Reversible Watermarking

Dinu Coltuc
Valahia University of Targoviste, Romania

INTRODUCTION

Watermarking is the imperceptible hiding of information about a certain digital work (image, video, sound, text) within that work itself. Its major utility is to increase data security (by copyrighting, fingerprinting, authentication). Besides data security, watermarking provides a hidden channel with applications in annotation, compressive data hiding and so on. The properties imposed to watermarking are strictly connected to its applications. Thus, the use of watermarking for copyrighting or fingerprinting demands robustness. For annotation watermarking, the stringent requirement is watermarking capacity, while robustness is not an issue. The required capacity can range from one bit in certain copyrighting applications to an amount which can represent a large fraction of the host size. Robustness and capacity are contradictory demands and so are robustness and imperceptibility, or capacity and imperceptibility.

Even imperceptible, the insertion of information within the host data introduces distortions. There are domains where no distortion is accepted (for instance, medicine, military, etc.). The reversible watermarking was introduced in order to extend watermarking to such special domains. Compared with its classical counterpart, the reversible watermarking removes the watermark and recovers the original host data with no distortion.

This article investigates the state of the art in reversible watermarking. The main approaches for reversible watermarking are presented and the selection of the appropriate scheme in function of the embedded bit-rate is discussed. We further focus on the difference expansion approach which is known to provide the best results. The extension of the scope of reversible watermarking by ensuring joint robustness and reversibility is also discussed.

BACKGROUND

The straightforward approach to reversible watermarking is by using lossless compression (Fridrich, Goljan, & Du, 2002, etc.). In order to make room for data embedding, a part of the host is compressed and substituted by the compressed data and the watermark. The imperceptibility of the watermarking imposes the substitution somewhere into the least significant bits of the host. Obviously, the least significant bits are noisy and, consequently, the compression ratio is rather low. The compression based approaches are either of rather low capacity, or, in order to gain in capacity, of rather high complexity. The best performances reported so far for compression based reversible watermarking are about 1 bpp (Celik, Sharma, & Tekalp, 2006).

Another approach is histogram shifting reversible watermarking. In the original approach of Ni, Zhicheng et al. (2006), image graylevels are shifted in order to create, into the image histogram, a gap of one graylevel adjacent to the most populated graylevel, i.e., to the histogram peak. Data embedding follows immediately by scanning the image and by flipping the pixels of the most populated graylevel to the one of the gap if the bit to be embedded is "1" and by not flipping for "0." In one watermarking level, the original method provides an embedding capacity of the order of the maximum histogram bin. Sharper histograms (Laplacian distributed), as the ones of the difference between adjacent pixel or of the prediction error, are used to increase the embedding capacity (Lin et al., 2008). In a single level of embedding, the histogram shifting reversible watermarking provides up to about 0.1-0.3 bpp at a very low distortion. Bit-rates greater than 1 bpp can be obtained by multiple embedding. Obviously, the distortion increases with each level of embedding.

The third major approach to reversible watermarking is by difference expansion (DE). Introduced by Tian (2003), the difference expansion reversible watermarking creates space by expanding two times

DOI: 10.4018/978-1-4666-5888-2.ch716

some differences. The expansion is a simple arithmetic shift that clears the least significant bit of the difference. Furthermore, the sequence of bits composed of the data and the auxiliary information is placed by simple additions into the cleared LSBs. Tian used the difference of adjacent pixels. The latter DE schemes use mainly the prediction error (Thodi & Rodríguez, 2007, etc.). Various predictors are used, ranging from the simple first order predictor used by Tian to more accurate predictors as the median edge detector (MED), the gradient-adjusted predictor (GAP), the average on the four horizontal/vertical neighbors and so on. The DE schemes appear to provide very good performances at medium and large embedding bit-rates.

Besides the three major directions mentioned above, there are other approaches as well. We shall mention only the approach proposed by Honsinger et al., 2001, inspired by the classical spread-spectrum watermarking (Cox et al., 2007). The basic principle is to embed one bit into the entire image by simply adding modulo 256 an integer white-noise watermark sequence. The detection is made by correlation with the watermark. Since the watermark is known at detection, the original host can be immediately recovered by subtraction modulo 256. The scheme ensures a certain degree of robustness, but provides low embedding capacity and generates “salt-and-pepper” noise.

The use of reversible watermarking in fragile authentication or in some data hiding applications is obvious. The problems appear mainly in copyrighting where the robustness is a must. Fridrich, Goljan, and Du (2002) proposed the use of reversible watermarking for copyrighting in the framework of the distortion-free robust watermarking paradigm. They considered the reversible watermarking of Honsinger discussed in the above paragraph. Obviously, in case of no attacks, the watermark is detected and the authorized party exactly recovers the original. In case of attacks, one can suppose that the robust watermark can still be detected, but the reversibility is lost. A better solution is proposed in Coltuc and Chassery (2007), where the joint robustness and reversibility is obtained by two stages of watermarking. Robust watermarking is performed first. Then, by reversible watermarking, the information needed to invert both the robust and the reversible watermarking is embedded. Compared with Fridrich, Goljan, and Du (2002), the distortion-free robust watermarking by multiple watermarking provides more flexibility.

MULTIBIT DIFFERENCE EXPANSION REVERSIBLE WATERMARKING

Next we present the multibit extension of the DE reversible watermarking. The classical DE scheme can be immediately recovered as a particular case.

Basic Principle

Let x be the graylevel of a pixel and let $\hat{x}$ be the predicted value. The prediction error follows as:

$$e = x - \hat{x} \tag{1}$$

Let further n be a fixed integer, $n \geq 2$, and let w be an integer code in $[0, n - 1]$. The prediction error is expanded n times and the integer code w is added to the expanded error:

$$E = ne + w \tag{2}$$

The expansion of the prediction error is obtained by modifying the pixel as follows:

$$X = \hat{x} + E = x + (n - 1)e + w \tag{3}$$

The transformed pixel should preserve image graylevel range. For 8 bit graylevel images, one should have $0 \leq X \leq 255$.

The transform described above is exactly invertible. The embedded codeword is extracted immediately by using modular arithmetic:

$$w = (X - \hat{x}) \bmod n \tag{4}$$

The original pixel is recovered as:

$$x = \frac{X + \left(n-1\right)\hat{x} - w}{n} \tag{5}$$

Equations (4) and (5) hold if one can recover, at detection, the same predicted value for x. This is obtained by using, for instance, anticausal predictors and by considering opposite scanning directions for marking and detection. Thus, if the marking is performed in raster-scan order starting with the upper left corner,