AN ALGORITHM FOR DIGITAL WATERMARKING OF STILL IMAGES FOR COPYRIGHT PROTECTION

Jahnvi Sen

IBM Kolkata, India,
jahnvi_sen@yahoo.co.in

A.M. Sen

Computer Centre, Assam University,
Silchar, Assam, India
angshumaan_sen@yahoo.com

K. Hemachandran

Department of Computer Science, Assam University,
Silchar, Assam, India
Kh_chandran@rediffmail.com

Abstract

The rapid expansion of the Internet has rapidly increased the availability of digital data such as audio, images and videos to the public and file sharing has become very convenient. As such, the problem of protecting multimedia information, the issues of copyright has gained interest of researchers. Owners are concerned about protecting any illegal duplication of their data or work. Protection of intellectual property is very important because digital multimedia content can be copied and distributed quickly, easily, inexpensively, and with high quality and precision. Watermarking has been accepted as a complementary technology to multimedia encryption, providing some additional level of protection of intellectual property rights. Here we present, an overview of digital watermarking and the range of applications that could benefit from applying digital watermarking technology. We propose a simple algorithm for watermarking of an image where it is implemented through Matlab 7.4. The algorithm enables the basic requirements of watermarking and there is future scope to incorporate additional security and robust natures.

***Keywords*:** Watermarking; watermark; frequency domain; discrete cosine transform.

1. Introduction

Computers, printers and high rate transmission facilities are fast becoming less expensive and more generally available. The rapid expansion of the Internet in the past years has rapidly increased the availability of digital data such as audio, images and videos to the public. As today's technologies grow, image editing become much easier, and the invention of the internet provides a convenient environment for file sharing. Digital images are easily being copied, modified or edited. As we have witnessed, the problem of protecting multimedia information becomes more and more important and a lot of copyright owners are concerned about protecting any illegal duplication of their data or work. Some serious work needs to be done in order to maintain the availability of multimedia information but, in the meantime, the industry must come up with ways to protect intellectual property of creators, distributors or simple owners of such data. This is an interesting challenge and this is probably why so much attention has been drawn towards the development of digital images protection schemes. Of the many approaches possible to protect visual data, digital watermarking is probably the one that has received most interest. Digital watermarking describes the process of embedding additional information into a digital media, without compromising the media's value. Depending on the real world applications, this technique requires a number of properties such as perceptual quality, robustness, capacity and efficiency. There is a trade off between perceptual quality and robustness, Su et al(1999). Its basic idea is to create some kind of metadata containing some information about a digital content to be protected. The metadata is called watermark and a digital content to be protected is called a cover work. The watermark should be imperceptibly embedded

into the cover work, and it should be robust enough to survive not only most common signal distortions, but also distortions caused by malicious attacks. It is clear that digital watermarking and encryption technologies are complementing each other, and that a complete multimedia security solution depends on both.

2. Watermarking Types

In digital watermarking, watermarks can be classified as many types according to its properties. In terms of its visibility, digital watermark can be divided into both visible and invisible watermark. The invisible watermark falls into two categories: fragile watermark and robust watermark, Cox et al (2002). The fragile watermark is very easily modified.

There are some built-in applications in some of the digital cameras. Each application allows the user to embed a fragile watermark into the photos produced by the digital camera. If anyone changes the photos by modifying the pixel values, then this fragile watermark is broken. However, the robust watermark is used very often for copyright marks because it is not easily being attacked. For example, if we embed a robust watermark throughout a picture, the ownership of the picture can be secured by this copyright mark, Perter (2002) and Petitcolas et al (1999). Watermarks can also be divided into informed and blind watermarks by using different detection techniques. Informed watermark can only be detected by comparing watermarked image and the original image. Blind watermark does not depend on original image. Therefore, blind watermarking is a technique that the original image is not needed in watermark extraction process. Internet digital information protection is achieved through blind watermarking because with watermarked information, message can be detected successfully without original data.

3. Basic Watermarking Process

The general watermarking process involves four phases: message coding phase, embedding phase, transmission phase and detection phase. The first step is message coding. The copyright information is encoded into a digital signal. The copyright information is normally turned into binary sequence (zeros and ones). This binary sequence or signal should be suitable to be inserted into the original image. We call this signal, the watermark. The second step is embedding the watermark. This involves combining the original image and the watermark to produce a watermarked image. Then, the watermarked image is transferred to the receiver side. But during the transmission process, noise can be involved. In the transmission phase, noise means any signal interference during transmission and any intentional attacks such as cropping the image or making the brightness change to the image and so on. The original image which known as cover work is the digital information created by an owner or producer. After embedding the message into the original image, the outcome is known as watermarked image, Koch et al (1994) and Bender et al (1996). In this report, cover work and watermarked image are used. The watermark messages can be embedded in either spatial or frequency domain. In spatial domain, pixel values in original image are being modified with minimum perceptual disturbance, LST (Least Significant bit Technique) is one of the earliest techniques in this area. In frequency or transformed domain, image coefficients are used in these techniques such as DCT (Discrete cosine transformation) and wavelet.

In the detection phase, all the noise has to be overcome, so that the watermark can be correctly extracted and decoded from the received image, and compared with the copyright information we encoded in step one. If the copyright information and the detected message match, the watermark presents in this image. Figure 1.1 illustrates the general watermarking process.

Table 1. The planning and control components.

Application Class	Purpose of the embedded watermark	Application Scenarios
Protection of Intellectual Property Rights	Convey information about the content ownership and intellectual property rights	- Copyright Protection - Copy Protection - Fingerprinting - Signature
Content Verification	Ensures that the original digital document has not been altered, and/or helps determine the type of alteration	- Authentification - Integrity Checking
Information Hiding	Represents side channel used to carry additional information	- Broadcast Monitoring - System - Enhancement

4. Digital Watermarking -Applications

Very frequently there is a need to insert some additional information within a document in digital form, such as music, text file, video or image. For example, a copyright notice may need to be inserted in a software code in order to identify a legal owner of that software. Since the digital watermark is in an ideal case inseparable from the content, digital watermarking seems to be suitable method for associating additional information, Gonzalez and Woods (2008). There are numerous watermarking application scenarios. The table 1 gives a classification based on the nature of the information contained in the watermark.

5. Digital Watermarking- Requirements

There are a number of important characteristics that a watermark can exhibit, Jalil and Mirza (2010); Bandyopadhyay and Paul (2010) . These include that the watermark is difficult to notice, survives common distortion, resists malicious attacks, carry many bits of information, can coexist with other watermarks, and requires little computation to insert or detect, Vanwasi (2001); Shoemaker and Rudko (2002). The importance of these characteristics depends on the application. Das et al (2009) gives a new introduction towards invisible image watermarking based on clour image. Abdullah and Wahab (2008) present the key based text watermarking of e-text documents in and object based environment using z-axis for watermark embedding.

5.1. Fidelity (Imperceptibility)

The watermark should not be noticeable to the viewer nor should the watermark degrade the quality of the content. The term “imperceptible” is widely used in this case. However, if a signal is truly imperceptible, then perceptually based lossy compression algorithms either introduce further modifications that jointly exceed the visibility threshold or remove such a signal, Gonzalez and Woods (2008). It is then important to develop techniques that can be used to add imperceptible or unnoticeable watermark signals in perceptually significant regions to counter the effects of signal processing.

5.2. Robustness

In general a digital watermark must be robust to transformations that include common signal distortions as well

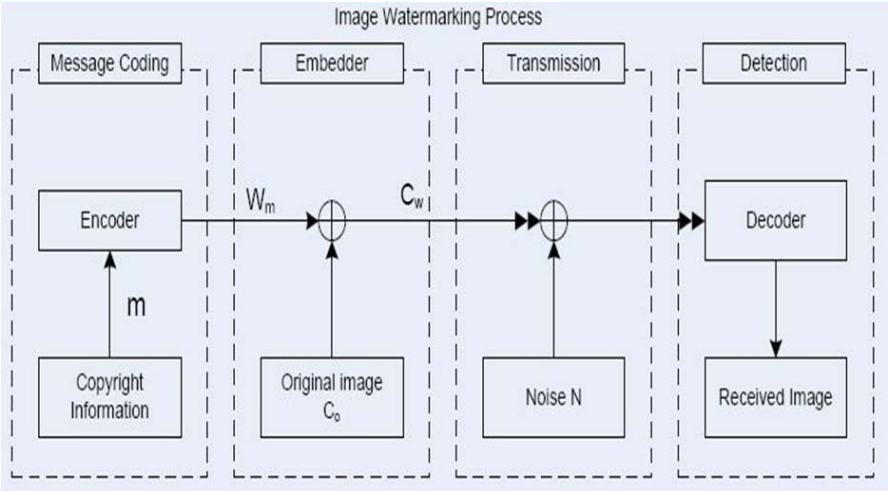

Fig. 1.1 General Watermarking Processs

as Digital - Analog/Analog - Digital conversion and lossy compression, unless the media is altered to the point of no value. There are two major problems when trying to guaranty robustness; the watermark must be still present in the media after the transformation or it must be still possible for the watermark detector to detect it.
When a signal is distorted, its fidelity is only preserved if its perceptually significant regions remain intact, while perceptually insignificant regions might be drastically changed with little effect on fidelity. Based on this argumentation, Cox et al (1996, 2002) support the fact that the inserting watermark signal in perceptually significant region of the media is the best way to achieve robustness.

5.3. Fragility

Some application fields require exactly the opposite of robustness. We consider for example, the use of paper watermarks in bank notes. The point of these watermarks is that they do not survive any kind of copying, and therefore can be use to indicate the bill's authenticity. In some application, the watermark is required to survive certain transformations and be destroyed by others and that makes the design of fragile watermarking difficult.

5.4. Modification and Multiple Watermarks

Changing a watermark can be accomplished by either removing the first watermark or then adding a new one, or Inserting a second watermark. The first alternative goes against the principle of tamper resistance, because it implies that a watermark is easily removable. Allowing multiple watermarks to coexist is the preferred solution. There is however security problem related to the use of multiple watermarks. The basis of watermarking security should lie on Kerckhoff's assumption that one should assume that the method used to encrypt the data is known to the unauthorized party . It means that watermarking security can be interpreted as encryption security leading directly to the principle that it must lie mainly in the choice of the embedded key. Allows insertion of multiple, independently detectable watermarks in an Image.

6. Attacks on Watermarks

There are several kinds of malicious attacks, which result in a partial or even total destruction of the embed identification key and for which more advanced watermarking scheme should be employed, Petitcolas et al (1998) and Fraunhofer (2006):

6.1. Active Attacks

Here, the hacker tries deliberately to remove the watermark or simply make it undetectable. This is a big issue in copyright protection, fingerprinting or copy control for example.

6.2. Passive Attacks

In this case, the attacker is not trying to remove the watermark but simply attempting to determine if a given mark is present or not. Cox et al (2002) suggest that, protection against passive attacks is of the utmost importance in covert communications where the simple knowledge of the presence of watermark is often more than one want to grant.

6.3. Collusion Attacks

In collusive attacks, the goal of the hacker is the same as for the active attacks but the method is slightly different. In order to remove the watermark, the hacker uses several copies of the same data, containing each different watermark, to construct a new copy without any watermark. This is a problem in fingerprinting applications *(e.g.* In the film industry) but is not the widely spread because the attacker must have access to multiple copies of the same data and that the number needed can be pretty important.

6.4. Forgery Attacks

This is probably the main concern in data authentication. In forgery attack the hacker aims at embedding a new, valid watermark rather than removing one. By doing so, it allows him to modify the protected data as he wants and then, re-implants a new given key to replace the destructed (fragile) one, thus making the corrupted image seems genuine.

7. Different Techniques

The different watermarking techniques can be broadly classified into the following three categories, Cox et al(1996); Petitcolas et al (1998); Hartung et al(1999):-

7.1. Watermarking in Spatial Domain

In spatial domain the values of the image pixels are directly modified as shown in figure 1.2, based on the watermark that has to be embedded. Such methods are simple and computational efficient, however most of them are not robust against image modifications.

7.2. Watermarking in Frequency Domain

The transform coefficients are affected. In transform domain technique, the host image is first converted into frequency domain by transformation method such as the discrete cosine transform (DCT), discrete Fourier transform (DFT) or discreet wavelet transform (DWT) ,etc. then, transform domain coefficients are modified by the watermark, Cox et al(2002); Yang and Kot (2004); Gonzalez and Woods (2009). The inverse transform is finally applied in order to obtain the watermarked image. The watermark is embedded into the DCT coefficients of subimages, which are obtained by subsampling the original image. Due to the complicated calculations of forward and inverse transform, these methods generally are more complex and involved higher computational costs than spatial domain methods; however, transformation domain methods are more robust against attacks than spatial domain methods.

8. Proposed Watermarking Method

In our work, ideas of spread spectrum is used to additively embed and extract a pseudo-random noise pattern. The process is described as follows:

- The image is read from source and stored in an array.
- The image is divided into smaller blocks.
- Block image transformation (Discrete Cosine Transform) is performed.
- **Choosing the Watermark**:-It is a Gaussian sequence of pseudo-random real numbers, length 4096.
- **Coefficient Selection**:-The DCT coefficients of 1st element of each 8x8 blocks of host image are chosen.
- **Embedding**:- $f'(m , n)= f(m , n)(1+\alpha * Wi)$ [as shown in figure 1.3]
- **Extraction**:- $Wi'=[f'(m ,n)-f(m ,n)]/[\alpha *f(m ,n)]$ [as shown in figure 1.4]

  α= embedding strength Wi/Wi′=Pseudo-random bits

  f(m ,n)= host image

  f′(m , n)= embedded image
- The embedding strength α is chosen such that it gives robustness to the watermarked data and also does not degrade the signal(data) quality.
- The edges of the8x8 blocks of host image was taken and the sum of each of these edges block(T′) found.
- A threshold(T) is set and if $(T' \rangle T)$, a higher value of α is chosen thus making the watermarked data more robust and also maintaining the perceptual quality of the signal.

In this experimental set, we have taken the snap of the very famous LENA image as the host image. The image is in jpeg extension. The watermark image is the Gaussian noise. From the watermarked image, the watermark is retrieved also as shown in the figure 1.5.

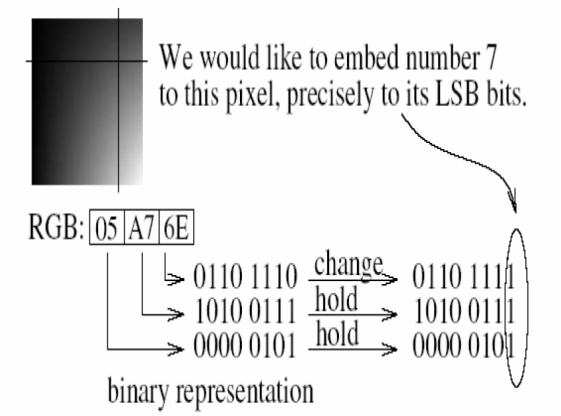

Fig. 1.2 Least Significant Bit (L.S.B) Techniques of Watermarking

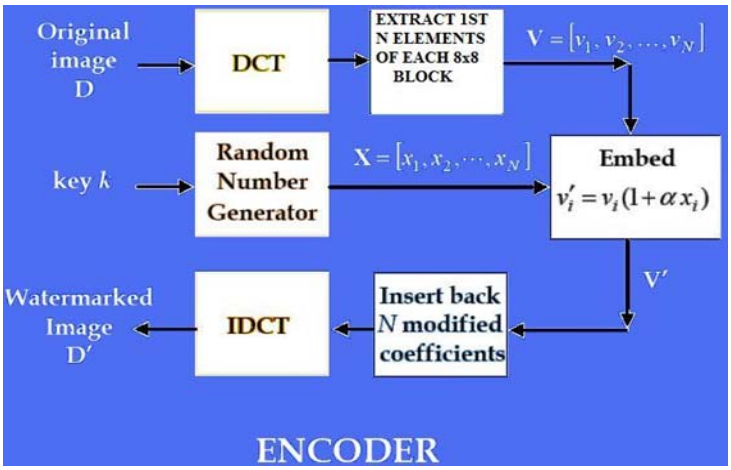

Fig. 1.3 Block Diagram for embedding the watermark in an image

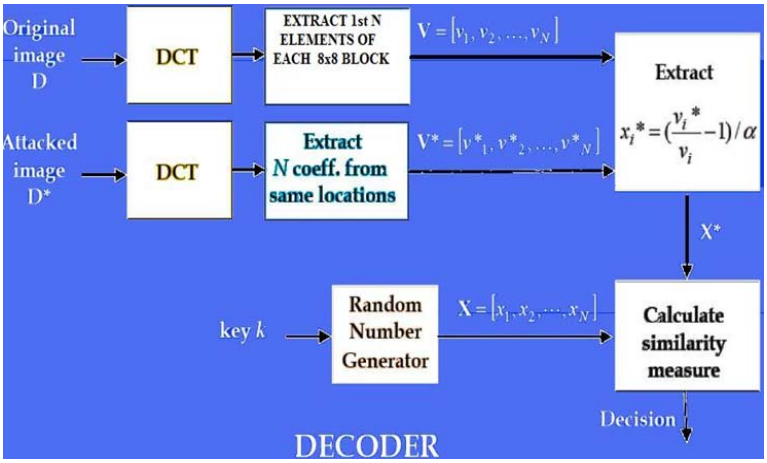

Fig. 1.4 Block Diagram for extracting the watermark

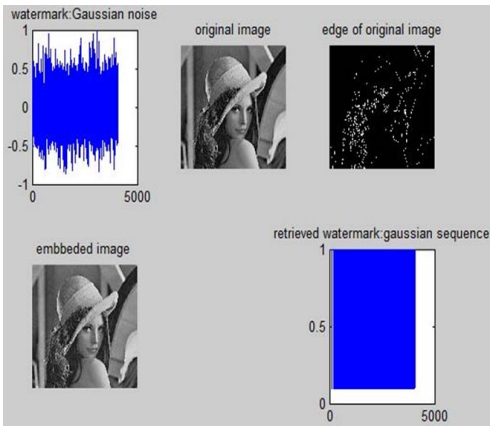

Fig. 1.5 Watermarking in frequency Domain

8. Conclusion

Image Watermarking has become an important data authentication technique nowadays for image products. The proposed scheme can be used to watermark digital images without distorting the vital regions that are of interest to the customer. Hence, the value of the image is preserved. At the same time, the ownership of the digital

image can be proven whenever required on the production of the key by the legal owner, thereby, keeping a check on illegal copying of the copyrighted image. we have surveyed some watermarking algorithms in both spatial and frequency domains and we have implemented a new algorithm using MATLAB 7.4. In frequency domain, the technique could be improved by embedding coefficients in different areas within the image and further more testing with varied embedding strength. The robustness property could be also improved by using different attacks to the image. In theory, cropping and rotating the image or changing the image format such as from jpeg to tiff file could be the possible attack to the watermarked image. If the technique developed survives such attack, the algorithm would be more robust.
If an intelligent and secure watermarking application software system can be build and be implemented in a high performance DSP processor, it has a huge potential market commercially.

References

[1] Abdullah, M. and Wahab, F. (2008). Key Based Text Watermarking of e-Text Documents in an Object Based Environment Using Z-Axis for Watermark Embedding. World Academy of Science.
[2] Bandopadyay, S.K.; Paul T.U. (2010). An Encryption based technique for Invisible Digital Watermarking.
[3] Bender, W.; Gruhl, D.; Morimoto N.; and Lu, A. (1996). Techniques for data hiding. IBM Systems Journal. 35(¾): 313–336.
[4] Cox, I. J.; Kilian, J.; Leighton, F. T. and Shamoon, T. (1996). A secure, robust watermark for multimedia in Information Hiding: First Int. Workshop Proc. (R. Anderson, ed.), Lecture Notes in Computer Science, Springer-Verlag.1174 : 185–206.
[5] Cox, I. J.; Miller M.; Bloom J.A. (2002). Digital Watermarking 1st Edition, Morgan Kaufmann Publisher, USA.20.
[6] Das, S.; Bandyopadhyay, P; Paul, S. Ray, A.S.; Banerjee, M. (2009). A New Introduction towards Invisible Image Watermarking on Colour Image. IEEE:1224-1229.
[7] Fraunhofer SIT.(2006) Watermarking Portal: http://watermarkingportal.ipsi.fraunhofer.de/, 2006.
[8] Gonzalez, R. C.; Woods, R. E. (2008). Digital Image processing, 3rd edition.
[9] Gonzalez, R. C.; Woods, R. E.; Eddins, S. L. (2009). Digital Image processing using Matlab, 2nd edition.
[10] Hartung, F.; Kutter, M. (1999). Multimedia Watermarking Techniques. Proceedings of the IEEE. 87(7) : 1085 – 1103.
[11] Jalil, Z. and Mirza, A.M.(2010) An Invisible Text Watermarking Algorithm Using Image Watermark, Springer , Netherlands.
[12] Koch, E.; Rindfrey, J. and Zhao, J. (1994). Copyright protection for multimedia data, in Proc. Of the Int. Conf. on Digital Media and Electronic Publishing.
[13] Perter, W. (2002). Disappearing Cryptography: Information Hiding – Steganography and Watermarking, MklMorgan Kaufmann Publishers, Boston.
[14] Petitcolas, F. A. P.; Anderson, R. J. and Kuhn, M. G. (1998). Attacks on copyright marking systems. In *Second workshop on information hiding*. : 218-238.
[15] Petitcolas, F. A. P.; Anderson, R. J. and Kuhn, M. G. (1999). Information hiding-a survey. *Proceedings of the IEEE*, Special Issue Identification and protection of multimedia information.
[16] Shoemaker, C. and Rudko (2002) Hidden Bits: A Survey of Techniques for Digital Watermarking. Independent Study, EER-290 and Spring 2002 www.web.vu.union.edu/~shoemakc/watermarking/watermarking.html. visited Dec.2011
[17] Su, J. K.; Hartung, F.; Girod, B. (1999). Digital Watermarking of Text Image and Video Document. Telecommunications Laboratory; University of Erlangen-Nuremberg, Germany. Elsevier.
[18] Vanwasi, A.K.(2008) Digital watermarking-Steering the Future of Security. The India Edition of Network Magazine- Solutions for the Competitive Edge, Indian Express Group, Mumbai, India, Copyright 2001. www.networkmagazineindia.com/200108/Security1.htm, visited Dec.2011.
[19] Yang, H. and Kot, A. C. (2004). Text Document Authentication by Integrating Inter Character and Word Spaces Watermarking. IEEE Inter-National Conference on Multimedia and Expo. : 26-30.