Strict Authentication Watermaking with Jpeg Compression (SAW-JPEG)

JASNI MOHD ZAIN

ABSTRACT

This paper addresses authenticity and integrity of medical images using watermarking. Hospital Information Systems (HIS), Radiology Information Systems (RIS) and Picture Archiving and Communication Systems (PACS) now form the information infrastructure for today's healthcare as these provide new ways to store, access and distribute medical data that also involve some security risk. Watermarking can be seen as an additional tool for security measures. As the medical tradition is very strict with the quality of biomedical images, the watermarking method must be reversible or if not, region of Interest (ROI) needs to be defined and left intact. Watermarking should also serve as an integrity control and should be able to authenticate the medical image. Strict Authentication Watermarking with JPEG Compression (SAW-JPEG) embeds the digital signature of the image in the ROI and the image can be reverted back to its original value bit by bit if required and is able to survive some degree of JPEG compression. Experimental results showed that such a scheme could embed and extract the watermark at a high compression rate.

Keywords: authentication, watermarking, JPEG compression

INTRODUCTION

Watermarking, that is the technique of placing and transmitting a small amount of data imperceptibly in the host or cover data has many applications including broadcast monitoring, owner identification, proof of ownership, and content authentication. Paper watermarks are used regularly as an authentication (anti-counterfeiting) measure in valuable documents, such as bank notes, cheques and visa stamps. For instance, the authenticity of a bank note is confirmed by the existence of a visible watermark pattern when the note is held to the light. Paper watermarks are designed to be i) easily detectable, ii) hard to reproduce, and iii) invisible or unobtrusive in normal use of the document. Digital watermarks inherit many of the paper watermarks features and properties: they are digital patterns superimposed on digital signals; the patterns should be easily detectable, yet be very hard to reproduce without specific knowledge (cryptographic keys); the watermark should be invisible or unobtrusive during normal use of the digital signal.
However, steganography or data hiding has a long history and the use of paper watermarks for copy protection can be traced back to the thirteenth century (Murray 1996). The earliest forms of information hiding can actually be considered to be highly crude forms of private-key cryptography; the "key" in this case being the knowledge of the method being employed (security through obscurity). Steganography books are filled with examples of such methods used throughout history. Greek messengers had messages tattooed into their shaved head, concealing the message when their hair finally grew back. Wax tables were scraped down to bare wood where a message was scratched. Once the tables were re-waxed, the hidden message was secure (Petitcolas 2000). Over time these primitive cryptographic techniques improved, increasing speed, capacity and security of the transmitted message.

Today, crypto-graphical techniques have reached a level of sophistication such that properly encrypted communications can be assumed secure well beyond the useful life of the information transmitted. In fact, it is projected that the most powerful algorithms using multi kilobit key lengths could not be comprised through brute force, even if all the computing power worldwide for the next 20 years was focused on the attack. Of course the possibility exists that vulnerabilities could be found, or computing power breakthroughs could occur, but for most users in most applications, current cryptographic techniques are generally sufficient.

Why then pursue the field of information hiding? Several good reasons exist, the first being that "security through obscurity" is not necessarily a bad thing, provided that it is not the only security mechanism employed. Steganography for instance allows us to hide encrypted messages in mediums less likely to attract attention. A garble of random characters being transmitted between two users may tip off a watchful third party that sensitive information is being transmitted; whereas baby pictures with some additional noise present may not. The underlying information in the pictures is still encrypted, but attracts far less attention by being distributed in the picture than it would otherwise.

Nowadays, there exist watermarking methods for virtually every kind of digital media: text documents (Su et al. 1998, Brassil et al. 1999), images (Tsai et al. 2004, Zhang et al. 2003, Paquet et al. 2003), video (Sun and Chang 2003, Okada et al. 2002), audio (Li and Xue 2003, Yan et al. 2004), even for 3D polygonal models (Kwon et al. 2003, Benedens and Busch 2000), maps (Barni et al. 2001) and computer programs (Monden et al. 2000). Interestingly, watermarking technology is not limited to digital media, but is also applicable to chemical data like protein structures, for example (Eggers et al. 2001).

IMAGE COMPRESSION

Image compression seeks to reduce the number of bits required to represent the image information. Two fundamental properties used in image compression are removal of redundancy and reduction of irrelevant content. Irrelevant content may include information not perceived by the viewer, namely the human visual system (HVS). Three types of redundancy may be exploited:

- Spatial redundancy or correlation between neighbouring pixels
- Spectral redundancy or correlation between different frequency bands
- Temporal redundancy or correlation between adjacent frames in a sequence of images (in video applications).

Compression algorithms can be divided into two main groups, lossless and lossy methods. In lossless compression schemes, only the redundancy is exploited, and the image is recorded in a more efficient manner. All the information is retained and so the reconstructed image is numerically identical to the original image. In lossy compression, information deemed irrelevant to the visual perception of the human viewer is discarded and so the compressed image cannot be perfectly reconstructed and distortion is introduced into the reconstructed image.

While lossless compression does not harm a watermarking system in any way (the original data can be perfectly reconstructed), lossy compression methods introduce distortion that has to be taken into account in watermarking applications. Lossy compression techniques are nowadays being commonly used as a means to effect a reduction on the requirement for bandwidth and storage space. It is therefore necessary to study the effects of lossy image compression on watermarking systems.

It should be observed that the design goal of lossy compression systems is opposed to that of watermark embedding systems. The HVS model of the compression system attempts to identify and discard perceptually insignificant information of the image, whereas the goal of the watermarking system is to embed the watermark information without altering the visual perception of the image. An optimal compression or de-noising system would immediately discard any such watermark information. Fortunately, all current compression methods are not optimal and allow watermarking schemes to be devised that will embed watermark information that is robust.

It remains unresolved how lossy compression should best be employed for the storage and transmission of medical images. There is little guidance from the scientific literature, professional practice standards, regulatory authorities, or the common law. Although lossy compression schemes are included in medical standards such as DICOM, their clinical use is not defined; it is only that the technology is available for use at the discretion of the user or implementer.

There is no good metric by which to judge lossy compression schemes or determine appropriate threshold levels for diagnostic use. Quantitative metrics based on an analysis of the image pixels such as