Digital Image Watermarking and Compression

Win Htun, Thi Thi Soe
University of Computer Studies (Manadalay)
winhtunucsm@gmail.com

Abstract

The growth of networked multimedia data such as images has complicated for authentication, copyright protection, broadcasting and integrity. Digital image watermarking is effective approach to distribute picture over the internet with privacy. Image compression is also needed to transmit over the Word Wide Web. This paper is aimed to develop the digital image watermarking and compression system. The output of the system displays whether the watermark can be detected or not. An effective watermark must withstand image compression, because images placed on the Internet or in databases are almost always compressed– sometimes to a very low data rate. Since compression tends to weaken a watermark in an image, it is important to find ways to maximize the amount of watermark that remains in the image after compression. Common image adaptive watermarks operate in the transform domain (DCT); the same domains are also used for popular image compression techniques.

1. Introduction

Digital images are now widely distributed on the Internet and via CD-ROM. Digital imaging allows an unlimited number of copies of an "original" to be easily distributed and/or forged. This presents problems if the image is copyrighted. The protection and enforcement of intellectual property rights has become an important issue in the "digital world." Many approaches are available for protecting digital data; traditional methods include encryption, authentication and time stamping. This paper focuses on invisible watermarks that are designed to exploit perceptual information in the watermarking process.

This paper describes image watermarking from a technical perspective. It is important to note that any technique that allows a user to assert their ownership of any digital object must also be placed in the context of intellectual property right law. In the final analysis how "well" a watermarking technique works depends on how effectively the technique protects an owner's intellectual property rights in a court of law. Overviews of digital watermarking are presented in [1]. The objective of the paper is to develop digital image watermarking and compression.

2. Related Work

Digital watermarking can link some useful information to the multimedia data by embedding watermark into the original data. An attacker cannot remove the embedded watermark easily. Publishing companies who commercially distribute their images could watermark them to prevent unauthorized distribution.

A watermark is a secret code or image incorporated into an original image. The use of perceptually invisible watermarks is one form of image authentication. A watermarking algorithm consists of three parts: the watermark, the marking algorithm and the verification algorithm. Each owner has a unique watermark. The marking algorithm incorporates the watermark into the image. Many digital watermarking techniques rely on random sequences into to an image's spatial or spectral representation. One approach adds a modified maximal-length linear shift register sequence (m-sequence) to the pixel data. User identifies the watermark using correlation techniques. Watermarks can also modify the image's spectral or transform coefficients directly. These algorithms most often modulate DCT coefficients according to a sequence known only to the owner [2].

There are several advantages to combine, at one end the image coding and watermark embedding scheme and at the other end, the image decoding and watermark extraction. In this paper, we present to encode the binary message, the watermark is placed in the transformed image prior to the uniform quantization used in the compression algorithm [3].

The original host image is needed in watermark detection mainly for extracting the featured coefficients necessary for robust detection and determining the value of one bit of the watermark spread into a block [4].

3. Watermark Theory

A watermark on a bank note has a different transparency than the rest of the note when a light is shined on it. Currently there are various techniques for embedding digital watermarks. Digital watermarks are added to images or audio data in such a way that they are invisible or inaudible unidentifiable by human eye or ear. Digital

watermarking is the content protection method for the multimedia era.

3.1. Data Hiding of Multimedia

With the recent growth of networked multimedia systems, techniques are needed to prevent the illegal copying, forgery and distribution of digital audio, images and video. It is also desire able to determine where and by how much the multimedia file has been changed from the original. One way to improve one's claim of ownership over an image, for instance, is to place a low-level signal directly into the image data. This signal, known as a digital watermark, uniquely identifies the owner and can be easily extracted from the image [5].

3.2. Type of Data Hiding Techniques

Copyright protection appears to be one of the first applications digital watermarking was targeted for. The metadata in this case contains information about the copyright owner. It is imperceptibly embedded as a watermark in the cover work to be protected. If users of digital content (music, images, and video) have an easy access to watermark detectors, they should be able to recognize and interpret the embedded watermark [6].

Annotation Watermark provides a technique for embedding metadata about an image into the image itself. This watermark can contain relevant information about the image such as search keywords, collection date, location, author commentary, etc. Annotation Watermarks are imperceptible and public, and should also be as robust as possible [7].

3.3. Classification of Watermarking Schemes

Digital watermarking is being used in numerous applications. Most of the current applications are devoted to copyright protection. It has the following purposes in general:

(1) Covert Communications: These are mainly applications of steganography. In military and intelligence applications, people would like to send messages to each other without being detected.

(2) Authentication: Sometimes it is necessary to verify the authenticity of input data, i.e., to determine whether the data are original, fake, or the altered version of the original. For authentication purposes, fragile watermarks seem to be a good solution.

(3) Identification of Ownership: Robust water - marking algorithms are developed to identify the ownership of digital media. In this kind of applications, a movie producer selling its products in digital formats is subject to copyright piracy. . In such situations, original producers would like to have legally proof that they are the real owners. A well-designed robust watermarking scheme is a possible solution to these cases [8].

4. System Design

The system design of digital image watermarking and compression consists of five modules:

Discrete Cosine Transformation (DCT)
Embedding Watermark
JPEG Compression
Extracting Watermark
Computing Similarity

This can be seen in Figure 1. In this system, Image compression system is developed. The DCT equation (EQ. 1) computes the i, jth of the DCT an image

$$D(i,j)=\frac{1}{\sqrt{2N}}C(i)(j)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}P(x,y)\cos\left[\frac{(2x+1)i\pi}{2N}\right]\cos\left[\frac{(2y+1)}{2N}\right] \quad (1)$$

$$C(u)=\begin{cases}\frac{1}{\sqrt{2}} & \text{if } u=0\\ 1 & \text{if } u>0\end{cases} \quad (2)$$

P(x,y) is the x,yth element of the image represented by the matrix p. N is the size of the block that the DCT is done on. The equation calculates one entry (i,jth) of the transformed image from the pixel values of the original image matrix. For the standard 8x8 block that JPEG compression uses. N equals 8 and x and y range from 0 to 7. Therefore D(i,j) would be as in Equation (3).

$$D(i,j)=\frac{1}{4}C(i)C(j)\sum_{x=0}^{7}\sum_{y=0}^{7}P(x,y)\cos\left[\frac{(2x+1)i\pi}{16}\right]\cos\left[\frac{(2y+1)i\pi}{16}\right] \quad (3)$$

Because the DCT uses cosine functions, the resulting matrix depends on the horizontal, diagonal, and vertical frequencies.

To get the matrix form of Equation (1), use the following equation

$$T_{ij}\begin{cases}\frac{1}{\sqrt{N}} & \text{if } i=0\\ \sqrt{\frac{2}{N}}\cos\left[\frac{(2j+1)i\pi}{2N}\right] & \text{if } i>0\end{cases} \quad (4)$$

Because the DCT is designed to work on pixel values ranging from -128 to 127, the original block is "leveled off" by subtracting 128 from each entry. The Discrete Cosine Transform is accomplished by matrix multiplication.

$$D = TMT' \quad (5)$$

It is important to note that the human eye is most sensitive to low frequencies, and results from the quantization step will reflect this fact.

$$C_{ij} = round\left(\frac{D_{ij}}{Q_{ij}}\right) \quad (6)$$

Reconstruction of image begins by decoding the bit stream representing the quantized matrix C. Each element of C is then multiplied by the corresponding element of the quantization matrix originally used.

$$R_{i,j} = Q_{i,j} \times C_{i,j} \qquad (7)$$

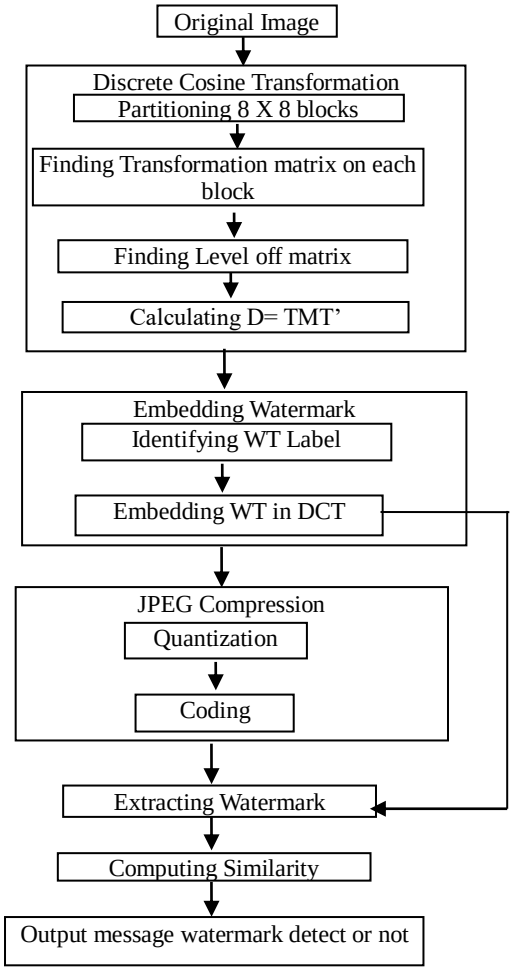

Figure 1. Component of System Design

Finally, 128 is added to the element of that result, giving us the decompressed JPEG version N of original 8x8 image block M.

$$N = round\left(T' R T\right) + 128 \qquad (8)$$

This is remarkable result, considering that nearly 70% of the DCT coefficients were discard prior to image block decompression /reconstruction. Given that similar results will occur with the rest of the blocks that constitute the entire image, it should be no surprise that the JPEG image will be scarcely distinguishable from the original. Remember, there are 256 possible shades of gray in a black-and-white picture, and a difference of, say, 10, is barely noticeable to the human eye [9].

4.1. Embedding Watermark

In visible watermarking, the information is visible in the picture or video. Typically, the information is text or a logo which identifies the owner of the media. In invisible watermarking, information is added as digital data to audio, picture or video, but it cannot be perceived as such (although it is possible to detect the hidden information). An important application of invisible watermarking is to copyright protection systems.

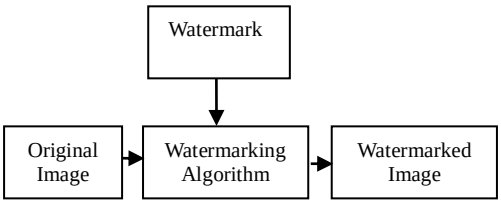

Figure 2. Diagram of Watermark Algorithm

4.2. Embedding WT

Watermark is embedded in the input image which comprises of two parts. They are identifying **WT** label and embedding WT in DCT. In our system, we identify WT label as a watermark which is 8×8 block as shown in the figure.

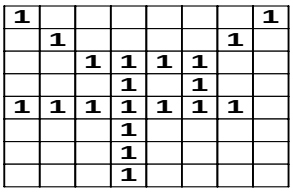

Figure 3. WT Label

4.3. JPEG Compression

A remarkable and highly useful feature of the JPEG process is that in this step, varying levels of image compression and quality are obtainable through selection of specific quantization matrices. This enables the user to decide on quality levels ranging from 1 to 100, where 1 gives the poorest image quality and highest compression, while 100 gives the best quality and lowest compression. As a result, the quality/compression ratio can be tailored to suit different needs.

Subjective experiments involving the human visual system have resulted in the JPEG standard quantization matrix. With a quality level of 50, this matrix renders both high compression and excellent decompressed image quality. For a quality level greater than 50 (less compression, higher image quality), the standard quantization matrix is multiplied by (100-quality level)/50. For a quality

level less than 50 (more compression, lower image quality), the standard quantization matrix is multiplied by 50/quality level. The scaled quantization matrix is the rounded and clipped to have positive integer values ranging from 1 to 255. For example, the following quantization matrices yield quality levels of 10 to 90.

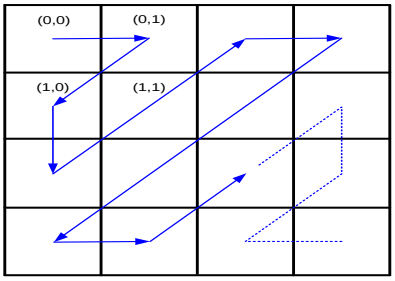

Figure 4. Zig-zag sequence

4.4. Extracting Watermark

The detection process needs the original image for extracting the signature as well as the presence of the watermark image. Original host image is needed in watermark detection mainly for extracting the featured coefficients necessary for robust detection and determining the value of the watermark spread into a block. The general extraction method can be decomposed into different steps. First of all, the host image and the watermarked one are transformed into the steer able pyramid coefficients with the same parameters as in the embedding stage. In order to localize the marked block, the same rule described latter is also available here. Then, the extraction of all signature occurrences is based on a comparison between the block of the two available images. Finally, this system succeeds to extract correctly the signature embedded by averaging all the occurrences. To extract watermark from image we need to compare the watermarked image with compressed watermarked image. In this method we need to input the original image, watermarking text and threshold and the output watermarking text.

Algorithm for Extraction Watermark in DCT

Step1: Input original image, image watermark and threshold.
Step2: Decompose image by using DCT transform.
Step3: Extract data from in level one.
Step4: Sort data in each sub bands in original image to extract the max coefficients and location for coefficients.
Step5: Compare between coefficients in two images depending on location of them,

If coefficient embedding > coefficient original then the data store in it is 1.

If coefficient embedding < = coefficient original then the data store in it is 0.

Step6: Compare between binary bits that generate three copies of extraction the watermark bits, if difference is more than half its mean this system get the correct value.
Step7: Display watermark text.

4.5. Computing Similarity

This section proves the similarity of watermarked image and un-watermarked image. The similarity of watermarked compressed and un-watermarked compressed image will also be computed with various threshold values in this system.

The evaluation of digital watermarking schemes can provide detailed information for watermark designer or end users. End users are mostly not interested in detailed information. They want to know if a given digital watermarking algorithm can be used for their application scenario, and if yes, which parameter sets seems to be the best.

Figure 5. Original Input Image

In this paper implement into many images, this result for one image by DCT transform, as shown in figure (5) the original image.

The image dimensions are 264x264, Image size before compression: 204.2 kb, Data Payload: 208 bit. The implementation in DCT method gives the result for PSNR after embedding and after low-pass, high-pass filters shown in table (1) and figure (6).

Table1. PSNR for Flower Image in DCT

Threshold	PSNR After Embedding	PSNR After LowPass Filter	PSNR After HighPass Filter
1	59.626	46.656	46.167
2	56.616	46.639	46.154
3	54.855	46.612	46.132
4	53.605	46.574	46.102
5	52.636	46.527	46.064
6	51.844	46.470	46.018
7	51.175	46.405	45.965
8	50.595	46.333	45.906
9	50.084	46.253	45.840
10	49.626	46.167	45.769
11	49.212	46.077	45.693

The result of PSNR depends on threshold, when the threshold increases PSNR decreases in the same image.

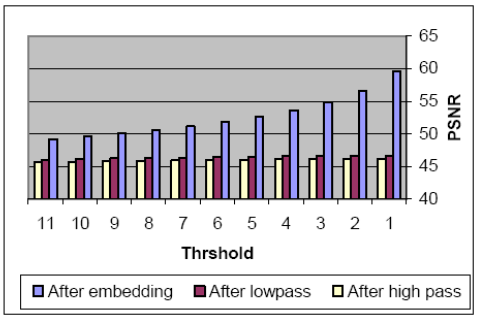

Figure 6. Relation PSNR after Embedding, Low-pass and High-pass

Apply image in implementation for JPEG. The results are discussed in table (2) and Figure (7).

Table2. Flower Image after JPEG in DCT

Threshold	Quality	Image Size	Comp. Ratio	PSNR	Success rate
1	88.0 87.9	51.5 37.5	3.96 5.44	59.597 50.959	100% 89.9%
2	87.9	37.5	5.44	50.816	98.5%
3	87.9 85.0 80.0 75.0 70.0	37.3 36.3 33.8 32.0 29.9	5.47 5.62 6.04 6.38 6.82	50.564 50.445 50.126 49.900 49.707	100% 100% 100% 100% 99.5%
4	70.0 65.0 60.0	29.9 27.8 25.5	6.82 7.34 8.00	49.535 49.391 48.890	100% 100% 99.5%
5	60.0 55.0 50.0 45.0	25.3 23.0 21.1 19.0	8.07 8.87 9.67 10.74	48.644 48.163 47.945 47.662	100% 100% 100% 99.5%
6	45.0 40.0	19.2 17.1	10.63 11.94	47.531 47.387	100% 99.0%
7	40.0 35.0	17.1 15.0	11.94 13.61	47.252 46.890	100% 98.5%
8	35.0 30.0 25.0	14.9 12.9 10.7	13.70 15.82 19.08	46.782 46.377 46.001	100% 100% 96.6%
9	25.0	10.8	18.90	45.950	99.0%
10	25.0	10.7	19.08	45.850	99.5%
11	25.0	10.8	18.90	45.769	100%

In this table when you select threshold (1) and quality (88.0) the image size is (51.5) and compression ratio (3.96), this shows the watermark extraction is completely (success rate is 100%) and in the same threshold when the quality deceases (87.9), image size decrease (37.5) and compression ratio (5.44) increases. This shows the watermark bit success rate (89.9%) , the solution for this case is by increasing the threshold can see that in threshold (2), the success rate is (98.5%) in (87.9) quality and threshold (3), the success rate is (100%) in (87.9) quality. When increase the threshold the PSNR decreases.

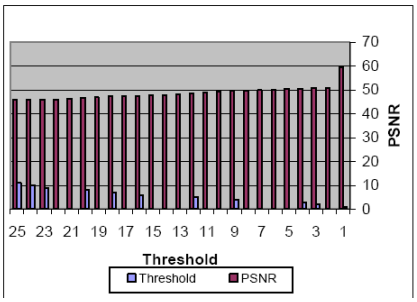

Figure 8. Relation between threshold and PSNR

4.6. Output Message

Figures show a general watermarking scheme. A watermark is called robust if it resists a designated class of transformations. Robust watermarks may be used in copy protection application to carry copy and access control information.

Watermark Transmission:

For transmission, the watermark **W** is generated as a pseudo-random sequence to ensure statistical invisibility. Signal information, such as DCT coefficients, are extracted from the original image **I** and embedded into the information. The watermarked image **I'** is formed with no visible differences between **I** and **I'**.

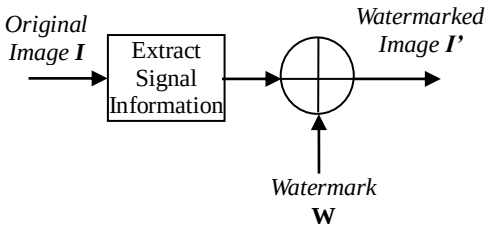

Figure 9. Watermark Transmission

Watermark Detection:

For watermark detection, a suspected image J is taken and its signal information is obtained. A suspected watermark V is extracted based on knowledge of the original image I and the watermark W. A similarity measure S is performed on V and W. Popular measures include the cross-correlation and correlation coefficient. Finally, S is compared to a threshold τ. If S is larger than the threshold, then the watermark W is detected. Otherwise, no watermark is detected.

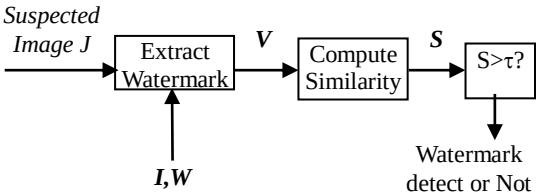

Figure 10. Watermark Detection

5. Implementation

In this system we discussed Image compression and the Discrete Cosine Transform system and implementation steps used in this system.

Figure 11. Gray Scale Image

In this system, Image compression system is developed**.**

The input image is RGB (true color image type) the input format type is jpeg. JPEG is the current international standard for color still image compression. Watermarked image is gray and deeply dark. Watermarked Compressed image is more deeply dark.

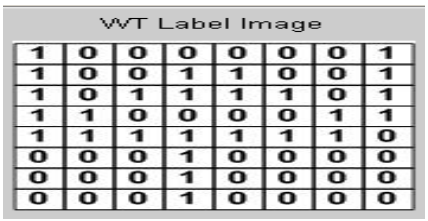

Figure 12. Watermark Label Image

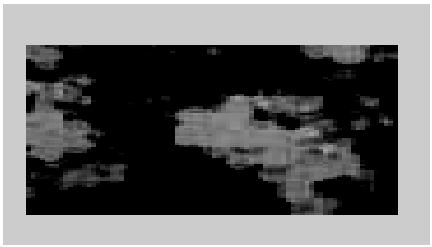

Figure 13. Watermark Image

Figure 14. Watermark Compressed Image

6. Conclusion

A digital watermark should be perceptually invisible to prevent obstruction of the original image and statistically invisible so it cannot be detected or erased. Watermark extraction should be fairly simple. Otherwise, the detection process requires too much time or computation. Watermark detection should be accurate. False positives, the detection of a no marked image, and false negatives, the non-detection of a marked image, should be few. Numerous watermarks can be produced. Otherwise, only a limited number of images may be marked. Watermarks should be robust to filtering, additive noise, compression, and other forms of image manipulation. The watermark should be able to determine the true owner of the image. This system is important to protect copyright and the attacker can not remove the embedded watermarked easily.

References

[1] R.B. Wolfgang, C.I. Podilchuk and E.Delp, "Perceptual watermarks for images and video," to appear in the *Proceedings of the IEEE*, May, 1999.

[2] R.B. Wolfgang and E.J. Delp," A Watermarking Technique for Digital Imagery: Further Studies," Video and Image Processing Laboratory (*VIPER*) School of Electrical and Computer Engineering Purdue University

[3] A. Makhlou_, A.O. Zaid, A. Bouallegue and R. Bouallegue," Quantization Watermarking Integrated In A Wavelet Compression System", SYSCOM IT-03 –ENIT-El Manar University.

[4] F. DRIRA, F. DENIS, A. BASKURT," Image watermarking technique based on the steerable pyramid transform", LIRIS, Laboratoire d'InfoRmatique en Image et Systèmes d'information FRE 2672 CNRS, INSA Lyon, UCB Lyon 1, EC Lyon, Univ. Lyon 2..

[5] E.J. Delp," Multimedia Security Research", Purdue University.

[6] E. Muharemagic and B. Furht, " Multimedia Security: Watermarking Techniques, "Department of Computer Science and Engineering Florida Atlantic University.

[7] D.W. Stouch," A Survey of Practical Applications in Image Watermarking," Boston University Metropolitan College.

[8] Zur Arranging des akademischen Grades Dr.Ing, "Digital_Watermarking Based Authenti- cation Techniques for Real-Time Multimedia Communication".

[9] C. Ken and G. Peter," Image Compression and the Discrete Cosine Transform," Math45 College of the Redwoods.