Multi Image Watermarking Based On Colour Channel

Shah Monika
MTech (SE) Student, Department Of Computer Science & Engineering,
Shrinathji Institute Of Technolgy & Engineering , Nathdwara ,
Rajasthan , India.

Abstract

A new robust multi image digital watermarking scheme is proposed based colour channel and on pixels intensity in the carrier images. The colour image is divided into its three basic colour channels (Red, Green, and Blue). Each channel is treated as a host image and broken into segments of equal sizes. A histogram is drawn for each segment in these channels formulating the number of pixels against intensity. Each channel embeds one modulating image resulting into multi-watermarked image. The channels are then re-integrated back to form the watermarked image. This technique is good for strong image authentication and authorized person who know key value can only get original image back .Hence, watermark bits values are distributed irregularly all over the carrier image making it extremely difficult to be noticed or extracted unless the key is known. Therefore, this method has proved to be very secure and robust against different types of noise, resizing and rotation.

1. Introduction

Embedding a digital signal (audio, video or image) with information which cannot be removed easily is called digital watermarking 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. The watermarked signal is then transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called an attack. There are many possible attacks. Detection is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was not modified during transmission, then the watermark is still present and it can be extracted. If the signal is copied, then the information is also carried in the copy. The embedding takes place by manipulating the content of the digital data, which means the information is not embedded in the frame around the data, it is carried with the signal itself. The watermark may be a logo, label or a random sequence. A typical good watermarking scheme should aim at keeping the embedded watermark very robust under malicious attack in real and spectral domain.

2. Requirements of Watermarking

Transparency: The embedded watermark should not degrade the original image. If visible distortions are introduced in the image, it creates suspicion and makes life ease for the attacker .It also degrades the commercial value of the image. [1]

Robustness: This is by far the most important requirement of a watermark. There are various attacks, unintentional (cropping, compression, scaling) and unintentional attacks which are aimed at destroying the watermark. So, the embedded watermark should be such that it is invariant to various such attacks.

Security: watermarking accounts for the protection of ownership against forgery and unlawful threats. Invisible watermark should be secret and must be undetectable by an unauthorized user in general.[4]

Capacity: It is a way to determines two different main classes of digital watermarking schemes by the length of the embedded message. In zero-bit or presence watermarking schemes, the message is conceptually zero-bit long, it is designed to detect the presence or the absence of the digital watermark in the marked object. In multiple-bit watermarking or non-zero-bit watermarking schemes, the n-bit-long stream message is modulated in the watermark.

Imperceptibility: It should be perceptually invisible so that data quality is not degraded and attackers are prevented from finding and deleting it. A watermark is called imperceptible if the watermarked content is perceptually equivalent to the original, unwatermarked content.

3. Basic Watermarking Scheme

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. The watermarked signal is then transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called an attack. There are many possible attacks.[3] Detection is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was not modified during transmission, then the watermark is still present and it can be extracted. If the signal is copied, then the information is also carried in the copy. The embedding takes place by manipulating the content of the digital data, which means the information is not embedded in the frame around the data, it is carried with the signal itself. Figure 1 and 2 shows the basic block diagram of embedding and extracting watermarking process. [2]

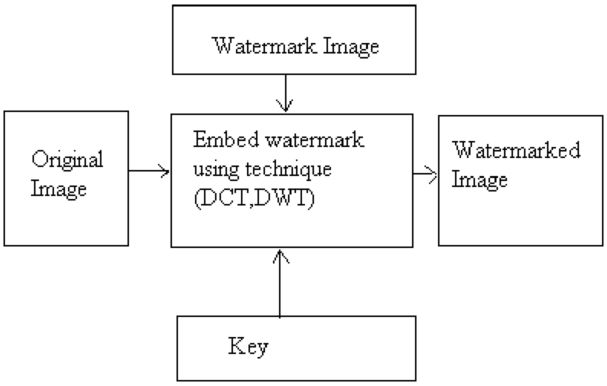


Fig.1 Embedding watermark

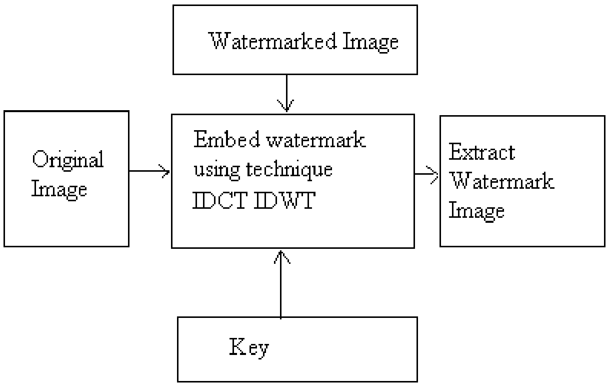


Fig.2 Extracting watermark

4. Proposed Watermarking Scheme

This paper presents an algorithm that utilizes the intensity histogram technique for embedding watermarks in colour image. The algorithm accepts three images (or logos) to be embedded in one colour image carrier. It splits the carrier image into its three basic components (red, green and blue), then embeds one watermark evenly in each component into all parts of the image according to the frequency analysis of maximum amplitude occurrence. The resulting three watermarked images are then recombined together to get the final modulated image, as shown in figure 3. The original logos can be recovered in a reverse process when required at the time of any copyright conflict.

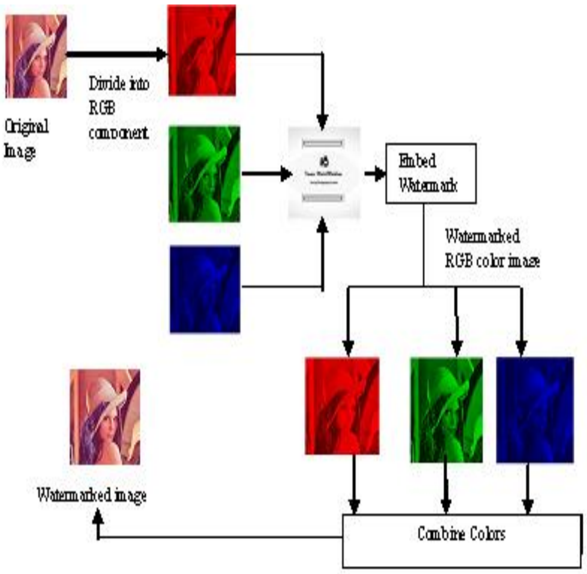


Fig.3. Embedding watermark

A. Watermark Embedding Algorithm

1: Read both of the carrier image, 1024x1024 pixels, and the three modulating images each one of size 128x128 pixels.

2: Split the carrier image into three channels according to the three original colours (Red, Green, and Blue) as shown in figure 3.

3: Convert the modulating images is converted into black and white colour space. Now it is possible to map each regional segment from the carrier image into one bit of modulating image as in the following steps.

4: Segment each colour channel of the carrier image into blocks of equal dimensions according to the process adopted in . Calculate and draw the histogram for the number of pixels versus intensity for each block, then select the pixel with maximum frequency of occurrence (i.e. the intensity that has the maximum value of pixels). The embedding process is performed depending on the bit value of the watermark binary image, if it is 1, the intensity is increased by 1 but if it is 0 then the intensity is decreased by 1. Then resemble these new blocks into new image.

5: The above step is repeated for the three watermarks involved to be embedded into the three colour channels.

6: Integrate the resulted images of the three channels of steps 4&5 into single modulated carrier image. Save this modulated image and the resized modulating image.

B. Watermark Extracting Algorithm

For the ownership proof, the proposed technique requires both the original image and the watermarked image.

1: Read the original image (carrier image) and the watermarked image.

2: Divided the carrier image into three channels and treated each channel as a single image. Each channel is then segmented into equal blocks and finds the intensity that has the maximum value of pixels in histogram for each block.

3: Divided the modulated image into three channels and treated each channel as a single image then each channel is segmented into blocks and find the intensity for each block after embedding .

4: Save the extracted watermark image.

5. Implementation and Experimental Results

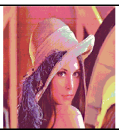
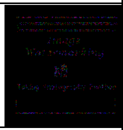
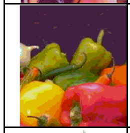
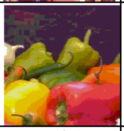
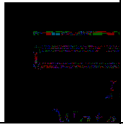
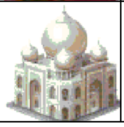
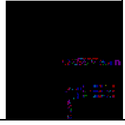
For having a better difference invisible effect on a watermarked image, a 1024x1024 Lena portrait and a 128x128 digital watermark image message will be chosen as the copyright material image and the watermark message for the experiment. Based on the pre-test PSNR results in different α values on different image partition settings, α=0.003 and 32x32 partition setting will be applied to both copyright material image and fingerprint watermark message.

To examine performance of the proposed watermarking technique, evaluation is depend upin value of the mean square error MSE and peak signal to noise ratio PSNR was calculated using equations 1 and 2.[5]

$$MSE=\frac{1}{MN}\sum_{i=1}^{m}\sum_{j=1}^{n}(fc(i,j)-fm(i,j))2 \qquad (1)$$

$$PSNR= \quad 10\log10\left(\frac{W*H}{MSE}\right) \qquad (2)$$

TABLE I
EXPERIMENTAL RESULT OF WATERMARKING TECHNIQUE

Cover Image	Waermark Image	Watermarked Image	Difference Image	PSNR (db)
	Image Watermarking Taking Photography Further			60.26
	Image Watermarking Taking Photography Further			60.29
	Image Watermarking Taking Photography Further			60.24

Attacks on Watermarked Image

There are different types of attacks can be applied on image ; namely salt& paper ,gaussian noise, poisson noise, resize noise, and compression noise, median filter,wiener noise, rotate noise, speckel noise.

By considering these types of attacks can measure applicability of proposed algorithm and for that eperimental results are shown in table 2.

TABLE III
EXPERIMENTAL RESULT OF WATERMARKING TECHNIQUE FOR VARIOUS TYPES OF ATTACKS

Original Image	Attack salt& paper	Attack gaussian	Attack possion	Attack resize
Attack compression	Attack median filter	Attack wiener	Attack rotate	Attack speckel

6. Conclusion

A new efficient algorithm has been suggested for digital image watermarking that is based on the modification of selected maximum intensity pixels. It benefits from the histogram plot of the pixel values. Dividing the original image into equal size blocks and drawing the histogram for each block. The intensity that has the maximum value of pixels has been obtained. The selected values of intensity were used to embed the watermark into the original image, so one bit of watermark image is embedded into each block of original image.
Tests have shown that the proposed method is very secure and robust against attacks.

Watermark image bits are embedded in all the blocks of the carrier image in an irregular manner. Using this algorithm better security to image can be provided and it is difficult any unauthenticated person to get that image. Moreover, any of the three basic colour components can be used for embedding watermark image allowed for multi-watermarking process. The algorithm implementation included embedding logos in one carrier image.

7. References

[1] Chi-Man Pun and Ioi-Tun Lam, J. 2009 Fingerprint Watermark Embedding by Discrete Cosine Transform for Copyright Ownership Authentication

[2] Samir K Bandyopadhyay, Debnath Bhattacharyya, Debashis Ganguly, Swarnendu Mukherje and Poulami Das, "A Tutorial Review on Steganography "

[3] Sabu M Thampi, P. 2007 Information Hiding Techniques: A Tutorial Review

[4] K-G Stenborg, M. J. 2005 Distribution and Individual Watermarking of Streamed Content for Copy Protection. Doctoral Thesis. LIU-TEK-LIC-2005:67., Link¨oping University.

[5] Hamza A. Ali and Sama'a A.K. Khamis, L. L. 2012. Multi Image Watermarking Scheme Based on Intensity Analysis