo-random number generator (PRNG)* is used to choose the place to write each bit. The values given by the pseudo-random number generator depend on the password, so it is not possible for someone trying to read the secret data to get the hidden file (not even the encrypted version) without knowing the password[8]. The sample images used are as shown in Fig 5.

Fig.5.Sample cover, fingerprint and stego images

This final image can be stored in smart cards and during authentication, the fingerprint will be extracted from the cover image. The cover image can be the photo of the person, so it will provide visual authentication [9] also.

6. RESULTS

6.1 PSNR value

PSNR is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of a logarithmic decibel scale.

A higher PSNR value indicates that the reconstruction is of higher quality. Typical values for the PSNR in a lossy image and video compression are between 30 and 50dB, where higher is better. Acceptable values for wireless transmission quality loss are considered to be about 20dB to 25dB.PSNR is most commonly used as a measure of quality of reconstruction of lossy compression codecs. The signal in this case is the original data, and the noise is the error due to hiding. The PSNR value is calculated by Eqn. (2)

$$PSNR(dB) = 10 * \log\left(\frac{255^2}{MSE}\right) \qquad (2)$$

where MSE: Mean-Square error and is given by Eqn.3.

$$MSE = \sum_{i=1}^{x}\sum_{j=1}^{y}\frac{(|A_{ij}-B_{ij}|)^2}{x*y} \qquad (3)$$

where x: width of image.
y: height.
x*y: number of pixels

The PSNR value was calculated for original and stego images and the results are as shown in Fig. 5.

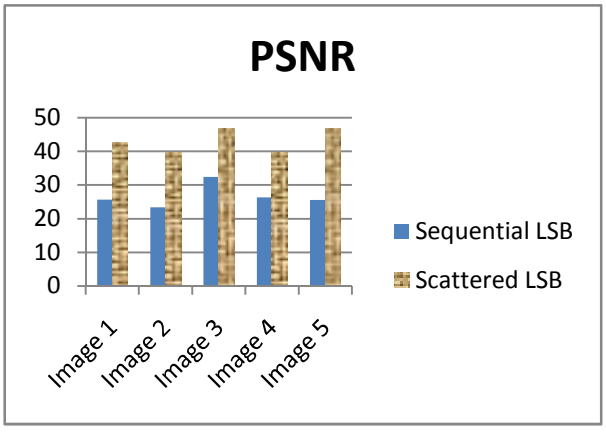


Fig.6. PSNR value

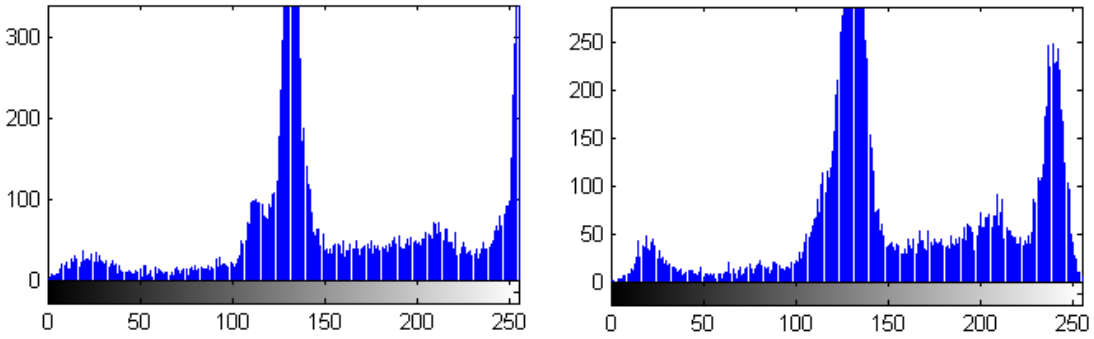
As shown in Fig 6. The PSNR value for Scattered LSB embedding is higher than Sequential LSB embedding.

6.2. Histogram analysis

The image histogram is computed for the original image and stego image and it is shown in Fig. 7. The histograms of both the images are quite similar when compared to the ordinary LSB embedding wherein the histograms show great difference as shown in Fig. 8. Hence the proposed technique is found to withstand statistical attacks based on histogram analysis.

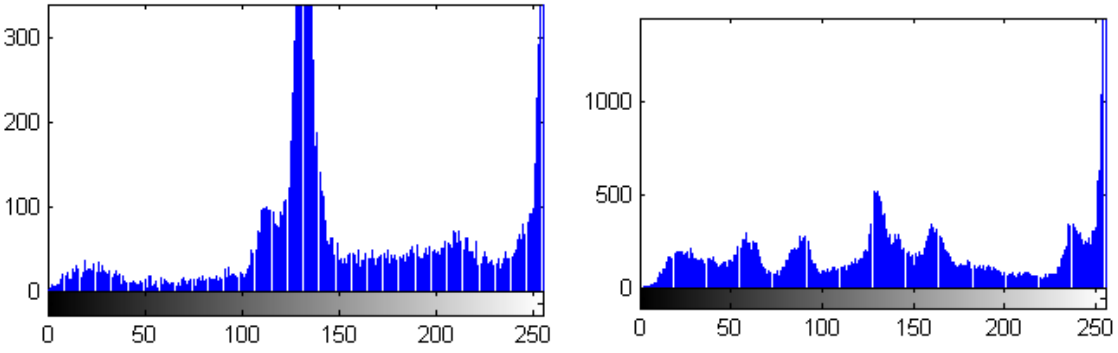
7. CONCLUSION

With the wide spread utilization of fingerprint based smart card identification systems, establishing the authenticity of biometric data itself has emerged as an important research issue. In this paper, a method based on Steganography has been suggested to protect the template. Two techniques, namely encryption and PRNG based embedding are used in LSB embedding to enhance its security. The performance of the proposed scattered LSB embedding technique is compared with that of sequential embedding and is found to be superior in terms of PSNR value and histogram plot.



Cover image **Stego image**

Fig. 7 Histogram- Scattered LSB embedding



Cover image **Stego image**

Fig.8 Histogram-Sequential LSB embedding

8. REFERENCES

[1] Lu, H.K.; Ali, A.M.; Durand, S.; Castillo, L.; ,"A New Secure Communication Framework for Smart Cards," Consumer Communications and Networking Conference, 2009.

[2] M.R.M.; Yahaya, Y.H.; Halip, M.H.M.; Khairuddin, M.A.; Maskat, K.;, "The design of fingerprint biometric authentication on smart card for PULAPOT main entrance system," Information Technology (ITSim), 2010 International Symposium in , vol.3, no., pp.1-4, 15-17 June 2010

[3] K. I. Chang, K. W. Bowyer, and P. J. Flynn. An Evaluation of Multimodal 2D+3D Face Biometrics. IEEE Transactions on Pattern Analysis and Machine Intelligence,27(4):619–624,April 2005

[4] Jain, A.K.; Jianjiang Feng; , "Latent Fingerprint Matching," Pattern Analysis and Machine Intelligence, IEEE Transactions on , vol.33, no.1, pp.88-100, Jan. 2011

[5] Weiqi Luo; Fangjun Huang; Jiwu Huang; , "Edge Adaptive Image Steganography Based on LSB Matching Revisited," Information Forensics and Security, IEEE Transactions on , vol.5, no.2, pp.201-214, June 2010.

[6] Yuhanim Hani Binti Yahaya, Mohd Rizal Bin Mohd Isa, "Fingerprint Biometrics Authentication on Smart Card", Second International Conference on Computer and Electrical Engineering, 2009.

[7] Huang, F.; Luo, W.; Huang, J.; , "Steganalysis of JPEG steganography with complementary embedding strategy," Information Security, IET , vol.5, no.1, pp.10-18, March 2011

[8] Xinyi Huang; Yang Xiang; Chonka, A.; Jianying Zhou; Deng, R.H.; , "A Generic Framework for Three-Factor Authentication: Preserving Security and Privacy in Distributed Systems," Parallel and Distributed Systems, IEEE Transactions on , vol.22, no.8, pp.1390-1397, Aug. 2011

[9] Mathew, Harlay Maria; Raj, S. Benson Edwin; Gundapu, Pandit Samuel J; Angeline, S Jeeva Flora; , "An improved three-factor authentication scheme using smart card with biometric privacy protection," Electronics Computer Technology (ICECT), 2011 3rd International Conference on , vol.3, no., pp.220-223, 8-10 April 2011