Information Sciences 279 (2014) 251–272

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

A recent survey of reversible watermarking techniques

Asifullah Khan *, Ayesha Siddiqa, Summuyya Munib, Sana Ambreen Malik

Pattern Recognition Lab, Department of Computer and Information Sciences, Pakistan Institute of Engineering and Applied Sciences, Islamabad, Pakistan

ARTICLE INFO

Article history:
Received 26 July 2013
Received in revised form 6 December 2013
Accepted 29 March 2014
Available online 4 April 2014

Keywords:
Information hiding
Histogram processing
Reversible watermarking
Error expansion
Quantization
Prediction error

ABSTRACT

The art of secretly hiding and communicating information has gained immense importance in the last two decades due to the advances in generation, storage, and communication technology of digital content. Watermarking is one of the promising solutions for tamper detection and protection of digital content. However, watermarking can cause damage to the sensitive information present in the cover work. Therefore, at the receiving end, the exact recovery of cover work may not be possible. Additionally, there exist certain applications that may not tolerate even small distortions in cover work prior to the downstream processing. In such applications, reversible watermarking instead of conventional watermarking is employed. Reversible watermarking of digital content allows full extraction of the watermark along with the complete restoration of the cover work. For the last few years, reversible watermarking techniques are gaining popularity because of its increasing applications in some important and sensitive areas, i.e., military communication, healthcare, and law-enforcement. Due to the rapid evolution of reversible watermarking techniques, a latest review of recent research in this field is highly desirable. In this survey, the performances of different reversible watermarking schemes are discussed on the basis of various characteristics of watermarking. However, the major focus of this survey is on prediction-error expansion based reversible watermarking techniques, whereby the secret information is hidden in the prediction domain through error expansion. Comparison of the different reversible watermarking techniques is provided in tabular form, and an analysis is carried out. Additionally, experimental comparison of some of the recent reversible watermarking techniques, both in terms of watermarking properties and computational time, is provided on a dataset of 300 images. Future directions are also provided for this potentially important field of watermarking.

1. Introduction

OVER the past few years, the enormous increase in the use of digital content has increased the issues such as online data vulnerability and copyrights violation [7,10,23,50,81]. One of the prominent solutions is the watermarking of the digital content. Beside watermarking, there exist other interesting methods that can also provide protection to the digital content e.g., cryptography, steganography etc. [13,29,48,58,65,111]. Steganography and watermarking both come under data hiding techniques i.e., they are used to hide secret information in the cover work. However, there exist subtle difference between steganography and watermarking i.e. steganography conceals the very existence of secret information. If the existence of secret information is revealed, steganography fails. Whereas, in watermarking the existence of secret information can be

* Corresponding author. Tel.: +92 512207381; fax: +92 512208070.
E-mail address: asif@pieas.edu.pk (A. Khan).

http://dx.doi.org/10.1016/j.ins.2014.03.118
0020-0255/

known [23]. Ideally, the goal of watermarking is to make the removal/manipulation of secret information impossible. In contrast, cryptography does not conceal the existence of secret information, rather it encrypts the information in such a way that it appears useless to a pirate unless decrypted with the appropriate key [10,23].

Through suitable watermarking techniques, the protection of the data can be ensured and one can know whether the received content has been tampered with or not. However, watermarking can cause damage to the sensitive information present in the cover work, and thus at the receiving end, the exact recovery of cover work may not be possible. In some applications, even the slightest distortion in the cover work is intolerable. For example, in the field of medical imagery, if a medical image is modified using conventional watermarking, the small change may affect the interpretation significantly and a physician may make a wrong diagnosis. Similarly, in case of military application, changes due to embedding of secret information can substantially alter the cover image and therefore, the decision taken may cost considerably. Consequently, there is a strong need to restore the cover work to its original form. Reversible watermarking, also known as lossless watermarking, allows full extraction of the embedded information along with the complete restoration of the cover work. Reversible watermarking can thus be considered as a special case of watermarking.

Reversible watermarking is gaining more attention for the last few years because of its increasing applications in military communication, healthcare, and law-enforcement. Fig. 1 shows the block diagram of a basic reversible watermarking system.

In the sequel, the terms information-to-be-embedded and watermark are used interchangeably. As regards general watermarking schemes, different types are reported in literature; namely robust, fragile, and semi fragile [11,12,14,25,34,37,39,49,57,70,74,104]. In robust watermarking schemes, watermark is designed to survive normal image processing operations. While, in fragile watermarking schemes, watermark breaks if the watermarked work undergoes any kind of modification, thus it is useful for authentication of digital media [94,109]. Whereas, in case semi-fragile watermarking schemes, watermark needs to survive minor modifications. These different types of watermarking schemes have different applications, and thus are used according to the nature of application. But, the existing reversible watermarking schemes are mostly fragile in nature. The two important properties of reversible watermarking are imperceptibility and embedding capacity. Roughly speaking, imperceptibility is the measure of similarity between watermarked and the cover image. While, embedding capacity is the measure of the maximum number of information bits that can be embedded in the cover image. The performance of a reversible watermarking technique is thus evaluated on the basis of these measures.

One of the first reversible watermarking method was introduced by Honsinger et al. [41]. They utilized modulo addition 256 to achieve reversibility in their watermarking technique. Macq [69] developed a reversible watermarking approach by modifying the patchwork algorithm and using modulo addition 256. Although, Honsinger et al. [41] and Macq [69] proposed reversible techniques, the imperceptibility of their approaches is not impressive. The watermarked images resulting from Honsinger et al. [41] and Macq [69] 's techniques suffer from salt and pepper noise because of the use of modulo addition 256. A reversible watermarking technique without using modulo addition 256 was then introduced by Fridrich et al. [30]. Fridrich et al. [30] proposed the concept of compressing the least significant bit (LSB) plane of cover image to make space for the watermark to be embedded. However, the embedding capacity of this approach was limited. To improve the embedding capacity and imperceptibility of the watermarked image, Fridrich et al. [31] then proposed another approach. Evolution of reversible watermarking started around 2000, and it is now quite difficult to keep up with the development that is going on in this field. Many reversible watermarking algorithms have been developed in the past decade. A number of new techniques, extensions or improved versions of the earlier techniques, have been proposed in recent years. The improvement is primarily based upon making a good imperceptibility versus capacity tradeoff.

Zheng et al. reported a comprehensive survey on robust image watermarking alogorithms [114]. Guo [35] and Guo et al. [36] reported reversible watermarking techniques for the halftone images. In past, reviews of different reversible watermarking techniques were also carried out [8,28,83]. Feng et al. [28] discussed key requirements of the watermark and classified reversible watermarking schemes into three categories: data compression, difference expansion and histogram shifting. A single reversible watermarking scheme is discussed in each of these categories. Some major challenges faced by the researchers in this field are also outlined. Pan et al. [83], categorized various reversible watermarking approaches into two classes; additive and substitution, based on embedding method. Comparison is carried out through empirical analysis of selected reversible watermarking approaches on medical images. Caldelli et al. [8] provided another review, which classifies reversible watermarking techniques, on the basis of watermarking properties, i.e., into robust, fragile and semi-fragile.

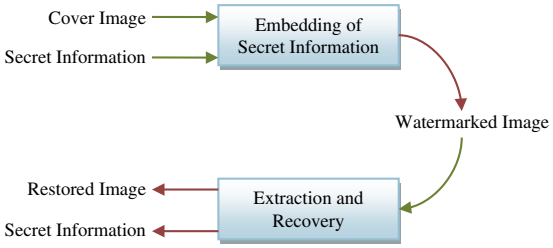

Fig. 1. Basic reversible image watermarking scheme.