DIGITAL IMAGE WATERMARKING - PART 2

BACKGROUND/REVIEW MATERIAL

2.1 BACKGROUND RESEARCH

The primary tool used in the research of Image watermarking is the Internet. The first objective was to understand the various terminologies related to the field. This was done through the Wikipedia and the hyperdictionary websites. Additional technical details were obtained from various articles listed under the References and Bibliography sections. The following concepts developed while understanding Image watermarking:

- Exactly identical copies of digital information, be it images, text or audio, can be produced and distributed easily. Therefore to validate the claim of ownership, a proof is required which is provided by the recovery of watermark. A **watermark** is a form, image or text that is impressed onto paper, which provides evidence of its authenticity.
- **Digital watermarking** is an extension of this concept in the digital world. It is a technique that provides a solution to the longstanding problems faced with copyrighting digital data. Digital watermarks are pieces of information added to digital data (audio, video, or still images) that can be detected or extracted later to make an assertion about the data. This information can be textual data about the author, its copyright, etc; or it can be an image itself.
- Current main **applications of watermarking** include the following:
    1. Copyright protection: The objective is to embed information about the source/owner of the digital media in order to prevent other parties from claiming the ownership of the media.
    2. Fingerprinting: The objective of fingerprinting is to convey information about the recipient of the digital media (rather than the owner) in order to identify every single distributed copy of the media. This concept is very similar to serial numbers of software products.
    3. Copy protection: Watermarking can be used to control data copying devices and prevent them from copying the digital media in case the watermark embedded in the media indicates that media is copy-protected.
    4. Image authentication: The objective is to check the authenticity of the digital media. This requires the detection of modifications to the data.

- **Requirements of Image Watermarking** is a watermark embedding system and a watermark extraction (recovery) system. The watermark embedding system takes as input the watermark bits, the image data, and optionally a watermark. The output of the watermark embedding system is the watermarked image. The watermark extraction system takes as input an image that possibly contains a watermark. Depending on the type of watermarking system used, it may also take as input the original image or the watermark. The watermark extraction system determines whether a watermark is present or absent in the image.

A useful watermarking scheme has the following properties:

1. *Imperceptibility of the watermark*: The watermarking system must embed the watermark in the image such that the visual quality of the image is not perceptibly distorted. Hence, a measure of distortion needs to be used when determining the imperceptibility of the watermarking algorithm.
2. *Robustness of the watermarking scheme*: Most of the watermarking applications require that the watermark should still be recovered even if the image is distorted. Perhaps we can call a watermarking algorithm "robust" if recovery of the watermark cannot be made impossible without perceptibly distorting the image. Robustness is not required for all applications. For example, a fragile watermark that has to prove the authenticity of the host data does not have to be robust against alterations of the image. This is due to the fact that, in this application, failure to detect the watermark proves that the host data has been modified and the image is therefore not authentic.
3. *Security*: The security of watermarking techniques is very similar to the security of the encryption techniques. A watermarking technique is truly secure if knowing the algorithms to embed and extract the watermark does not help an unauthorized party to detect the presence of the watermark.
4. *Payload of the watermark*: The amount of information that can be stored in an image for watermarking depends on the application and the image. Usually, the robustness of the watermark is increased if the payload of the watermark is bigger.

Image Watermark Categories:

1. Robust watermark- Used for copyright protection.

   Requirements: the watermark should be permanently intact to the host signal, removing the watermark result in destroying the perceptual quality of the signal.

2. Fragile watermark- Used for tamper detection or as a digital signature.

   Requirements: Break very easily under any modification of the host signal.

3. Semi Fragile watermark- Used for data authentication.

   Requirements: Robust to some benign modifications but break very easily to other attacks.

   Provide information about the location and nature of attack.

There are two techniques of digital watermarking: Spatial Domain and Transform Domain. **Spatial domain watermarking** is a technique in which the watermark is embedded by directly modifying the pixel values. Least Significant Bit Substitution is a spatial domain technique. The embedding of the watermark is performed choosing a subset of image pixels and substituting the least significant bit of each of the chosen pixels with watermark bits. Extraction of the watermark is performed by extracting the least significant bit of each of the selected image pixels. If the extracted bits match the inserted bits, then the watermark is detected. This technique is not popular in digital world because it is not robust enough to resist some common attacks. **Transform domain watermarking** is a technique in which the watermark is embedded in the transform domain e.g., DCT, DFT, DWT. Watermarking Based on DCT Coefficient Modulation technique embeds the watermark in the DCT domain to increase the robustness of the watermarking scheme against JPEG compression. The watermark bits are embedded in each 8x8 DCT block of the image. It is not wise to embed the watermark bits in the low frequency components of the DCT block, because these coefficients are subject to heavy quantization during JPEG compression. Hence, it is better to embed the watermark in mid or high-frequency DCT components.

Discrete Cosine Transform (DCT): The classic and still most popular domain for image processing is that of the Discrete-Cosine-Transform, or DCT. The DCT allows an image to be broken up into different frequency bands, making it much easier to embed watermarking information into the middle frequency bands of an image. The middle frequency bands are chosen to provide additional resistance to lossy compression techniques.

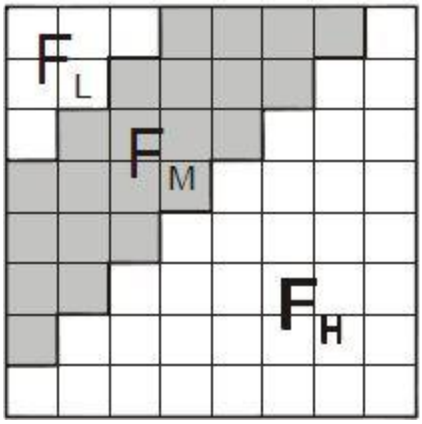

Fig 2 - Frequency bands in an image

Avoid the most visual important parts of the image (low frequencies) without overexposing themselves to removal through compression and noise attacks (high frequencies).

Middle-band Coefficient Exchange algorithm: This technique utilizes the comparison of middle-band DCT coefficients to encode a single bit into a DCT block. FL is used to denote the lowest frequency components of the block; FH is used to denote the higher components while FM is used to denote the middle frequency components. FM is chosen as the embedding region as to provide additional resistance to lossy compression techniques, while avoiding significant modification of the cover image. Two locations Pk(i1, j1) and Pk(i2, j2) are chosen from the FM region for comparison. We choose the two locations such that they have identical quantization values shown below in Table 1. Due to this any scaling of one coefficient will scale the other by the same factor preserving their relative size.

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

Fig 3 - Quantization table

We observe that the locations (5, 2) and (4, 3) or (1, 2) and (3, 0) have identical values, therefore we choose them for comparison. The DCT block will encode a "1" if Pk(i1, j1) > Pk(i2, j2); otherwise it will encode a "0". The coefficients are then swapped if the relative size of each coefficient does not agree with the bit that is to be encoded.

Following is a list of **attacks** against which watermarking system could be judged. We do not make a difference between intentional and unintentional processing.

JPEG compression: JPEG is currently one of the most widely used compression algorithms for images and any watermarking system should be resilient to some degree of compression.

Geometric transformations:

Horizontal flip: Many images can be flipped without losing any value. Although resilience to flipping is usually straightforward to implement only very few systems do survive it.

Rotation: Small angle rotation, often in combination with cropping, does not usually change the commercial value of the image but can make the watermark undetectable. Rotations are used to realign horizontal features of an image and it is certainly the first modification applied to an image after it has been scanned.

Cropping: In some cases, infringers are just interested by the "central" part of the copyrighted material, moreover more and more Web sites use image segmentation, which is the basis of the "Mosaic" attack. This is of course an extreme case of cropping.

Scaling: This happens when a printed image is scanned or when a high resolution digital image is used for electronic applications such as Web publishing. This should not be neglected as we move more and more toward Web publishing. Scaling can be divided into two groups, uniform and non-uniform scaling. Under uniform scaling we understand scaling which is the same in horizontal and vertical direction. Non-uniform scaling uses different scaling factors in horizontal and vertical direction (change of aspect ratio). Very often digital watermarking methods are resilient only to uniform scaling.
Deletion of lines or columns: This attack is very efficient against any straightforward implementation of spread-spectrum techniques in the spatial Domain. Removing k samples at regular intervals in a pseudo random sequence (hence shifting the next ones) typically divides by k the amplitude of the cross correlation peak with the original sequence.
Generalized geometrical transformations: A generalized geometrical transformation is a combination of non-uniform scaling, rotation, and shearing.
Random geometric distortions (StirMark): Image-watermarking tools, which do not survive them, should be considered unacceptably easy to break.
Geometric distortions with JPEG: Rotation and scaling alone are not enough they should be also tested in combination with JPEG compression. Since most artists will first apply the geometric transformation and then save the image in a compressed format. It makes sense to test robustness of watermarking system to geometric transformation followed by compression.. However experience from professionals shows that "quality factors" down to 70% are reasonable. Artists seem to use JPEG extensively as well as resizing.

TYPES of watermarking algorithms:

- Non-blind- use the original signal
- Semi-blind- does not use the original signal but use some side information and/or the original watermark.
- Blind- does not use the original signal or any side information (most challenging).

2.2 **LITERATURE SURVEY**

Watermark in color image by Ren-Junn Hwang, Chuan-Ho Kao and Rong-Chi Chang, Department of Computer Science and Information Engineering, TamKang University, Tamsui, Taipei, 251, Taiwan, R.O.C.

There are more and more productions to be saved as digital form. In digital world, we can keep the production will not going off forever. But it also has some disadvantages that people can do a copy very easily. Watermark is an important protection method in digital media nowadays. When one media was public or put on the network, it is very easy to be copied or misappropriated. The author can prove that he own the media by use open algorithm and security key to extract the watermark. So one watermark technique must resist some attacks and cannot influence the quality of image. It is usually used to embed watermark in spatial domain and frequency domain. Each of them has specialized skills. In this paper, the authors have proposed an image watermark technique based on spatial domain in color image. The algorithm embeds a watermark in saturation on the HSI space. It is

easy to embed and cannot be detect easily. It can save the high quality with image. Also they have shown some experimental results in this paper to prove their method can resist some attack.

DCT-based Watermark Recovering without Resorting to the Uncorrupted Original Imageby A. Piva, M. Barni, F. Bartolini, V. Cappellini, Dipartimento di Ingegneria Elettronica Universit`a di Firenze, International Conference on Image Processing (ICIP '97) 1997 IEEE
In this paper a new watermarking technique to add a code to digital images is presented. The method operates in the frequency domain embedding a pseudo-random sequence of real numbers in a selected set of DCT coefficients. Watermark casting is performed by exploiting the masking characteristics of the Human Visual System, to ensure watermark invisibility. The embedded sequence is extracted without resorting to the original image, so that the proposed technique represents a major improvement to methods relying on the comparison between the watermarked and original images.

Experimental results demonstrate that the watermark is robust to most of the signal processing techniques and geometric distortions.

A sequence of pseudo-random real numbers having normal distribution is embedded in a set of DCT coefficients, selected by arranging the DCT coefficients in a zigzag scan like in the JPEG algorithm, and by extracting the first L + M coefficients; the lowest L coefficients are skipped to preserve the perceptual invisibility, and the watermark is embedded in the following M coefficients. After embedding, the watermark is adapted to the image to be signed by exploiting the masking characteristics of the Human Visual System in order to achieve watermark invisibility without diminishing its robustness. Experimental results demonstrate that the watermark is robust to several signal processing techniques and geometric distortions, including JPEG compression, low pass and median filtering, histogram equalization and stretching, Gaussian noise addition, resizing, cropping and multiple watermarking. Future research will focus on color image watermarking (currently color images are watermarked by simply processing the image luminance, thus ignoring the correlation between image bands); more experimental work is needed to look for the optimum selection of the mark length and its optimum positioning in the DCT spectrum. Also the maximum number of marks that can be generated without compromising the algorithm robustness requires deeper investigation.

Improved Robust Watermarking in DCT Domain for Color Images by Xiaoqiang Li, Xiangyang Xue, Department of Computer Science and Engineering Fudan University, 18th International Conference on Advanced Information Networking and Application (AINA’04) 2004 IEEE
This paper proposes a new DCT domain watermarking expressly devised for RGB color images based on the diversity technique in communication system. The watermark is hidden within the data in the same sequence by modifying a subset of block DCT coefficients of each color channel. Detection is based on a combination method by taking into account the information conveyed by three color channels.

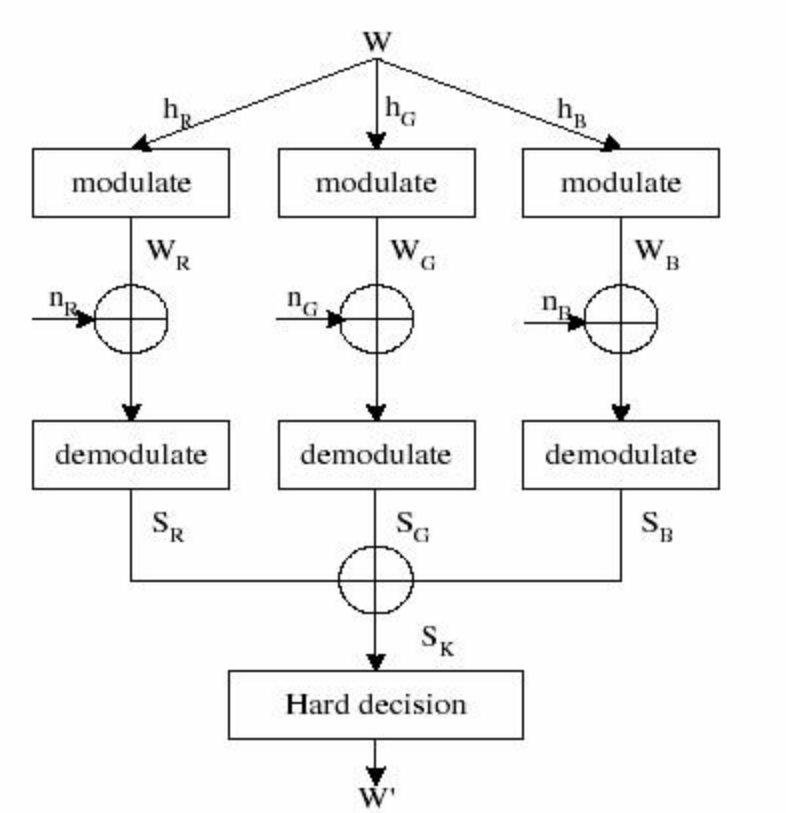

Fig 4 - Diversity-based watermarking

A Novel DCT-based Approach for Secure Color Image Watermarking

Narges Ahmidi, Reza Safabakhsh Amirkabir University of Technology, International Conference on Information Technology: Coding and Computing (ITCC'04) 2004 IEEE

In this paper, focusing on visually meaningful color image watermarks, we construct a new digital watermarking scheme based on the Discrete Cosine transformation. The proposed method uses the sensitivity of human eyes to adaptively embed a watermark in a color image. In addition, to prevent tampering or unauthorized access, a new watermark permutation function is proposed, which causes a structural noise over the extracted watermark. Also, we have proposed a procedure to eliminate this noise to decrease false positives and false negatives in the extracted watermark. The experimental results show that embedding the color watermark adapted to the original image produces the most imperceptible and the most robust watermarked image under geometric and volumetric attacks.

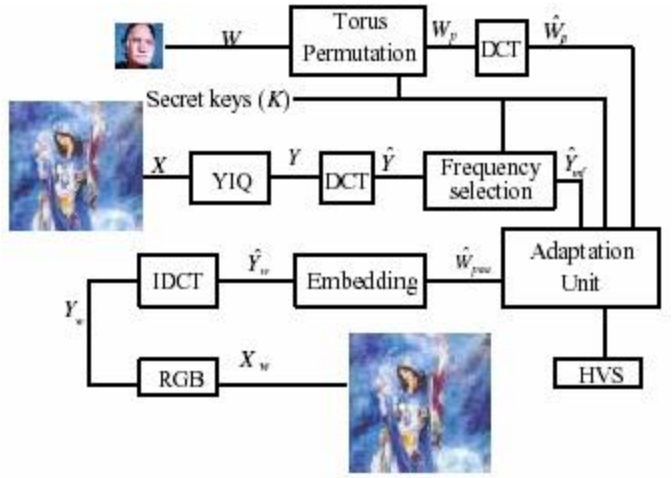

Fig 5 - Proposed Watermarking algorithm

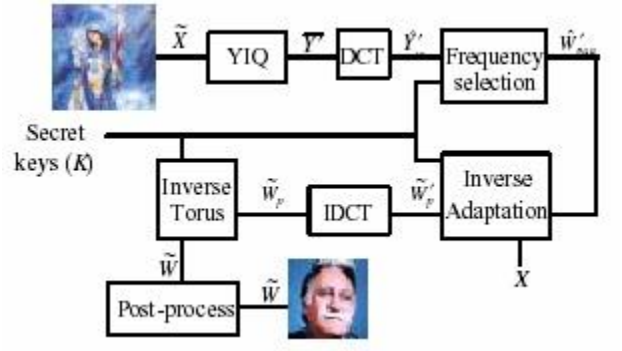

Fig 6 - Proposed Extraction algorithm

The experimental results showed that the proposed scheme was the most robust method, especially for higher lossy compression ratios. Also, on the average, it was the most robust system under blurring attacks. Indeed, the watermarked image robustness did not decrease when blurring increased due to larger filter size. In addition, the proposed scheme was the most robust method under image cropping attacks.

An Efficient Method to Improve the Quality of Watermarked Cover Image by Wen-Shyong Hsieh, Chuan-Fu Wu, Jen-Yi Huang, Jyh-Long Lin, Buh-Yun Sher, Department of Computer Science and Engineering National Sun Yat-Sen University,Taiwan, International Conference on Distributed Computing Systems Workshops (ICDCSW'02) 2002 IEEE

In this paper, a general concept called n+k/n method is introduced. In n+k/n method, a special mapping function is defined to map an intermediate set with n+k bits into n bits information set. In the embedding process, the intermediate set is embedded into cover image rather than embedding the information set. If the distance between the features of cover image and the bits of intermediate set is less than that between the features and information bits, the better cover image quality can be gained. According to the idea of n+k/n method, a special case called n+1/n method is proposed. In this method, the mapping function is an exclusive-or operation. When an information set is given, two sets which satisfy the mapping function can be got. The one which has smaller distance from feature bits is selected as intermediate set. In the paper, it is proved that the maximum distance between the intermediate set and feature set is less than the average distance between the information set and the

feature set. The reduction rate of feature modification for n+1/n method will reach 25%, and the improving quality in embedded cover image is more than 2.5db.

2.3 **REVIEW**

Serial #	Name of the research paper	Name of the author(s)	Overview of the paper	Inference/Conclusion
1	Watermark in color image	Ren-Junn Hwang, Chuan-Ho Kao and Rong-Chi Chang	In this paper, the authors have proposed an image watermark technique based on spatial domain in color image.	Embedding a watermark in saturation on the HSI space makes it easy to embed and cannot be detected easily. It can save the image with high quality.
2	Improved Robust Watermarking in DCT Domain for Color Images	Xiaoqiang Li, Xiangyang Xue	Here the watermark is hidden within the data in the same sequence by modifying a subset of block DCT coefficients of each color channel.	It modulates and demodulates all the three color channels and hence becomes difficult to harm the watermark.
3	DCT-based Watermark Recovering without Resorting to the Uncorrupted Original Image	A. Piva, M. Barni, F. Bartolini, V. Cappellini	A sequence of pseudo-random real numbers is embedded in a set of DCT coefficients and by extracting the first L + M coefficients, watermark casting is performed by exploiting the masking characteristics of the Human Visual	Using the pseudorandom sequences for embedding the watermark enhances the robustness of their algorithm. Their experimental results show resistance to various strong attacks also.

Serial #	Name of the research paper	Name of the author(s)	Overview of the paper	Inference/Conclusion
			System, to ensure watermark invisibility	
4	A Novel DCT-based Approach for Secure Color Image Watermarking	Narges Ahmidi, Reza Safabakhsh	To prevent tampering or unauthorized access, a new watermark permutation function is proposed. Additionally they have proposed a procedure to eliminate this noise to decrease false positives and false negatives in the extracted watermark.	Experimental results have proved their algorithm is very robust to geometric attacks, blurring attacks, especially for higher lossy compression ratios. Permutation made algorithm very robust.
5	An Efficient Method to Improve the Quality of Watermarked Cover Image	Wen-Shyong Hsieh, Chuan-Fu Wu, Jen-Yi Huang, Jyh-Long Lin, Buh- Yun Sher	The n+k/n method is introduced and the intermediate set is embedded into cover image rather than embedding the information set. If the distance between the features of cover image and the bits of intermediate set is less than that between the features and information bits, the better cover image quality can be gained.	The mapping function is an exclusive-or operation which is easy to implement. Here they have proved that the maximum distance between the intermediate set and feature set is less than the average distance between the information set and the feature set is less than the average distance between the information set and the feature set which is obviously very good.

Source: http://www.botskool.com/programming-tutorials/fourth-year-projects/digital-image-watermarking/digital-image-watermarking-page-2