Journal of Engineering and Applied Sciences 12 (Special Issue 8): 8421-8425, 2017
ISSN: 1816-949X

A Novel Method for Enhancing Biometric Systems Security Using Watermarking

[1]S. Balaji, M. Janga Reddy and [2]Habibullah Khan
[1]CMR Institute of Technology, Hyderabad, India
[2]KL (Deemed to be University), Guntur, India

Abstract: In order to identify an individual, biometric systems are extensively used in India. Recently JNT University, Hyderabad has introduced finger print Biometric system for all faculty working in various private engineering colleges in Telangana. Every day the faculty have to record their biometric attendance in the college, so that, it will be recorded in the server of JNTU, Hyderabad. In this way, the university will have a way to monitor the faculty who are really working in private Engineering college, so that, they can identify the presence of real faculty members. However, the system is vulnerable to various kinds of attacks. In this study, we introduce a novel method for enhancing security of biometric systems by combining watermark with the fingerprint system. Two spatial domain watermarking methods for fingerprint images are proposed in this. The first method utilizes gradient orientation analysis in watermark embedding, so that, the watermarking process alters none of the features extracted using gradient information. The second method preserves the singular points in the fingerprint image which in turn preserves the classification of the watermarked fingerprint image (e.g., into arch, left loop classes). In both methods, watermark data consisted of 154 bits corresponding to the 7 bit ASCII code of string fingerprint watermark.

Key words: Biometrics, watermark, steganography, data embedding, JNTUH, fingerprint

INTRODUCTION

To begin with the meaning of "watermark" (on a paper) is a mark that is not traceable to the naked eye in ordinary conditions but is visible when paying attention through a unique light. A digital water marked signal is also not easy to discriminate from the original signal normal conditions. In fact, there should be no noticeable distinction between the original signal and watermarked signal. The wish to communicate secretly is a human trait that dates back to the old times. This led to the discovery of steganography at first and encryption at a later stage. Before the origin of watermarking technique there were two methods called "steganography" and "encryption" (Chen *et al*., 2007**)**.

Watermarking is defined as the put into practice of altering a job to insert a message about that work. Embedding a digital signal (audio, video or image) with information which cannot be removed simply is called digital watermarking. Figure 1 shows different methods of protection of template of biometrics.

Watermarking is the straight embedding of additional data into the original content or host signal (Ferri *et al*., 2002). Preferably, there should be no detectable difference between the watermarked and unique signal and the watermark should be not easy to remove or alter without damaging the host signal. In some cases, the amount of information that can be concealed and detect reliably is important. It is easy to see that the necessities of imperceptibility, toughness and capacity clash with each other. For instance, a simple way to provide an barely visible watermark is to embed the watermark signal into the perceptually unimportant portion of the host data. However, this makes the watermark susceptible to attack because it is fairly easy to eradicate or alter the watermark without affecting the host signal. To provide a strong watermark, a good plan is to embed the watermark signal into the significant portion of the host signal. This portion of the host data is highly sensitive to modifications, however and may produce very audible or visible noise in the host data. Applications for digital watermarking comprise copyright security, fingerprinting,

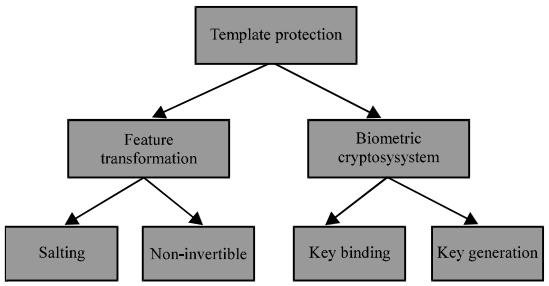

Fig. 1: Categorization of template protection scheme

Corresponding Author: S. Balaji, CMR Institute of Technology, Hyderabad, India

authentication, copy control, tamper finding and information hiding applications such as broadcast monitor. Although, these biometrics have been widely used in security systems, they have some limitations. First, biometrics are noisy by nature, restrictions of acquisition technology or environmental conditions but cryptographic keys are demanded to be correct (Clancy *et al*., 2003).

Watermarking can fundamentally be categorized into visible and invisible watermarking. Visible watermarking apparently includes practice of logos, trademarks and other interrelated things for exclusive identification (Chang and Roy, 2007). Invisible watermarking is classified basing on the ability to endure attacks into strong and delicate watermarking. Delicate watermark is capable of detecting any tiny transformation made to the watermarked content of the host signal. It is easy to embed this into the signal. This can be proficient by accommodating it in the insignificant portions of the original data (Connie *et al*., 2005).

Digital watermarking is such a multidisciplinary field that combines principles from communications, signal processing and cryptography (the study of secret writing). Therefore, all the techniques developed for the above disciplines can be applied but one must take into account that the noise is often not Gaussian which an assumption commonly is made in a communication channel problem.

All digital watermarking techniques have common procedures or schemes. They are 'insertion' and 'extraction' of watermarks. For the case of robust watermarks there is also 'detection' of watermarks.

In watermark insertion the input image, user key and the watermark are combined using various techniques discussed in the next section to produce watermarked image.

To determine either authenticity or copyright ownership of the watermarked object, the user key and the watermarked object are combined in the process or either watermark extraction which recovers and/or verifies the watermark.

Depending on whether the original image is used for the watermark extraction process, the process of watermark extraction can be divided into 2 types. They are Non-blind decoding or extraction of watermark, Blind decoding or extraction of watermark. Non-blind decoding or extraction of the watermark refers to a situation where extraction is accomplished with the aid of the original, non marked image. In spite of the benefits it gives in terms of robustness, non-blind decoding is not desirable in many applications where the availability of the original data cannot be granted. In blind decoding, the decoder does not need the original image or any information derived from it to recover the watermark (IBG, 2013). In picture watermarking, the watermark indication is either fixed into the spatial domain representation of the image or one of many transform domain representations such as DCT, fourier and wavelet. It is generally argued that embedding watermarks in transform domains provides better robustness against attacks and leads to less perceptibility of an embedded watermark due to the spread of the watermark signal over many spatial frequencies and better modeling of the Human Visual System (HVS) when using transform coefficients. An example of watermarking in the spatial domain is given in Fig. 2. Amplitude modulation is applied to the blue channel pixels to embed the 32 bit watermark data, represented in decimal form as 1234567890. This is a strong watermarking scheme: the watermark data can be retrieved correctly even after the watermarked image is modified. For example, the embedded data 1234567890 is retrieved after the watermarked image is blurred via. filtering the image pixels with a 5×5 structuring element and compressed (via. JPEG algorithm with a quality factor of 75) and decompressed.

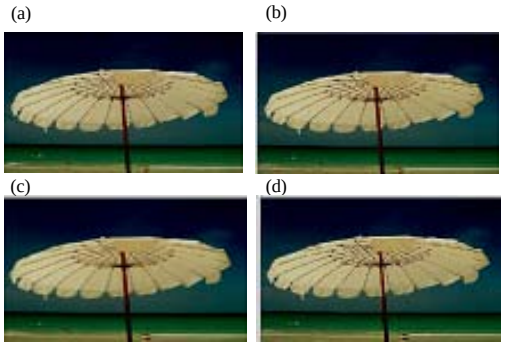

Fig. 2: Image watermarking; a) Original image (640×480, 24 bpp; b) Water-marked image carrying the data 1234567890; c) Image blurred after watermarking and d) Image JPEG compressed-decompressed after watermark

Specific classes of watermarks, called delicate watermarks are typically used for authenticating multimedia data. Unlike robust watermarks, any attack on the image invalidates the delicate watermark present in the image and helps in detecting/identifying any tampering of the image. Hence, a delicate watermarking scheme may need to possess the following features: detecting tampering with high probability, being perceptually transparent not requiring the original image at decoding site and locating and characterizing modifications to the image (Chora, 2007). Typical delicate image watermarking

techniques embed the watermark in the least significant bit planes of an image. To increase their security, several variants such as embedding image hash values have been proposed.

An example of fragile image watermarking is given. The tampering of the watermarked image is identified via. the change in the regular structure of the decoded watermark image.

FINGERPRINT WATERMARKING SYSTEMS

A data hiding technique which is related to fingerprint images compacted with the WSQ (Wavelet Scalar Quantization) wavelet-based scheme. The discrete wavelet transform coefficients are distorted during WSQ encoding by intriguing into contemplation possible image deprivation. The image obtained after the data embedding-compressing-decompressing series. The input image was obtained with an optical sensor. The compression proportion was set to 10.7:1 and the embedded information (randomly generated bits) size was almost 160 bytes. As seen from the image feature does not suffer drastically due to data embedding, even though the data size is significant. A spatial watermark image is set in in the spatial field of a fingerprint image by utilizing a authentication key (Chen *et al*., 2005). Their technique can localize any region of image that has been tampered after it is watermarked; consequently, it can be used to check reliability of the fingerprints.

ARCHITECTURE OF THE PROPOSED SYSTEM

We investigate the effects of watermarking fingerprint images on the recognition and retrieval accuracy using a proposed invisible fragile watermarking technique for image verification applications on a specific fingerprint recognition system.

A function setting is considered in this. The essential data hiding method is the same but it differs in the uniqueness of the embedded data, the host image moving that data and the medium of data transfer (Gunsel *et al*., 2002). While fingerprint characteristic vector is used as embedded data, other information such as user name (e.g., \Johnny"), user identification number (\12345′) or authorizing foundation (\CMR") can also be concealed into the images as shown in Fig. 3-5. Figure 6 involves a steganography-based function the biometric data (fingerprint minutiae) that need to be transmitted (possibly via. a non-secure communication channel) are concealed in a host (also called cover or carrier) image, whose only function is to carry the information. For example, the fingerprint minutiae may need to be transmitted from a regulation enforcement agency to a

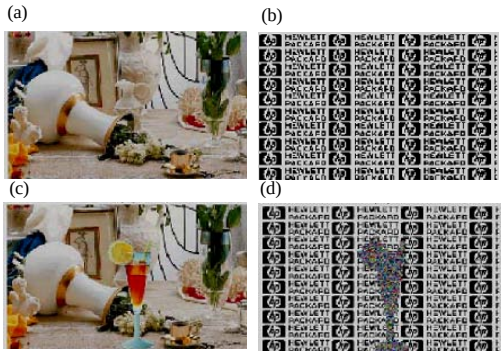

Fig. 3: Fragile image watermarking; a) Watermarked image; b) Watermark image decoded from the image; c) Altered image addition of the glass object and d) Watermark image decoded from the altered image

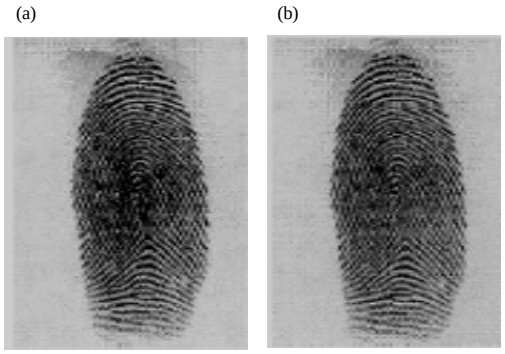

Fig. 4: Compressed-domain fingerprint watermarking; a) Input finger print and b) Data embedded compressed decompressed fingerprint

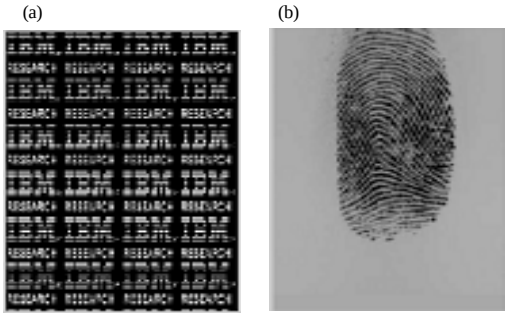

Fig. 5: Fragile print watermarking; a) Watermark image and b) Finger print image carrying the image

template database or vice versa (Uludag and Jain, 2014). In Fig. 7, we present a fingerprint watermarking system which involves communication channel, the security of the system is based on the privacy of the communication. The host image is not related to the concealed data in

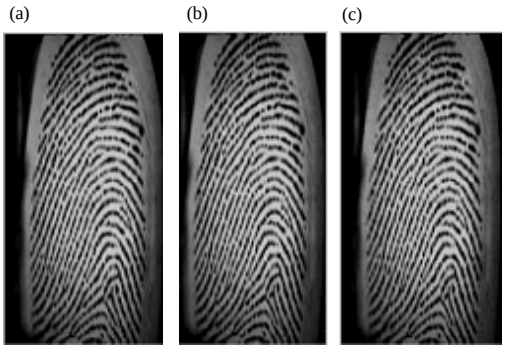

Fig. 6: Fingerprint watermarking results for; a) Input fingerprint; b) Fingerprint image watermarked using gradient orientation and c) Fingerprint image watermarked using singular points

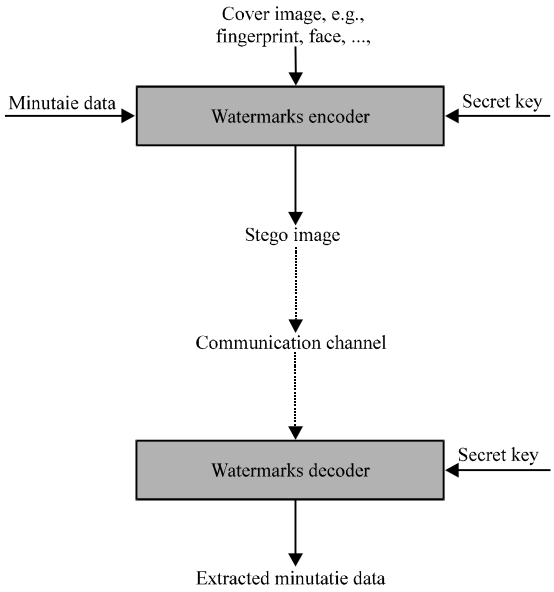

Fig. 7: Block diagram of fingerprint watermark system

any way. As a result, the host image can be any image available to the encoder. Along with the fingerprint matching, the proposed scheme will also extract the face information hidden in the fingerprint image. The recovered face will be used as a second source of authentication either automatically or by a human in a supervised biometric application. In this scenario one biometric (e.g., face) is embedded into another (e.g., fingerprint) in order to increase the protection of the latter.

CONCLUSION

The capability of biometrics-based individual identification techniques to discriminate between an certified person and an impostor who deceitfully acquires the access opportunity of an approved person is one of the main reasons for their reputation compared to traditional identification techniques. However, the protection and integrity of the biometric data itself raise significant issues which can be ameliorated using encryption, watermarking or steganography. In totaling to watermarking, encryption can also be used in order to additional boost the security of biometrics data. The purpose was related to escalating the security of biometric data exchange which was based on steganography. The information was concealed in such a way that the features that were used in fingerprint matching were not drastically changed during programming and decoding. As a result, the verification precision based on decoded watermarked images was very alike to that with original images. For applications where the watermarked images need to be processed by individual (e.g., manual fingerprint matching), the planned technique utilizes several properties of the human visual system to keep the visibility of the modifications to the host images small. In addition, the proposed scheme can be attached with a delicate watermarking scheme to detect illegal alteration of the watermarked templates.

REFERENCES

Chang, E.C. and S. Roy, 2007. Robust extraction of secret bits from minutiae. Proceedings of the International Conference on Biometrics, August 27-29, 2007, Springer, Berlin, Germany, pp: 750-759.

Chen, H., H. Sun and K.Y. Lam, 2007. Key management using biometrics. Proceedings of the 1st International Symposium Data, Privacy and E-Commerce (ISDPE07), November 1-3, 2007, IEEE, Chengdu, Sichuan, China, ISBN:0-7695-3016-8, pp: 321-326.

Chen, Y., S.C. Dass and A.K. Jain, 2005. Fingerprint quality indices for predicting authentication performance. Proceedings of the 5th International Conference on Audio and Video-Based Biometric Person Authentication, July 20-22, 2005, New York, USA., pp: 160-170.

Chora, M., 2007. Emerging methods of biometrics human identification. Proceedings of the 2nd International Conference on Innovative Computing, Information and Control (ICICIC'07), September 5-7, 2007, IEEE, Kumamoto, Japan, ISBN:0-7695-2882-1, pp: 365-365.

Clancy, T.C., N. Kiyavash and D.J. Lin, 2003. Secure smartcardbased fingerprint authentication. Proceedings of the 2003 ACM SIGMM Workshop on Biometrics Methods and Applications, November 8, 2003, ACM, Berkley, California, ISBN:1-58113-779-6, pp: 45-52.

Connie, T., A. Teoh, M. Goh and D. Ngo, 2005. PalmHashing: A novel approach for cancelable biometrics. Inform., Process., Lett., 93: 1-5.

Ferri, L.C., A. Mayerhoefer, M. Frank, C. Vielhauer and R. Steinmetz, 2002. Biometric authentication for ID cards with hologram watermarks. Proceedings of the International Conference Security and Watermarking of Multimedia Contents, April 29, 2002, SPIE, San Jose, California, pp: 629-640.

Gunsel, B., U. Uludag and A.M. Tekalp, 2002. Robust watermarking of fingerprint images. Pattern Recognit., 35: 2739-2747.

IBG., 2013. The henry classification system. International Biometric Group, New York, USA.

Uludag, U. and A.K. Jain, 2014. Attacks on biometric systems: A case study in fingerprints. Master Thesis, Michigan State University Computer Science and Engineering, East Lansing, Michigan.