A NOVEL APPROACH FOR DIGITAL IMAGE WATERMARKING

M V S BABU M.Tech., MCSA, D V L SUSEELA, P PRASANNA LAKSHMI, A JYOTHI
Asst.Professor, ECE, RISE KRISHNA SAI PRAKASAM GROUP OF INSTITUTIONS, ONGOLE

Abstract-- The algorithm of discrete wavelet transform is developed to achieve the integrity authentication of color image contents through embedding watermarking. Firstly, a new watermarking image is generated with the XOR between the original binary watermarking and the image which is processed with Hankel transform. When the watermark is embedded, the original image color is converted first and the brightness component is decomposed into three discrete wavelets. Then, the low frequency approximation sub-image of third-level is extracted, and its least significant bit is set 0. Finally, the new watermark is embedded into its least significant bit. Through comparing the pixels of original watermarking image with that of the extracted watermarking image, it can be determined whether the watermarking image has been tampered, and the tampered area of the original color image is located. The results of simulation experiment shows that the algorithm has the strong capabilities of detection and location and it also can keep the original image quality well.

Keywords: wavelet transform, hankel transform, digital image watermarking, image authentication.

I Introduction

1.1. Overview

In the last few years, fragile watermarking has been widely used to authentication and content integrity verification. The technique modify the host image in order to insert the pattern but the permanent embedding distortion is intolerable for the applications that requires high quality images such as medical and military images. The most adequate solution for this problem is robust watermarking algorithm. The robust watermarking not only provides authentication and tamper proofing but also can recover the original image from the suspected image. After the verification process if the transmitted image is deemed to be authentic the doctor reconstitutes the original image and uses it in its diagnosis avoiding all risk of modification. An intriguing feature of the robust watermark embedding is the reversibility, that is one can remove the embedded image to restore the original image.

From the information hiding point of view, the robust image embedding hides some information in the digital image in such a way that an authorized party could decode the hidden information and also restore the image to its original state. A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as an audio, video or image data. It is typically used to identify ownership of the copyright of such signal. “Watermarking” is the process of hiding digital information in a carrier signal; the hidden information should[1] but does not need to, contain a relation to the carrier signal. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. It is prominently used for tracing copyright infringements and for banknote authentication. Example of a watermark overlay on an image; the logo of Wikipedia can be seen on the center to represent the owner of it. Like traditional physical watermarks, digital watermarks are often only perceptible under certain conditions, i.e. after using some algorithm.[2] If a digital watermark distorts the carrier signal in a way that it becomes easily perceivable, it may be considered less effective depending on its purpose.[2] Traditional watermarks may be applied to visible media (like images or video), whereas in digital watermarking, the signal may be audio, pictures, video, texts or 3D models.

A signal may carry several different watermarks at the same time. Unlike metadata that is added to the carrier signal, a digital watermark does not change the size of the carrier signal. The needed properties of a digital watermark depend on the use case in which it is applied. For marking media files with copyright information, a digital watermark has to be rather robust against modifications that can be applied to the carrier signal. Instead, if integrity has to be ensured, a fragile watermark would be applied.

Both steganography and digital watermarking employ steganographic techniques to embed data covertly in noisy signals. But whereas steganography aims for imperceptibility to human senses, digital watermarking tries to control the robustness as top priority. Since a digital copy of data is the same as the original, digital watermarking is a passive protection tool. It just marks data, but does not degrade it or control access to the data. One application of digital watermarking is source tracking. A watermark is embedded into a digital signal at each point of distribution. If a copy of the work is found later, then the watermark may be retrieved from the copy and the source of the distribution is known. This technique reportedly has been used to detect the source of illegally copied movies.

The information to be embedded in a signal is called a digital watermark, although in some contexts the phrase digital watermark means the difference between the watermarked signal and the cover signal. The signal where the watermark is to be embedded is called the host signal. A watermarking system is usually divided into three distinct steps, embedding, attack, and detection. In embedding, an algorithm accepts the host and the data to be embedded, and produces a watermarked signal.

Then the watermarked digital signal is transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called an attack. While the modification may not be malicious, the term attack arises from copyright protection application, where third parties may attempt to remove the digital watermark through modification. There are many possible modifications, for example, lossy compression of the data (in which resolution is diminished), cropping an image or video, or intentionally adding noise. Detection (often called extraction) is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was unmodified during transmission, then the watermark still is present and it may be extracted. In robust digital watermarking applications, the extraction algorithm should be able to produce the watermark correctly, even if the modifications were strong. In
fragile digital watermarking, the extraction algorithm should fail if any change is made to the signal.

![Watermarking Procedure](image)

**Fig. 1: Watermarking Procedure**

## General Requirements

A digital watermark is called robust with respect to transformations if the embedded information may be detected reliably from the marked signal, even if degraded by any number of transformations. Typical image degradations are JPEG compression, rotation, cropping, additive noise, and quantization for video content, temporal modifications and MPEG compression often are added to this list. A digital watermark is called imperceptible if the watermarked content is perceptually equivalent to the original, un-watermarked content. In general, it is easy to create robust watermarks -or- imperceptible watermarks, but the creation of robust and imperceptible watermarks has proven to be quite challenging. Robust imperceptible watermarks have been proposed as tool for the protection of digital content, for example as an embedded no-copy-allowed flag in professional video content.

### 2.1 Robustness

A digital watermark is called fragile if it fails to be detectable after the slightest modification. Fragile watermarks are commonly used for tamper detection (integrity proof). Modifications to an original work that clearly are noticeable commonly are not referred to as watermarks, but as generalized barcodes. A digital watermark is called semi-fragile if it resists benign transformations, but fails detection after malignant transformations. Semi-fragile watermarks commonly are used to detect malignant transformations. A digital watermark is called robust if it resists a designated class of transformations. Robust watermarks may be used in copy protection applications to carry copy and no access control information.

### 2.2 Perceptibility

A digital watermark is called imperceptible if the original cover signal and the marked signal are (close to) perceptually indistinguishable. A digital Watermark is called perceptible if its presence in the marked signal is noticeable, but non-intrusive.

### 2.3 Capacity

The length of the embedded message determines two different main classes of digital watermarking schemes: The message is conceptually zero-bit long and the system is designed in order to detect the presence or the absence of the watermark in the marked object. This kind of watermarking scheme is usually referred to as zero-bit or presence watermarking schemes. Sometimes, this type of watermarking scheme is called 1-bit watermark, because a 1 denotes the presence (and a 0 the absence) of a watermark.

#### 2.4 Blind

Some of the conventional watermarking schemes require the help of an original image to retrieve the embedded watermark. However, the reversible watermarking can recover the original image from the watermarked image directly. Therefore, the reversible watermarking is blind, which means the retrieval process doesn’t need the original image.

### 2.5. Higher embedding capacity

The capable size of embedding information is defined as the embedding capacity. Due to the reversible watermarking schemes having to embed the recovery information and watermark information into the original image, the required embedding capacity of the reversible watermarking schemes is much more than the conventional watermarking schemes.

The embedding capacity should not be extremely low to affect the accuracy of the retrieved watermark and the recovered image. The procedure of conventional and reversible watermarking schemes can be illustrated by using the flowcharts in the above figure. The steps of conventional watermarking and reversible watermarking are similar except there is an additional function to recover the original image from the suspected image. Therefore, the robust watermarking is especially suitable for the applications that require high quality images such as medical and military images. In addition, there are two research fields often connected with digital watermarking: data hiding and image authentication. The purpose of data hiding is using the cover image to conceal and transmit the secret information. And the purpose of image authentication is to verify the received image whether it be tampered or not. In order to achieve the goals, the data hiding scheme should have a large embedding capacity to carry more secret information, and it has to be imperceptible to keep the secret undetectable. The image authentication schemes also require embedding some information into the protected image, and also has to keep the imperceptibility between the preprocessed image and processed image. As in the definition, the goals of the robust watermarking are to protect the copyrights and can recover the original image.

The robustness, imperceptibility, high embedding capacity, high embedding capacity, readily embedding and retrieving, and blind are the basic criterions of the reversible watermarking. A reversible data hiding scheme and a reversible image authentication scheme can be also defined as the schemes which can recover the original image from the embedded image.

### III Multi-Level Decomposition of Wavelet and Hankle Transform Based Data Hiding

#### 3.1 Multi-Level decomposition

For the information hiding algorithms (such as DFT, DCT, DWT, and so on), the secret information may be extracted by applying the exhaustive algorithm to the information intercepted when these information hiding algorithms are used to conceal the information merely. However, if the secret information is scrambled through the algorithm before it is concealed, it will become disorderly and unsystematic.
Then, when it is embedded into the information carriers, the information will be transmitted more safely. In this case, the secret information will not be identified even if it is extracted, and it will be regarded as that the extracting algorithm is wrong or the information carriers contain nothing.

Fig. 2: Process of decomposing the digital image with wavelet transforms

In Figure 2, the original image is decomposed into four sub-images, including one low frequency subimage LL1 with quarter pixels and three high frequency sub-images with quarter pixels: HL1 details in the vertical direction, LH1 details in the horizontal direction and HH1 details in the diagonal direction. When the approximate sub-image LL1 is decomposed again, four lower resolution sub-image images are obtained. If the lower resolution sub-image images are decomposed repeatedly, the wavelet decomposition of digital images can be reached. The main power is contained in the lowest frequency sub-image which includes the main characteristics.

The low frequency sub-images have the capability of resisting the noises, and the high frequency subimages are easy to be affected by the noises and they are unstable relatively. For improving the speed and security of embedding the watermarking, three-stage discrete wavelet transform is applied and LL3 is selected to be disposed. Because the low frequency sub-images contains the main power of image discomposed, it can embody the invisibility of watermarking and reduce the effect of watermarking on the original image that embeds the watermarking into the least significant digit of the third wavelet transform.

IV Watermark Embedding

4.1 Embedding procedure

The digital watermarking embedded process based on wavelet transform (DWT) is shown as Figure 3.

Step 1: A binary watermarking image is scrambled through using the Hankel matrix for several times, and the purpose is to make watermark disorderly with the times of scrambling as a key.

Step 2: The original color image is under binarization process with better threshold value chosen.

Step 3: A new watermarking image is generated through applying the XOR processing to the image from Step 1 and Step 2.

Step 4: Accordance to the RGB-YUV color space Conversion formula for original image color space conversion, the color image is converted from the RGB color space to the YUV color space.

Step 5: Apply the three discrete wavelet decomposition to the Y component (luminance component) of the YUV color space, and the lowest effective low-frequency of the third-level wavelet transform is postied 0;

Step 6: The new generated watermark is embedded into the least significant bit after Step 5 treatment.

Step 7: Apply three discrete wavelet inverse transform.

Step 8: Combine the new Y component (luminance component) with the UV components (color components).

Step 9: The image after the process of Step 8 is converted from the YUV to RGB, and a final image with the watermark generated...

Fig. 3: Flowchart for embedding

Fig. 4: Flowchart for extraction

4.2 Extraction of the watermark

The first stage of fragile digital watermarking extraction and detection is same, namely, the image detection is transformed by three-stage discrete wavelet and then select the part of the third level on LL3. The difference is that the latter part, it is need to extract the LSB of the third level LL3 of the image to be detected, the threshold is used to treat a given color image detection to generate a binary image, and then the generated binary image XOR the extracted LSB image, generating a watermarking image, the watermark generate anti-replacement plan at last. The tamper localization of the fragile watermarking is completed. The process part of digital watermarking extraction and detection is shown in Figure 4.

5. Results

5.1 A robust watermark embedding using hankel transform

A 512-by-512 color Lena image is taken as the input image. This image is converted binary image. Interpolation technique is applied to the input image to form the interpolated image. Interpolation is the method of determining high resolution in an image from its low resolution counterparts. Later that image was resized to 64-by-64.
VI Conclusion

In this Paper the watermarking image is scrambled with Hankel transform before it is embedded. The watermarking image formation, the carrier image are used for generating a new watermark, and then the watermark is embedded with Hankel matrix, which can effectively hide and protect the watermarking information from the usual malicious attacks to common image. Thus, it becomes more difficult that the attackers extract the watermark. Even if the attack is not very strong, the watermark extraction can also play a good location performance.

VII Reference


