Chapter 9
Using Statistical Texture Analysis for Medical Image Tamper Proofing

Samia Boucherkha
Mentouri University, Algeria

Mohamed Benmohamed
Mentouri University, Algeria

ABSTRACT

This chapter discusses an approach for both authentication of medical images and confidentiality for the related textual data in an online medical application paradigm. The image authentication is achieved in a soft manner through a feature-based digital signature while the confidentiality of the related patient information is achieved through reversible data hiding. The selected features are robust towards geometric transformations, while fragile towards texture alterations that are characteristic of medical images. The processing scheme is done in a block by block basis to permit the localization of tampered image's regions. The effectiveness of the scheme, proven through experiments on a sample of medical images, enables us to argue that implementing mechanisms lying on this approach will help to maintain personal patient privacy and medical image integrity.

INTRODUCTION

Advanced computer based medical equipment is nowadays widely used in management of disease. Image processing technology is often used in computer based medical applications; the images are processed, stored, or transferred to a distant location over Internet or local networks. The resulting processed images can then be made available with patient information to medical researchers, second opinion physicians, students, and social security institutions. In such medical applications, the protection of the integrity and confidentiality of healthcare records is a critical issue.

Indeed, manipulation of medical images might lead to wrong interpretation and false diagnosis while the secrecy of the related patient information is imposed by the legal and ethic considerations, since patient data are very personal, and therefore, sensitive. The risks of unauthorized manipulation and misappropriation are increased when dealing with an open environment. So, before patient records can be distributed online, it is necessary to integrate in the medical application, mechanisms that maintain personal privacy and data integrity.

Encryption is a widely used technology to ensure several security services such as confidentiality, integrity, source authentication, and non-repudiation. The issues concerning medical applications are source authentication, non-repudiation, and integrity (Coatrieux, Maitre, Sankur, Rolland, & Collorec, 2001).

Source authentication is required to verify if the doctor who is claiming to have sent the record has actually sent it; Non-repudiation ensures that the doctor who sent the record cannot claim that he did not, while integrity will verify that the received record is exactly the same as the one sent and has not been modified by unauthorized people. Besides this, confidentiality of patient information is highly mandatory.

The traditional methods used for data authentication are digital signature (DS) (Stallings, 2003). To obtain the DS of an image, the digest of this latter is computed using a one-way hash function, then encrypted with the private key of a public-key cryptosystem. At the receiver's side, the DS is decrypted with the sender's public key, and again the image's digest is computed with the same hash function, then compared to the received one. Thanks to public-key cryptography, the resulting scheme ensures source authentication, non-repudiation, and integrity services.

Given the one-way characteristics of the hash function, it is unlikely that two different images will have the same digest, and even if a single bit changes, the DS may be totally different. This property may be convenient for text messages, but it does not offer the flexibility often asked with digital images. In fact, many image applications may tolerate more or less manipulations, such as format conversion, moderate level of filtering, and contrast adjusting without suffering from content changing. Thus, the image will be improperly categorized as inauthentic by the previous hash-based mechanism. In this case, an authentication procedure that uses some special-purpose functions to extract essential image invariant features and aims at authenticating the semantic content of images, in place of the hash digest is more convenient. As a result, the process can distinguish content-preserving manipulations such as filtering, compression, and scaling from content-changing manipulations such as cropping, objects addition, deletion, and modification. This way to proceed is generally referred to as features-based digital signature and leads to a more "soft" authentication. The current literature includes many of such authentication techniques which features are based on color, intensities, edges, or shapes (Bas, Chassery, & Macq, 2002; Li, Lou, & Chen, 2000; Thiemert, Sahbi, & Steinebach, 2005). The obtained DS may be appended to the transmitted image file, or alternatively embedded in the image itself via data hiding.

Data hiding is an emerging technology that enables the insertion of secret information invisibly throughout the image without degrading its visual quality. This technique takes advantage of the fact that digital images contain a lot of redundant information due to large spatial correlations, so some of this redundancy could be replaced by the secret information without perceptually changing the appearance of the image. A useful data hiding technique should be robust against malicious attacks to remove the embedded information and should not greatly affect the quality of the original image.

Data hiding has been adapted to medical imagery to connect visual and related textual data by several authors (Acharya, Anand, Bhat, & Niranjan, 2001; Boucherkha & Benmohamed,