

Recent Advances and Classification of Watermarking Techniques in Digital Images

Chunlin Song, Sud Sudirman, Madjid Merabti
School of Computing and Mathematical Sciences
Liverpool John Moores University, UK
c.l.song@2004.ljmu.ac.uk, {s.sudirman, m.merabti}@ljmu.ac.uk

Abstract — This paper surveys recent advances in watermarking techniques in digital images. The aim of digital watermarking is to include subliminal information in multimedia information to ensure a security service or simply a labelling application. It would be then possible to recover the embedded message at any time, even if the information was altered by one or more non-destructive attacks, whether malicious or not. Its commercial applications range from copyright protection to digital right management. This paper then classifies the different watermarking techniques into several categories depending upon the domain in which the hidden data is inserted; the size of the hidden data and the requirement of which the hidden data is to be extracted. An experiment is conducted to further tests the robustness of some of these techniques. At the end, this paper analyses challenges that have not been met in current watermarking techniques

Keywords — Watermarking, Advance Techniques, Challenges, Experiment.

I.INTRODUCTION

Digital watermarking technology is now drawing the attention as a new method of protecting copyrights for digital images. It is realized by embedding data that is insensible for the human visual system. The embedded information data is called watermark. So watermarking in digital images is the process by which a discrete data stream is hidden within an image imposing imperceptible changes of the image. The root of watermarking as an information hiding technique can be traced in ancient Greece as Steganography [2], the science of watermarking is a modern subject was organized developed in recent years. The first Information Hiding Workshop (IHW), which included digital watermarking as one of its primary topic, was held in 1996. The SPIE began devoting a conference specifically to Security and Watermarking of Multimedia Contents, beginning in 1999. Subsequently, up until now, there are more than one hundred institutes around the world [1] which deal with the issue. The application of watermarking ranges from copyright protection, file tracking and monitoring.

It was proposed in [16] one of a main classification structures of watermarking techniques. This is shown in Figure 1. From this classification, there are two types of watermarks, the visible ones, like different logos either on paper or on a TV screen and the most important one, the invisible or transparent watermarks, which cannot be

perceived by the human sensory system. An invisible watermark can be either robust or fragile. The use of a fragile watermark is important when one wants to verify if the protected media was tampered with or not. The type of watermark is especially designed to be as fragile as possible, so even the slightest modification of the marked media will destroy it, indicating that someone tampered with the media in question. This type of watermark is like a CRC (cyclic redundancy code). On the other hand, robust watermarking is designed to provide proof of ownership of the media in question. Recently, it is used as one of the means of Digital Right Management. This paper concerns with the survey of this category of digital image watermarking and henceforth will be referred to as watermarking only for brevity.

A watermarking system conceals information inside some other data. There are three criteria that can be used to measure the performance of a watermarking system. They are Embedding Effectiveness, Fidelity and Data payload, different application has different preferences based on its nature and requirements [2]

We define embedding effectiveness of a watermarked work as a work that when input to a detector results in a positive detection. With this definition of watermarked works, the effectiveness of a watermarking system is the probability that the output of the sender will be watermarked. In other words, the effectiveness is the probability of detection immediately after embedding. This definition implies that a watermarking system might have an effectiveness of less than 100%.

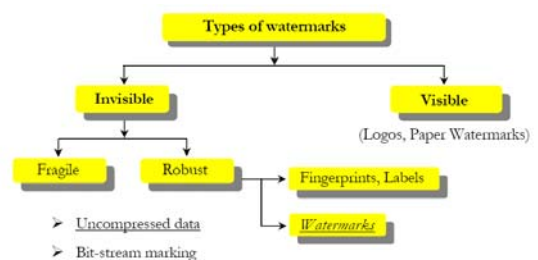


Fig. 1. A classification of watermarking techniques based on [16].

In general, the fidelity of a watermarking system refers to the perceptual similarity between the original and watermarked versions of the cover work. However, when the watermarked work will be degraded in the transmission of

fidelity may be more appropriate. We define the fidelity of a watermarking system as the perceptual similarity between the un-watermarked and watermarked works at the point at which they are presented to a consumer.

Data payload ratio is the ratio between the size of watermark and the size of its carrier. Different watermark algorithms are designed with a specific type of data to hide in mind. This in turns affects the payload ratio of that algorithm. Those such as in [2] attempt to hide watermark inside another image, while for example Digimarc, only hides a small amount of text information.

The general process involved in watermarking is illustrated in Figure 2. The process can be divided into 3 parts, Embedding, Transmission and Extraction.

In the embedding process, the watermark may be encoded into the cover data using a specific key. This key is used to encrypt the watermark as an additional protection level. The output of the embedding process, the watermarked image, is then transmitted to the recipient. During this transmission process, the watermarked image may be subjected to attacks either deliberately or due to transmission error or noise. Therefore, there is no guarantee that the watermarked image received by the recipient is exactly the same data as that sent by the transmitter. This data nonetheless need to be decoded to extract the watermarked image. In the model shown in Figure 2, the original cover data is needed in the extraction process. This process is therefore called a blind technique. In a non-blind technique, the original cover data is unknown to the recipient hence the decoding process will have just rely on the watermark

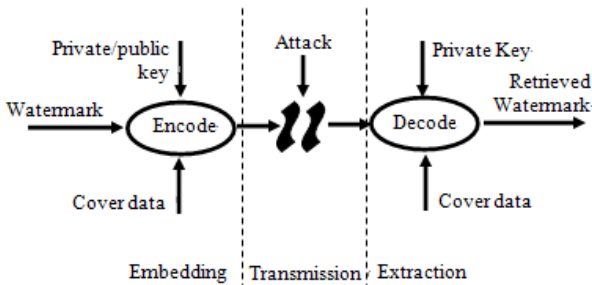


Fig. 2. General processes involved in a watermarking system. The watermark is encoded into the cover data in the embedding phase. An optional encryption mechanism may also be used to add another layer of security. In the transmission phase, the watermarked image can be subject to attack from third party. This in turns provides some challenges to the decoder to retrieve as accurate as possible the hidden data from the received watermarked image.

II. RECENT ADVANCES IN WATERMARKING TECHNIQUES IN DIGITAL IMAGES

There have been many proposed novel techniques to hide watermark in digital images. These techniques can be classified into different categories according to several criteria [2]. The first criterion is the type of domain in which the data embedding takes place. There are two major

domain types, spatial and transform domains. The second criterion is according to the ability of watermark to resist attack; fragile watermarks are ready to be destroyed by random image processing methods, the change in watermark is easy to be detected, thus can provide information for image completeness, robust watermarks are robust under most image processing methods can be extracted from heavily attacked watermarked image. The third criterion used to categorize watermark techniques is the type of information needed in the extraction process. Using this criterion, techniques can be classified into 2 categories; they are blind and non-blind categories. A blind watermark system requires the cover image to recover the watermarked image. On the other hand, a non-blind system requires nothing other than the watermarked image itself.

A. Spatial Domain

An analogue image can be described as a continuous function over a two-dimensional surface. The value of this function at a specific coordinate on the lattice specifies the luminance or brightness of the image at that location. A digital image version of this analogue image contains sampled values of the function at discrete locations or pixels. These values are said to be the representation of the image in the spatial domain or often referred to as the pixel domain.

Spatial embedding inserts message into image pixels. The oldest and the most common used method in this category is the insertion of the watermark into the least significant bits (LSB) of pixel data [2][5][6]. The embedding process of the LSB technique can be illustrated as follows:

Consider that the system is required to hide a watermark number 178 in a 2x2 gray-scale (8-bit) image. Let's assume that the image pixels are 234, 222, 190 and 34. In an 8-bit binary format the number 178 is represented as 10110010. Since there are 4 pixels that can be used to store this data we can easily decide to embed pairs of bits of the watermark to the last 2 insignificant bits of the pixels. The process therefore modifies the original bits from 11101010, 11011110, 10111110 and 00100010 to 11101010, 11011111, 10111100 and 00100010 respectively.

In decimal representation the watermarked image has pixel values of 234, 223, 188 and 34.

Since the modification of pixel values occurs in the LSB of the data, the effect to the cover image is often visually indifferent. This effect however becomes more apparent as more bits are used to hide the watermark.

One of the major limitations in spatial domain is the capacity of an image to hold the watermark. In the case of LSB technique, this capacity can be increased by using more bits for the watermark embedding at a cost of higher detection rate. On the other hand capacity can also be improved by means of lossy embedding the watermark. In the latter approach, the watermark is quantized before the embedding process. Improving this limitation seems to be one of the major drives in spatial domain research.

The problem of improving payload is also addressed by El-Emam [17]. In his paper, he proposed a technique that is

claimed to be able to hide images which size is as large as 75% of the cover image. This is achieved partly due to the application of a compression algorithm to compress the watermark prior to embedding it. The embedding process involves segmentation and filtering of the cover image to reduce the number of color. It then uses what it terms Main Case and Sub Case concept to select the best pixels to embed the compressed watermark.

B. Transform Domain

Transform domain embeds a message by modifying the transform coefficients of the cover message as opposed to the pixel values. Ideally, transform domain has the effect in the spatial domain of apportioning the hidden information through different order bits in a manner that is robust. There are a number of transforms that can be applied to digital images, but there are notably three most commonly used in image watermarking. They are Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT).

Discrete Fourier Transform

Fourier Transform (FT) is an operation that transforms a continuous function into its frequency components. The equivalent transform for discrete valued function requires the Discrete Fourier Transform (DFT). In digital image processing, the even functions that are not periodic can be expressed as the integral of sine and/or cosine multiplied by a weighing function. This weighing function makes up the coefficients of the Fourier Transform of the signal. Fourier Transform allows analysis and processing of the signal in its frequency domain by means of analyzing and modifying these coefficients.

In their paper, Ganic proposed a watermark algorithm based on DFT [7]. This paper describes a new circular watermark scheme that embeds one watermark in lower frequencies and another in higher frequencies components of the cover image. The circularly symmetric watermark is embedded in DFT domain by considering the magnitude of DFT coefficient of the cover image, the scaling factor and the circular watermark. The paper presented extensive experimental results to show the performance of the proposed technique given a number of attacks and shows that by embedding the watermark in both frequency groups can increase the robustness of the watermarking system.

Pereira et. al. proposed a method for copyright protection by embedding a digital watermark in the DFT domain [9]. The properties of this technique based on polar maps for the accurate and efficient recovery of the template in an image which has undergone a general affine transform. In this technique, the watermark is composed of 2 parts: one is a template which contains no information in itself but can detect any transformations undergone by the image, and another one is a spread spectrum message that contains the hidden information. The length of the hidden information is supposed to be short and it is subjected to a preprocessing

algorithm to produce the new message of length. Prior to embedding the hidden message, the luminance component of the cover image is extracted and is used to calculate the DFT coefficients. The hidden data and the template are then embedded in these coefficients. The template is embedded along 2 lines in the cover image which go through the origin and its purpose is to detect any attacks (transformation) the image has undergone.

Discrete Cosine Transform

Discrete Cosine Transform is related to DFT in a sense that it transforms a time domain signal into its frequency components. The DCT however only uses the real parts of the DFT coefficients. In terms of property, the DCT has a strong "energy compaction" property [14] and most of the signal information tends to be concentrated in a few low-frequency components of the DCT. The JPEG compression technique utilizes this property to separate and remove insignificant high frequency components in images.

Srayazdi [19] proposed a blind gray-level watermarking scheme by dividing the cover image into 4x4 non-overlapping blocks. The technique first estimates the first five DCT coefficients of each block in a zigzag order. It then embeds a gray-level value of the watermark data by replacing each low frequency DCT value in the central block with its estimated modified values. In [20], the author created a new robust hybrid non-blind watermarking scheme based on discrete cosine transform (DCT) and Singular Value Decomposition (SVD). In this method, after applying the DCT in the cover image, the DCT coefficients are mapped in zigzag order into 4 quadrants, which represent frequency bands from the lowest to the highest. SVD is then applied to each quadrant. The same process is also applied to the watermark. The technique then modifies the singular values in each quadrant to obtain a set of modified DCT coefficients. The decoding process involves mapping the modified DCT coefficient back to their original positions and applying the inverse equation to produce watermarked cover image.

In [10], a watermarking algorithm based on low luminance smooth blocks in compressed DCT domain is proposed. The watermark is embedded by setting the sign of a subset of low-frequency DCT coefficients in these smooth blocks. In this algorithm, DCT is applied to a set of 8x8 pixel blocks. The DCT takes such a signal as its input and decomposes into 64 orthogonal basis signals. The quantized DC and the AC coefficients denote the average luminance and the different frequency bank of a block which could reflect its texture respectively. Firstly, the appropriate low luminance smooth blocks should be selected based on DC and AC coefficient. Then the coefficients are quantized in zigzag order. These DCT coefficients are then modified according to some robustness measure and the watermarking information. The process is repeated until a desired number of smooth blocks are embedded with watermarks.

Discrete Wavelet Transform

Wavelet Transform is a modern technique frequently used in digital image processing, compression, watermarking etc. The transforms are based on small waves, called wavelet, of varying frequency and limited duration. A wavelet series is a representation of a square-integrable function by a certain orthonormal series generated by a wavelet. Furthermore, the properties of wavelet could decompose original signal into wavelet transform coefficients which contains the position information. The original signal can be completely reconstructed by performing Inverse Wavelet Transformation on these coefficients.

Watermarking in the wavelet transform domain is generally a problem of embedding watermark in the subbands of the cover image. There are four subbands created at the end of each level of image wavelet transformation: they are Low-Low pass subband (LL), High-Low (horizontal) subband (HL), Low-High (vertical) subband (LH) and High-High (diagonal) pass subband (HH). Subsequent level of wavelet transformation is applied to the LL subband of the previous one. Figure 3 illustrates the subband decomposition of an image using 2D wavelet transform after 2 levels of decomposition. [11]

In 2007, another novel technique was invented for robust wavelet-based watermarking [12]. The main idea of this paper embeds the signature data to the selected group of wavelet transform coefficients, varying the watermark strength according to the subband level and the group where the corresponding coefficients reside. Initially, the input image decompose into 4 levels by DWT, so we get approximation subbands with low frequency component and 12 detail subbands with high frequency component. Next, the author detect edge in each component by using Sobel edge detector, so it is forming 2 groups of coefficients, at the meanwhile, morphological dilation capture the coefficients that near the edge for forming another group. In the end, the watermark energy distribute among these groups with a variable strength.

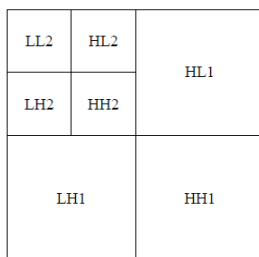


Fig. 3. Subbands created after two levels of Discrete Wavelet Transformation of an image.

A novel blind image watermark scheme is developed based on discrete wavelet transform in 2007 [13]. In this paper, the author point is to make the watermark robust and transparent; the watermark is embedded in the average of

wavelet blocks that is smaller change than individual coefficient to make watermark more robust and concealed by using the visual model based on the human visual system. The process first defines the average of wavelet block by the length and width of wavelet block and n LSB of wavelet coefficient, and then determine adjusting average by the n LSBs of i^{th} wavelet coefficient in the k^{th} wavelet block, so that the watermark consisting of a binary pseudo random sequence is embedded by adjusting the average of wavelet blocks by suitable formula.

III. EXPERIMENT

An experiment is conducted to preliminary test the performance of the different watermarking techniques when deliberate attacks were done as an attempt to remove the watermark. The three watermarking techniques used are Least Significant Bit, DCT [14] and DWT [11]. The techniques were applied to embed the Hat image into the Lena image as shown in Figure 4. The results of these watermarking processes were then subjected to four attack mechanisms with the purpose of completely destroying the watermarking signal inside the watermarked image. The four attacks mechanisms with the purpose of completely destroying the watermark signal inside the watermarked image. The four attacks are sharpen, blur, histogram equalization and Gaussian noise with different alpha values.


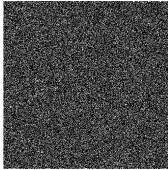


As the performance measure we calculate the difference between the watermark signals in both the original watermarked image and the attacked watermarked image. The difference value is further converted to Peak-to-Signal Ratio (PSNR) to give a more representative picture of distortion severity relative to signal strength. The PSNR is calculated by $PSNR = 20\log_{10}(255/RMSE)$, where RMSE is the square root of Mean Squared Error between the original and attacked watermark signal.

Figure 5 shows the extracted watermark signal from the three different algorithms after the watermarked image is subjected to the four attacks mechanism





From figure 5, all watermarked image extracted completely after attack, most of watermark is recovered, but the LSB watermark after the blur attack is totally distorted. Compare with PSNR in different specific algorithm, LSB contains lowest PSNR, both DCT and DWT has their strong point. In other words, the robustness of DCT and DWT in frequency domain are far better than LSB in spatial domain, both DCT and DWT have their advantages each.







Fig. 4 Cover Image and Watermark

<p>Sharpen(0.5)</p>  <p>PSNR: 3.4031</p>	<p>Blur(0.005)</p>  <p>PSNR: 3.8796</p>
<p>Histogram(10)</p>  <p>PSNR: 3.2901</p>	<p>Noise(0.005)</p>  <p>PSNR: 3.0084</p>

a. extracted distort watermarked image of LSB

<p>Sharpen(0.5)</p>  <p>PSNR: 15.8705</p>	<p>Blur(0.005)</p>  <p>PSNR: 11.8911</p>
<p>Histogram(10)</p>  <p>PSNR: 3.3751</p>	<p>Noise(0.005)</p>  <p>PSNR: 9.0479</p>

b. extracted distort watermarked image of DCT

<p>Sharpen(0.5)</p>  <p>PSNR: 17.6742</p>	<p>Blur(0.005)</p>  <p>PSNR: 5.4608</p>
<p>Histogram(10)</p>  <p>PSNR: 11.2473</p>	<p>Noise(0.005)</p>  <p>PSNR: 7.5685</p>

c. extracted distort watermarked image of DWT

Fig.5 Extracted distort watermarked image and PSNR

One major reason why frequency domain is more robust than spatial domain because of watermark embeds into the band of the transformed host image. Watermarking in high frequency band tends to be less robust but has a lesser effect

on the quality of original image, while watermarking in low band will achieve a better robustness but at the expense of significant alteration to the original image, a mid-band scheme is used since it can provide a good trade-off between the imperceptibility and robustness

IV. CHALLENGES IN WATERMARKING

There are four criteria that can be used to measure the performance of an information hiding system. They are invisibility, robustness or security, payload ratio and computational cost. From the observation of the current watermarking systems, it can be seen that some of these criteria are less satisfied than others.

The first criterion is invisibility. A watermarking system is of no use if it distorts the cover image to the point of being useless, or even highly distracting. Ideally the watermarked image should look indistinguishable from the original even on the highest quality equipment.

The second criterion which is often overlooked when assessing system performance is robustness. Robust watermarking systems are expected to withstand different kind of attacks. Image compression, introduction of noise, low pass filtering, and image rescaling, cropping, rotation are some but a few of types of attacks that often are not addressed in most literatures. Both pixel domain and transform domain watermarking techniques share the same level of exposure to these attacks. There are a few tools that can be used to measure a system robustness level, e.g., Stirmark.

Many of the proposed watermarking techniques aim at hiding data with large size. These techniques manage to hide image as large as, or even larger than, the cover image. Although this is impressive in its own right, very little discussion and analysis is given to what extent this feature can be used to bring together watermarking with image compression techniques. Digital images are often transmitted over the internet in compressed format. Being able to seamlessly incorporate watermarking algorithm into image compression system would be a challenge for researchers.

The fourth criterion that is often overlooked is the computational cost of the encoding and decoding processes. The computational cost determines how fast the technique can be executed and how many resources required to do so. Although this criterion is probably considered the least important by research community, it is nonetheless a significant factor to consider when the technique is deployed as a commercial product.

Figure 6 shows tradeoffs between robustness, invisibility and capacity, a good watermarking system should balance these three variables.

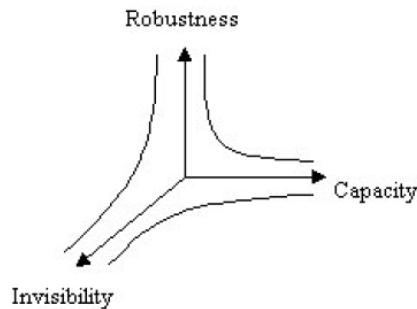


Fig. 6. Tradeoffs between robustness, invisibility and capacity [18]

V. CONCLUSION

In this paper we have presented description and analysis of recent advances in watermarking in digital images. These techniques are classified into several categories depending upon the domain in which the hidden data is inserted, the size of the hidden data and the requirement of which the hidden data is to be extracted.

The experiment shows the different effective algorithms of watermark. The result indicates frequency domain is more robustness than spatial domain.

Several challenges that are often un-addressed in the literature have also been identified. Meeting these challenges is essential in advancing the current state of the art of watermarking in digital images.

REFERENCES

- [1]. Petitcolas, F. A. P., Anderson, R. J.: Kuhn, M. G., Information Hiding – A Survey, *Proceedings of the IEEE, Special Issue on Protection of Multimedia Content*, 1062-1078, July 1999.
- [2]. Cox, I., Miller, M., Bloom, J., Fridrich, J., Kalker, T.: Digital Watermarking and Steganography, 2nd Ed. ISBN: 978-0123725851
- [3]. Pfizmann, B.: Information Hiding Terminology, *Information Hiding, First International Workshop*, 1174, 1996
- [4]. Marvel, L. M., Hartwig, G. W., Boncelet, C.: Compression-Compatible Fragile and Semi-Fragile Tamper Detection, *Proc. SPIE*, vol. 3971, 131–139
- [5]. Wang, R. Z., Lin, C. F., Lin, J. C.: Image hiding by optimal LSB substitution and genetic algorithm, *Pattern Recognition*, vol. 34, 671-683, 2003.
- [6]. Swanson, M. D., Kobayashi, M., Tewfik, A. H.: Multimedia Data-Embedding and watermarking Technologies, *Proc. IEEE*, vol. 86, 1064 – 1087, 1998
- [7]. Ganic, E., Eskicioglu, A. M.: A DFT-Based Semi-Blind Multiple Watermarking Scheme For Images
- [8]. Youail, R. S., Khadhim, A-K. A-R., Samawi, V. W.: Improved Stegosystem Using DFT with Combined Error Correction and Spread Spectrum, *Industrial Electronics and Applications, 2007. ICIEA 2007. 2nd IEEE Conference*, 1832-1836, 2007
- [9]. Pereira, S., Pun, T.: Robust Template Matching for Affine Resistant Image Watermarks, *IEEE Transactions on Image Processing*, vol.9, 1123-1129, 2000.
- [10]. Zhou, H.T., Qi, C., Gao, X. C.: Low Luminance Smooth Blocks Based Watermarking Scheme in DCT Domain, *Communications, Circuits and Systems Proceedings, 2006 International Conference*, vol. 1, 19-23, 2006
- [11]. Tao, P. N., Eskicioglu, A. M.: A robust multiple watermarking scheme in the Discrete Wavelet Transform domain, *Internet Multimedia Management System Conference*, vol. 5601, 133-144, 2004#
- [12]. Ellinas, J. N.: A Robust Wavelet-based Watermarking Algorithm Using Edge Detection, *Proceedings of World Academy of Science, Engineering and Technology*, vol. 25, 438-443, 2007
- [13]. Jin, C., Pan, L-G., Su, T.: Image Watermark using Visual Model Based Discrete Wavelet Transform, *IJCSES International Journal of Computer Sciences and Engineering System*, vol.1, 119-124, April 2007
- [14]. K. R. Rao and P. Yip.: *Discrete Cosine Transform: Algorithms, Advantages, Applications* (Academic Press, Boston, 1990).
- [15]. Chang, C.C., Hsial, J.Y., Chiang, C.L: An Image Copyright Protection Scheme Based on Torus Automorphism. *First International Symposium*, 2002
- [16]. Serdean C.V: Spread Spectrum-Based Video Watermarking Algorithms for Copyright Protection. PhD thesis, university of Plymouth, 2002
- [17]. Nameer, N. E.: Hiding a Large Amount of Data with High Security Using Steganography Algorithm, *Journal of Computer Science*, 223-232, 2007
- [18]. Zain, J. Clarke, M: Security in Telemedicine: Issues in Watermarking Medical Images, *SETIT 2005, 3rd International Conference: Science of Electronic, Technologies of Information and Telecommunications*, 2005
- [19]. Saryazdi, S., Demehri, M.: A Blind DCT Domain Digital Watermarking, 3rd International Conference: Sciences of Electronic, Technologies of Information and Telecommunications, 2005
- [20]. Sverdllov, A., Dexter, S., Eskicioglu, A. M.: Robust DCT-SVD Domain Image Watermarking for Copyright Protection: Embedding Data in all Frequencies, International Multimedia Conference, Proceedings of the 2004 workshop on Multimedia and security, 166-174, 2004