Reversible Watermarking Method of Digital Images

S.Bhagya Rekha, T Siva Shankar
Department of Information Technology
Teegala Krishna Reddy Engineering College
bhagyarekha2001@gmail.com,
sivatalari@yahoo.com

Abstract— **Basically in comparing two images to see if they were identical was to check the size of each. If they don't match then we know almost immediately that the images are not identical. It would be quicker if I could somehow compare a 'hash' of each image to see if they were identical. As we know, a hash is a unique value of a fixed size representing a large amount of data, in this case our image data. Hashes of two images should match if and only if the corresponding images also match. Small changes to the image result in large unpredictable changes in the hash. In This paper the concept the concept is to takes a byte array of data as an input parameter and produces a 56 bit hash of that data. By computing and then comparing the hash of each image, I would be quickly able to tell if the images were identical or not. The problem would be to convert the image data stored in the GDI+ Bitmap objects to a suitable form, namely a byte array. The main aim of this paper Image Organizing – Explorer style, Image converter, Applying Filters, Implement watermarking.**

Keywords-Digital Watermarking, Filters, Image Comparison, Image Conversion

I. INTRODUCTION

Digital watermarking has grown explosively in the last few years. It embeds an invisible (in some cases, visible) mark (payload) into digital content for the purpose of copyright communication and protection, content authentication, counterfeit deterrence, forensic tracking, connected content, or broadcast monitoring, etc. For a detailed review of digital watermarking, we refer to 1 – 6

From the application point of review, most digital watermarking methods can be divided into two categories: robust watermarking and fragile watermarking. Robust watermarking is mainly aimed at copyright protection. Here “robust” means the embedded watermark should be very resistant to various signal processing operations. On the other hand, fragile watermarking is aimed at content authentication. A fragile watermark will be altered or destroyed when the digital content is modified. As a special subset of fragile watermarking, reversible watermarking has drawn lots of attention recently. Reversible watermark, (which is also called 4, 7 – 1 2 lossless watermark, invertible watermark, erasable watermark), has an additional advantage such that when watermarked content has been detected to be authentic, one can remove the watermark to retrieve the original, unwatermarked content. Such reversibility to get back unwatermarked content is highly desired in sensitive imagery, such as military data and medical data.

In this paper, we present a reversible watermarking method of digital images. Our method can be applied to digital audio and video as well. Compared with other reversible watermarking methods, our method employs an integer wavelet transform to losslessly remove redundancy in a digital image to allocate space for watermark embedding. The embedding algorithm starts with a reversible color conversion transform. Then, we apply the integer wavelet transform to one (or more) decorrelated component. The purpose of both the reversible color conversion transform and the integer wavelet transform is to remove irregular redundancy in the digital image, such that we can embed regular redundancy into the digital image, for the purpose of content authentication and original content recovery. The regular redundancy could be a hash of the image, a compressed bit stream of the image, or some other image content dependent watermark. In the integer wavelet domain, we look into the binary representation of each wavelet co e cent and embed an extra bit to “expandable” wavelet coincident. Besides original content retrieval bit streams, an SHA-56 hash of the original image will also be embedded for authentication purpose.

II . OVERVIEW OF WATER MARKING TECHNIQUES

Current watermarking techniques described in the literature can be grouped into three main classes. The first includes the spatial domain methods, which embed the watermark by directly modifying the pixel values of the original image. The second class includes the transform domain methods, which embed the data by modulating the transform domain signal coefficients. The transform domain techniques have been found to have the greater robustness, when the watermarked signals are tested after having been subjected to common signal processing. The third class is the feature domain technique. This technique takes into account region, boundary and object characteristics. Such watermarking technique may give additional advantages in terms of detection and recovery from geometric attacks, compared to previous approaches.

2.1 Spatial Domain Technique

The most straightforward method of watermark embedding would be to embed the watermark into the least significant bits of the cover object [13]. Given the extraordinarily high channel capacity of using the entire cover for transmission in this method, a smaller object may be embedded multiple times. Even if most of these were lost due to attacks, a single surviving watermark would be considered a success. LSB substitution however despite its simplicity brings a host of drawbacks. Although it may survive transformations such as cropping, any addition of noise or lossy compression is likely to defeat the watermark. An even better attack would be to simply set the LSB bits of each pixel to one fully defeating the watermark with negligible impact on the cover object. Furthermore, once the algorithm is discovered, an intermediate party could easily modify the embedded watermark. LSB modification proves to be a simple and fairly powerful tool, however lacks the basic robustness that watermarking applications require. Another technique for watermark embedding is to exploit the correlation properties of additive pseudorandom noise patterns as applied to an image [14]. A pseudo-random noise (PN) pattern W(x, y) is added to the cover image I(x, y), according to the equation 1.

$Iw(x,y) = I(x,y) + k^* W(x,y)$ …………………..(1)

In equation.1, k denotes a gain factor, and IW the resulting watermarked image. Increasing k increases the robustness of the watermark at the expense of the quality of the watermarked image. Rather than determining the values of the watermark from "blocks" in the spatial domain, we can employ CDMA spread-spectrum techniques to scatter each of the bits randomly throughout the cover image, increasing capacity and improving resistance to cropping [14] . To detect the watermark, each seed is used to generate its PN sequence, which is then correlated with the entire image. If the correlation is high, that bit in the watermark is set to "1", otherwise a "0". The process is then repeated for all the values of the watermark. CDMA improves on the robustness of the watermark significantly, but requires several orders more of calculation.

Algorithm for Spatial Domain

If the watermarked image is unchanged, then d = 0. When is larger than a defined tolerance the block fails the watermark test. A larger threshold provides more robustness but increases the probability of missing a forgery the authors revised this watermarking technique to improve security and localization. Localization is the ability to identify where in the image any changes have occurred. The block size is 8x8 pixels and each block is formed as follows:

- A large span m-sequence (n = 96) is generated with the first 128 bits skipped.
- The next 64 bits are inserted in the first block of the watermark column by column. The next m bits are skipped.
- The procedure repeats for the remaining blocks.

With the advances in networked multimedia technology, reproduction of multimedia data has become easier. This has created a need for the copyright protection of the data.

2.2 Digital Watermarking

Is the technique in which a visible / invisible signal (watermark) is embedded in the data for copyright protection? Here, we describe a visible watermarking scheme

Digital watermarking is defined as a process of embedding data (watermark), into a multimedia object to help to protect the owner's right to that object. The embedding data (watermark) may be either visible or invisible. In visible watermarking of images, a secondary image, the watermark, is embedded on a primary image such that the watermark is intentionally perceptible to a human observer; whereas in the case of invisible, the embedded image data that is not perceptible, but may be extracted by a computer program. Some of the desired characteristics of visible watermarks are listed below [2,3].

- A visible watermark should be obvious in both color and monochrome images.
- The watermark should spread in a large and important area of the image in order to prevent its deletion by clipping.
- The watermark should be visible yet must not significantly obscure the image details beneath it.
- The watermark must be difficult to remove, rather removing a watermark should be more costly and labor intensive than purchasing the image from the owner.
- The watermark should be applied automatically with little human intervention and labor.

There are very few visible watermarking techniques available in current literature.

The IBM Digital Library Organization has used a visible watermarking technique to mark digitized pages of manuscript form the Vatican archive [5]. Rajmohan [6] proposes a visible watermarking technique in DCT domain. He divides the image into different blocks, classifies these blocks by perceptual classification methods as proposed in [5] and modifies the DCT coefficients of host image as follows.

$X'n = \mu n\ Xn + bn\ Wn$ …………(2)

The µn and bn coefficients are different for different classes of blocks. Xn are the DCT coefficient of the host image blocks and Wn are the DCT co-efficients of the watermark image block.

Here, we propose a visible watermarking scheme that modifies gray values of each pixel of the host image. The modification is based on the local as well as global statistics of the host image. The characteristics of the Human Visual System (HVS) are taken into consideration so that the perceptual quality of the image is not very much affected.

2.3 Proposed Watermarking Technique

The steps for watermark insertion are discussed below.

· The original image I (one to be watermarked) and the watermark image W are divided into blocks (both the images may not be of equal size, but blocks should be of equal size).

· m and s , the global mean and variance of the image I are computed.

· For each block the local statistics mean mn and variance sn are computed.

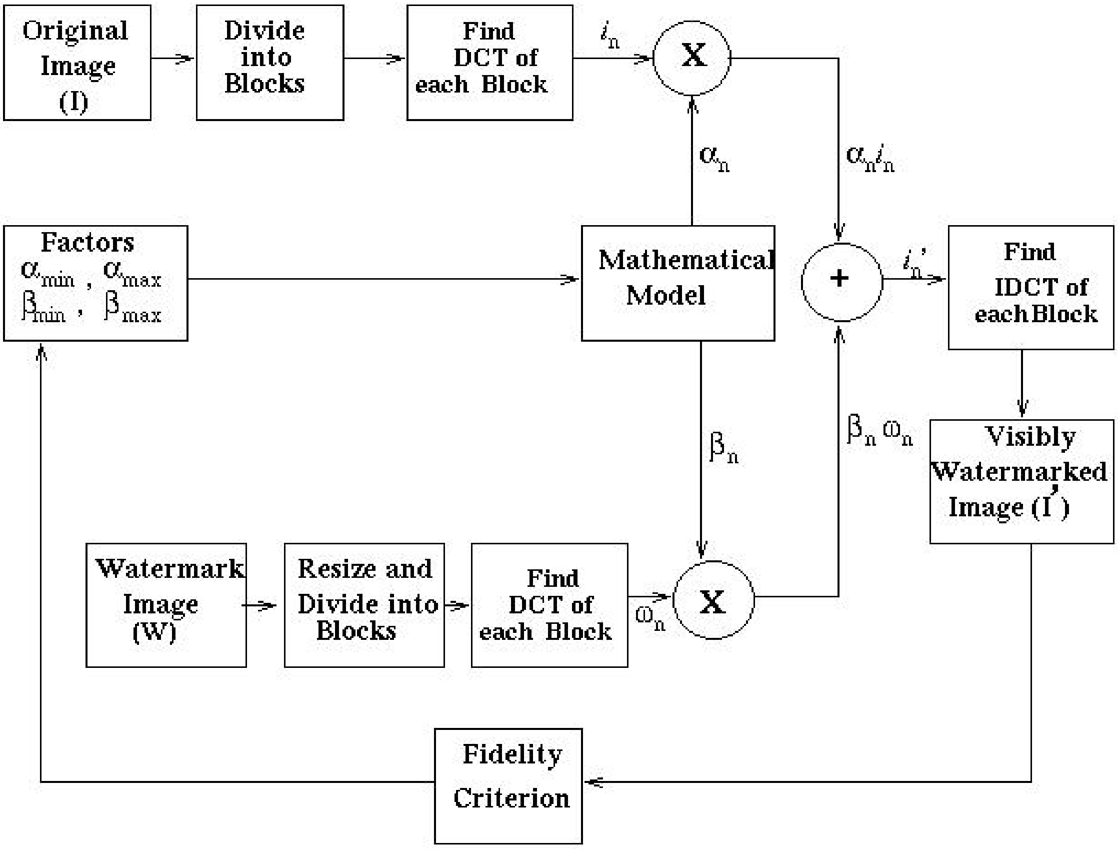

Figure 1: Watermark Insertion Process

· Let in denote the nth block of original image I ,and wn denote the nth block of watermark image W. Denoting the nth block of watermarked image by in', we have,

in' = an .in + bn wn n = 1,2, ……. (3)

where µn and bn are scaling and embedding factors respectively for each block computed as described below.

Figure 1 gives the schematic representation of the insertion process.

The choice of an's and bn's are governed by certain characteristics of Human Visual System (HVS) which for watermark images can be translated into following requirements [7,6- 8].

· The edge blocks should be least altered to avoid significant distortion of the image. So one can add only small amount of watermark gray value in the edge block of host image. This means that scaling factor an should be close to amax , (the maximum value of the scaling factor) and embedding factor bn should be close to bmin (the minimum value of the embedding factor).

· Its also pointed out in [7,6-8] that blocks with uniform intensity (having low variance) are more sensitive to noise than the blocks with non-uniform intensity (having high variance). So one can add less to the blocks with low variance and add more to the blocks with high variance. We assume the scaling factor an is inversely proportional to variance whereas bn directly proportional to variance. · Yet another characteristic of HVS is that the blocks with mid-intensity are more sensitive to noise than that of low intensity blocks as well as high intensity blocks. This means that the an should increase with local mean gray value up to mid gray value and again decrease with local mean gray value. The variation of an with mean block gray value is assumed to be Gaussian in nature. The variation bn with mean gray value is reverse to that of an . Basing on the above discussion we propose the following mathematical model.

For edge blocks
an = amin + (smin (amax - amin)/sn) exp(- ((mn - m m)/s)2 / 2) ….(4),

For other blocks

bn = bmin + (sn (bmax - bmin) / smax) [1 - exp(- ((mn - m)/s)2 / 2)], ….(5)

Where, amin and amax are respectively minimum and maximum values of scaling factor, bmin and bmax are respectively minimum and maximum values of embedding factor, smin and smax are respectively minimum and maximum values of block variances, mn and sn are respectively normalized mean and variance of each block, and m and s are respectively normalized mean & variances of the image.

III. TYPES OF DIGITAL WATERMARKS

Watermarks and watermarking techniques can be divided into various categories in various ways. Watermarking techniques can be divided into four categories according to the type of document to be watermarked as follows:

· Text Watermarking
· Image Watermarking
· Audio Watermarking
· Video Watermarking

In the case of imagery, several different methods enable watermarking in the spatial domain. An alternative to spatial watermarking is frequency domain watermarking.1.6
Extracted c x
Signature (S')
Original
Signature (S)

In other way, the digital watermarks can be divided into three different types as follows: [], [2-3], and [4]

· Visible watermark
· Invisible-Robust watermark
· Invisible-Fragile watermark

Visible watermark is a secondary translucent overlaid into the primary image. The watermark appears visible to a casual viewer on a careful inspection. The invisible-robust watermark is embed in such a way that alternations made to the pixel value is perceptually not noticed and it can be recovered only with appropriate decoding mechanism. The invisible-fragile watermark is embedded in such a way that any manipulation or modification of the image would alter or destroy the watermark. From application point of view digital watermark could be:
· source based or
· destination based.
Source-based watermark are desirable for ownership identification or authentication where a unique watermark identifying the owner is introduced to all the copies of a particular image being distributed. A source-based watermark could be used for authentication and to determine whether a received image or other electronic data has been tampered with. The watermark could also be destination-based where each distributed copy gets a unique watermark identifying the particular buyer. The destination-based

.

IV.CONCLUSION AND FUTURE DIRECTIONS OF REASERCH

Digital watermarking technology is an emerging field in computer science, cryptology, signal processing and communications. The watermarking research is more exciting as it needs collective concepts from all the fields along with Human Psycho visual analysis, Multimedia and Computer Graphics. The watermark may be of visible or invisible type and each has got its own applications. We have developed two visible and two invisible algorithms as a part of the project work.

There are very few visible watermarking algorithms, so far [5] [6]. Out of the two visible watermarking algorithms proposed in this project, one is in spatial domain and the second is in DCT domain. To make the visible watermark visually pleasant, the mathematical models are developed taking the human visual system into consideration. The most significant application of visible watermarking is in Digital Libraries, where the owner wants to make the image available for research purpose but not for commercial use. The IBM Research Center people have used the visible watermarks for Vatican City Library Project.

There are few fragile invisible algorithms available in current literature even though it has got its own applications. We think some attention should be given to this area.

The robust invisible watermarking has been a topic of considerable interest due to their potential use for copyright protection. We have developed here two robust invisible watermarking algorithms. One of them is in spatial domain and the other one in DCT domain. Both of them are robust to various attacks and have the desired characteristics. As pointed out in [19] the ability to put robust watermarks does not necessarily solve the ownership problem. Still lots of work need are to be done in order to make the robust invisible watermark legally useful. All the algorithms we have proposed can be extended to video. Only the fourth one can be extended to audio. Further, research is needed to make it work if the insertion/extraction is to be performed in real time. For video watermarking one should also try to exploit the temporal redundancy to make real time algorithms.

.

V. REFERENCES

[1] Hal Berghel, "Watermarking Cyberspace", Comm. of the ACM, Nov.1997, Vol.40,No.11, pp.19-24.)

[2] M.M Yeung et al. "Digital Watermarking for High-Qulaity Imaging" , 1997 IEEE First Workshop on Multimedia Signal Processing, Jun 23-25, 1997, Princeton, New Jersey, pp 357-362I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[3] W. Zeng and B Liu, "On Resolving Rightful Ownership of Digital Images by Invisible Watermarks", Proc. IEEE 1997 Intl Conference on Image Processing, ICIP- 97, Vol. 1, pp 552-555.

[4] F. Mintzer, et.al., "Effective and Ineffective Digital Watermarks", IEEE 1997 Intl. Conference on Image Processing, ICIP-97, Vol. 3, pp 9-12.

[5]] J. Zhao, et. al., "In Business Today and Tommorrow", Comm of Acm, July 1998, Vol. 41, No. 7, pp 67-72.
F. C. Mintzer, et. al., "Towards Online Worldwide Access to Vatican Library Materials", IBM Journal of Research and Development, Vol. 40, No. 2, Mar 1996, pp 139-162.
http://www.software.ibm.com/is/diglib/vatican.html
http://www.ibm.com/IBM/ibmgives/diglib.html
http://www.research.ibm.com/image_apps

[6] B.Tao and B.Dickinson, "Adaptive Watermarking in DCT Domain", Proc IEEE 1997, International Conf on Accoustics, Speech and Signal Processing, ICASSP-97, Vol 4, pp 2985-2988

[7] Rajmohan, Watermarking of Digital Images, ME Thesis Report, Dept. Electrical Engineering, Indian Institute of Science,Banglore, India, 1998