11-7-2007

2D barcodes as watermarks in image authentication

Prashan Premaratne
University of Wollongong, prashan@uow.edu.au

Farzad Safaei
University of Wollongong, farzad@uow.edu.au

2D barcodes as watermarks in image authentication

Abstract

2D barcodes are increasingly used as tags in every type of goods for unique identification. Compared with the 1D barcodes, 2D barcodes not only can carry more data but also can withstand errors in subsequent scans. This property has significant parallels to watermarking logos as such watermarks will withstand multiple manipulations that are common with image transactions. We use a 2D Barcode as the watermark as this has error correction capabilities and show that this can be used to insert data imperceptibly into the host image. One Barcode is inserted into the low frequency component of the image and a second Barcode watermark is embedded into low pass component of any wavelet decomposition at a specific level only known to the author. This improves the resistance of the watermarking scheme to attack. Our experimental results indicate that these invisible watermarks can carry significant information and are robust to many image manipulations.

Disciplines

Physical Sciences and Mathematics

Publication Details

This conference paper was originally published as Premaratne, P., Safaei, F., 2D barcodes as watermarks in image authentication, 6th IEEE/ACIS International Conference on Computer and Information Science ICIS 2007, 11-13 Jul, 432-437.

2D Barcodes as Watermarks in Image Authentication

Prashan Premaratne and Farzad Safaei
School of Electrical, Computer & Telecommunications Engineering,
University of Wollongong, Australia.
prashan@uow.edu.au

Abstract

2D barcodes are increasingly used as tags in every type of goods for unique identification. Compared with the 1D barcodes, 2D barcodes not only can carry more data but also can withstand errors in subsequent scans. This property has significant parallels to watermarking logos as such watermarks will withstand multiple manipulations that are common with image transactions. We use a 2D Barcode as the watermark as this has error correction capabilities and show that this can be used to insert data imperceptibly into the host image. One Barcode is inserted into the low frequency component of the image and a second Barcode watermark is embedded into low pass component of any wavelet decomposition at a specific level only known to the author. This improves the resistance of the watermarking scheme to attack. Our experimental results indicate that these invisible watermarks can carry significant information and are robust to many image manipulations.

1. Introduction

The Internet has revolutionized the information exchanges and many of the traditional information exchanges now take place at a flick of a button. This in turn has created a plethora of problems where the exchanges are ripe for misuse. Today, increasing number of digital security experts are employed just to keep tabs on this illicit trade, piracy and unauthorized dealings on the Internet. The rising tension and stress in safeguarding these rights can only be lessened with increasing attention to these issues by the research community. Duplication and redistribution of images especially of high commercial value such as satellite ground imagery are costing the industry millions of dollars every year. Curtail of such illicit trade will not only guarantee the future investment by the industry but will pave way for safeguarding artistic value of these media.

Digital watermarking is intended to encode secret or copyright information into host digital data to demonstrate and protect the ownership of these products. The three main digital data types in wide usage are audio/speech, images and video. Audio data and the feasible copyright protection is governed to a large extent by human auditory perception and is beyond the scope of this article. The research reported here is specifically aimed at images and video copyright protection related to the Human Visual System (HVS). Copyright or the ownership of any digital image is aimed at individuals or business entities who might potentially misuse or attempt to illegally make profits by claiming ownership. Watermarking is also used to authenticate the contents of the data and convey side information such as access control metadata or annotations. The main requirements of an effective watermark are given below.

1. **Perceptual invisibility**: A watermark should not protrude from the host so as to degrade its commercial or art value.
2. **Robustness**: A watermark should withstand unintentional or malicious manipulations.
3. **Trustworthy Detection**: The presence of a watermark should be easy to detect without false alarms.
4. **Efficiency**: Low computation overhead is desirable for watermark embedding to support real-time applications. There are other requirements such as
5. **Blind detection** where original host data is not needed for watermark detection.

In general, most existing watermark detection schemes can be categorized into public or private schemes [1]. In private schemes, a secret key is used to decipher the watermark but this is a highly undesirable approach in public schemes such as that which might be used in a DVD player. This is because of the absence of the original data or a public domain key. Hence, many watermarking schemes do trade-off robustness with relatively higher false alarm rates. This

6th IEEE/ACIS International Conference on Computer and Information Science (ICIS 2007)
0-7695-2841-4/07 $25.00 © 2007 IEEE

paper attempts to combine the versatility of few schemes [2] we have developed so that the combination would be robust to many watermark attacks [3], [4], [5].

To date, there are many public watermarking schemes. Some assume low correlation between the secret key and the image and hides data using spread spectrum in the spatial domain or compressed domain. Wong et al. [1] embeds cocktail watermark in the spatial domain whereas Lu et al. [6] extends this to become a blind multipurpose watermarking system having both robust and fragile watermarks. The latter is capable of detecting malicious modifications if the watermark is known. Langelaar et al. [7] embed the watermark as a bit sequence making use of the energy difference between adjacent blocks. Zhang et al. [8] embeds a watermark in DCT domain utilizing DC and low-frequency AC coefficients.

While single watermark embedding schemes are in the majority, there exist some schemes embedding more than a single watermark [9], [10]. Cox et al [9] assumes that the multiple watermarks are closer to orthogonal and extends the single watermark algorithms to embed multiples of them.

Though there are many spatial domain watermarking schemes, only a handful embeds watermarks in JPEG-compressed images. Choi et al. [11] and Loo et al. [12] use inter-block correlation to embed the bit information in selected DCT coefficients in JPEG images. This is achieved by adding or subtracting an offset to the mean value of the neighboring DCT coefficients. In another approach, Huang et al. [13] embed a watermark in low frequency DCT coefficients. This is a good approach to safeguard watermarks under JPEG compression schemes which manipulate coefficients in DCT blocks rendering many watermarking schemes very vulnerable. However, the major limitation of their scheme is that they have not demonstrated the feasibility of carrying useful information inside the watermark and recovering it faithfully in the midst of attacks. We build on their approach of watermarking using DC coefficients and expand the scheme to embed useful information using error correcting that withstands many image manipulations.

2. Where should the watermark lie?

Most of the early image watermarking schemes embeds information in Least Significant Bits (LSB) so as to ensure the watermark is perceptually invisible. These LSB components are in fact high frequency components that are easily masked by basic image manipulations and the addition of noise. Cox et al. [9] proposed that the watermark be embedded in perceptually significant components in order to preserve it in the midst of attacks. However, manipulation of DC components is very well known to cause block artifacts in watermarked images and coefficients have explicitly been excluded as possible hosts [14], [9]. Huang et al. [13] indicate that embedding a watermark in DC components of the DCT yields watermarks that are robust to compression. However, their approach produces watermarks that can easily trigger false alarms as a result of simple image manipulation tasks such as increasing brightness. Our approach to embedding a watermark or multiple watermarks is designed to achieve robustness in many watermarking attacks. We try to achieve robustness to noise, JPEG compression, cropping and other simple attacks that do not distort the low pass image information. In order to achieve robustness to JPEG type compression, a watermark (2D Barcode) is inserted into the DC components in the transform domain. We have successfully demonstrated this concept in [2]. Another watermark is then inserted into the low pass wavelet decomposition such that it would be almost impossible to unravel the decomposition depth and the type of wavelet decomposition used as they are unknown to anyone but the author. Since this approach is independent of the image content, the amount of computational complexity is low. Another advantage is that by designing a proprietary wavelet filter bank, users may find it almost impossible to decipher the watermark.

3. Watermarking in Wavelet domain

Image watermarking can be described as the superimposing of a weak image on the host image. Many have attempted to insert bit patterns into the high frequency component of the wavelet decomposition [15]. We have pursued research in this area and demonstrated that image manipulations such as the simple addition of noise can irrecoverably mask the watermark. Hence, the high frequency component of the image is certainly not the best choice for point of insertion of the watermark. Alternatively, it is known that the low pass component of the wavelet decomposition is untouched by the addition of noise if the decomposition is deep enough. That is, noise affects the watermark to a lesser extent if this watermark is superimposed on a level 2 decomposition than on a single level decomposition. When higher levels of wavelet decompositions are sought, more and more high frequency information is separated out of the low pass image. However, the deeper the decomposition, the smaller the host image size becomes and there is thus a reduction in the area

available for watermarking. This is crucial as our 2D Barcode can encode more information into the host image when the image size is large. Fig. 1. shows a gray scale 512x512 sized version of the well known 'Lenna' image. Fig. 2 (a), (b), (c), and (d) show the low pass components of the wavelet decomposition using Daubechies' type 4 wavelet ('db4') [16] at 1, 2, 3 and 4 levels. When compared with Fig. 1, Fig. 2(a)-(d) accurately represent the image sizes when undergoing wavelet decomposition.

Fig. 1. Original image of 'Lenna'.

(a) (b) (c) (d)

Fig. 2. Low pass components of Fig. 1 at wavelet decomposition levels (a) 1, (b) 2, (c) 3, and (d) 4 using 'Daubechies' type 4 wavelet.

Superposition of watermarks on host images in the spatial domain has been proven to be susceptible to watermark attacks. Such watermarks can easily be wiped out buy pixel wise manipulations such as smoothing. To counteract this, we use transform domain watermarking; we have found that this is robust to many deliberate image manipulations.

In this section, we present a watermarking algorithm that embeds a watermark in transform domain on the low frequency component of the wavelet decomposition of the host image. Multiple copies of the watermark are added to the relatively flat regions (higher frequencies) of the transformed low pass component so that the resulting watermarked image is visibly unaltered. The presence of multiple copies would facilitate the detection of the presence of a watermark as well as recognition of the watermark without triggering false alarms. The watermarking steps can be highlighted as follows:

1. Decompose the host image into any level of wavelet decomposition and obtain the low pass image
2. Convert this low pass image into the transform domain using 2D Fast Fourier Transform (FFT)
3. Generate a 2D Barcode with encoded data (this is the data sitting in the watermark) which is a 1, -1 2D bit pattern of much smaller size than the transformed low pass image
4. Adaptively embed (superimpose) a weighted 2D Barcode so that the highest barcode intensity is achieved in the resulting watermarked image.

The above steps can also be mathematically described. The original image $f(x,y)$ is decomposed to level n and isolate the low frequency component. That is

$$f(x,y) \overset{2DWT}{\rightarrow} .. \overset{2DWT}{\rightarrow} L_n + V_n + H_n + D_n \qquad (1)$$

where L_n, V_n, H_n, D_n stand for low, vertical, horizontal and diagonal 2D wavelet decomposition at level n. Then the low frequency component (L_n) is transformed into the Discrete Fourier Transform (DFT) domain and is subdivided into odd k non overlapping regions where and large magnitude components are grouped into few regions such that

$$DFT(L_n) = \bigcup_k I_k \, . \qquad (2)$$

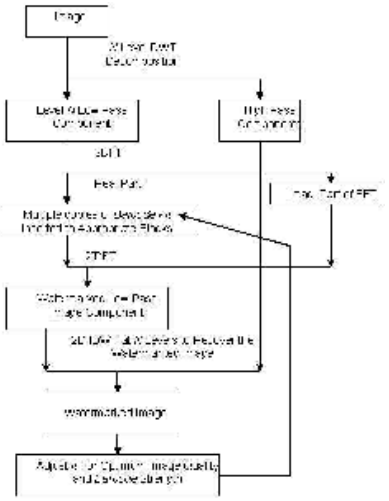

Fig. 3. Flow chart representing the wavelet domain watermark embedding scheme.

The algorithm then selects a few regions where the block signal strength is low and embeds the weighted *Barcode* adaptively - optimizing its intensity while generating a visually imperceptible watermark. This process can be mathematically described as follows:

$$I_k' = \begin{cases} I_k + \mu B \text{ , if } \sum I_k \ll \sum I_0 \\ I_k \text{ , otherwise} \end{cases} \quad (3)$$

Here, μ is the weight value for the *Barcode* intensity and I_k are non overlapping blocks in the transform (DFT) domain. I_0 is the block with the highest magnitude low frequency. Once the optimum *Barcode* is inserted, it can be inverse Fourier transformed to arrive at the wavelet low pass component and can be combined with other high frequency components to inversely transform to the watermarked image as follows:

$$\bigcup_k I_k' \xrightarrow{2IDFT} L_n' + V_n + H_n + D_n \xrightarrow{2IDWT} L_{n-1} \xrightarrow{2IDWT} .. \xrightarrow{2IDWT} f'(x,y) \quad (4)$$

The flowchart shown in Fig. 3. summarizes the wavelet domain watermark embedding process. As can be seen from the diagram, this is an optimization process performed by the user to estimate the optimum strength of the *Barcode* on the host image so that the watermarked image remains visibly unchanged. An original 'Lenna' of size 512x512 under 'db4' wavelet decomposition produces a low pass component of 38x38 at level 4. This is very much like a thumbnail of the original image stripped off its high frequency information. In our approach, we treat this low resolution image as the one to be watermarked in the transform domain. Using 2D FFT, this image is transformed into a 64x64 frequency domain array.

It is also very important to discuss our selection of a 2D *Barcode* as the watermark in this research. The merit of this choice is the 2D *Barcode's* ability to encode relatively large amounts of information into a 2D array which is easily detectable as having only two levels of value (1 or -1). A modest 18x18 *Barcode* (*datamatrix*) can hold 24 numeric values or 16 alpha numeric values and can correct up to 6 bit errors and can cope with 9 erased values [17]. As an example, Fig. 4. depicts a 12x12 *datamatrix* encoded with the message 'prashan'. Another advantage of this kind of watermark is that it does not depend on the host image content and thus results in low computational complexity for the overall watermarking scheme. It also facilitates the archiving of ownership information of digital images as many watermarks can be reused alleviating the need for unique signatures.

Fig. 4. *Datamatrix* encoded with the message 'prashan' to be used for watermarking.

(3)

4. Watermarking of DC components

Another aspect of robust watermarking is that it should be resistant to compression type attacks. In order to develop a JPEG compression resilient watermark, it is important to understand the JPEG compression scheme. The JPEG scheme initially divides an image into 8x8 blocks and use DCT to obtain the coefficients of these blocks. Then zig-zag scanning is used to discard most of the high frequency coefficients resulting in high compression. Therefore, most watermarking schemes that hide data in details (high frequencies) of images are not resistant against JPEG compression. As indicated by Huang et al. [**Error! Bookmark not defined.**], manipulating the DC coefficient or lower frequency AC components can produce a watermark robust against JPEG compression. However, as mentioned earlier, brightness adjustment of a watermarked image can trigger false alarms (detection) using their method. We build on their technique to embed a 2D watermark with error correction ability, which uses the image DC components in the transform domain.

Initially the original image is divided into non overlapping 8x8 blocks and the technique evaluates the DCT of each block. This is followed by selection of the DC value of each block and a 2D array is formed. This array is then treated as the host image and is converted into the transform domain once again using 2D FFT. A few copies of a weighted *Barcode* can then be inserted into higher frequency areas with low coefficient values. These steps are similar to the steps in Section 3. We have embedded 5 copies of the 12x12 *Barcode* in our experiments. The redundancy is aimed at detecting the watermark when deliberate attacks such as cropping take place. Section 5. describes other merits of this approach.

5. Performance of the combined watermark

The versatility of any watermarking scheme lies in the robustness of the watermark to tampering and image manipulations. Therefore, we evaluated our scheme using basic image manipulations e.g. cropping, and JPEG compression and deliberate attacks such as smoothing and addition of noise.

Fig. 5. Watermarked 'Lenna' using the scheme in the wavelet domain (left) and Watermarked image using DC components (right)

5.1. Robustness to cropping

Cropping is in essence the physical separation of part of the original image to form a sub image. This could be a deliberate attempt to disguise the ownership of the original image or an innocent effort to highlight certain attribute of an image. In any case, it is important that the original watermark is still intact in the sub image and still detectable in the sub image.

Since we embed the watermark in the transform domain of the low pass image component, the watermark information is distributed throughout the image. By forming a sub image, this information can not be completely wiped out but could possibly become frail. However, by inserting 5 copies of the Barcode in the transform domain, our experiments have shown that enough information is present for watermark detection as shown in the experiments. The original "Lenna" image of size 512x512 was used to embed the Barcode as shown in Fig. 5. Here we used the 'db4' wavelet transform and decomposed the image to 4 levels resulting in a 65x65 low pass component. After the optimum intensity of the Barcode was evaluated adaptively, we inserted the Barcode in the transform domain. This image can then be treated as an original image and the previous steps of wavelet decomposition and subsequent transformation to the Fourier domain can be performed to detect whether the watermark is intact. The level 4 wavelet decomposition of this image using 'db4' would produce a 33x33 array and this can be converted into a 64x64 transform domain array using 2D FFT function. This image can then be treated as an original image and the previous steps of wavelet decomposition and subsequent transformation to the Fourier domain can be performed to detect whether the watermark is intact. The level 4 wavelet decomposition of this image using 'db4' would produce a 33x33 array and this can be converted into a 64x64 transform domain array using 2D FFT function. It is important to exploit the original watermarking knowledge when selecting the real array portion in which the potential watermark may lie. We inserted 5 copies of 12x12 Barcode into the transformed image. However, since some of the energy of the Barcode has been removed due to cropping, we can estimate the pixel energy ratio of the same area of the original non-watermarked image by referring to a similar image that has been similarly cropped. Mathematically this ratio can be given as

$$\rho = \frac{\text{energy}[\text{Real}(\sum_{1}^{5} T_k)]\big|_{\text{NonWatermarked}}}{\text{energy}[\text{Real}(\sum_{1}^{5} T_k)]\big|_{\text{Suspect}}} \qquad (5)$$

where T_k denotes the blocks of array (here the block size is 12x12 which was the size of the *Barcode*) in which the potential watermark should have been embedded and the energy is estimated as the sum of the squared array elements. For this experiment ρ was found to be 8.7 indicating that there is a significant difference between the non watermarked image sections and the suspect image sections and this could be due to the presence of the watermark. ρ should have values around 1 if not watermarked and this ratio is a good detector for the presence of watermark in this scheme.

5.2. Robustness to additive noise

Noise has the most impact on lower magnitudes of high frequency components and since we embed both watermarks on DC and lower frequency components, its effect is minimal. Fig. 6(a) shows a noisy watermarked image with peak signal-to-noise ratio (PSNR) of 26dB and 6(b) shows the recovered DC component watermark. Here, the *Barcode* has only 4-bit errors which can easily be corrected as it is less than the maximum 6 correctable errors for a 12x12 *datamatrix*.

5.2. Robustness to JPEG compression

Our main goal in watermarking the DC components in transform domain was to achieve high robustness to JPEG compression. It is important to see how robust our approach is in this regard. We used the non compressed image which had been watermarked using DC components and compressed it to 50% of the original quality using JPEG. The resulting compressed image is shown in Fig. 6(c) with PSNR of 30dB and the recovered datamatrix is shown in 6(d) with only 2-bit errors.

(a) (b) (c) (d)

Fig. 6. (a) Watermarked noisy image with PSNR of 26dB and the recovered matrix (b), JPEG compressed watermarked 'Lenna' with 50% quality (c) and the recovered matrix (d)

6. Discussion and conclusion

We set out to embed two types of watermarks in two different domains so that they would be robust to different kinds of attacks or manipulations. The watermark embedded in DC components is seen as a fragile watermark whereas the one embedded in wavelet domain can not be detected or manipulated by the end user. This is termed as a fragile watermark since it can easily be compromised by an attacker. The wavelet domain watermark can also be interpreted as a quality measure relative to the original watermarked image possessed by the author. Even if the end user removes the DC component watermark, the wavelet domain watermark signals the presence of a watermark and indicates possible attack. Since a proprietary wavelet filter can be used at any level of low pass filtering to embed a watermark, the end user may never be able to detect or destroy the watermark without distorting the image. However, we are actively involved in work aiming to recover the datamatrix when attacks are introduced on to the wavelet domain watermark.

10. References

[1] P.H.W. Wong, O.C. Au, and Y.M. Yeung, "A novel blind multiple watermarking technique for images," *IEEE Trans. Cirsuits Syst. Video Technol*., vol. 13, pp. 813-830, Aug. 2003.

[2] P. Premaratne, C. C. Ko, "A novel watermark embedding and detection scheme for images in DFT domain," in *Proc. 7th Int. IPA*, July 1999, vol. 2, pp. 780-783.

[3] S. Voloshynovskiy, S. Pereira, and T. Pun, "Attacks on digital watermarks: Classification, estimation-based attacks, and bench marks," *IEEE Comm. Magazine*, pp. 118-125, Aug. 2001.

[4] M. Wu, and B. Liu, "Attacks on digital watermarks", in *Proc. 33rd Asilomar Conference on Signals, Systems and Computers*, Oct. 1999, vol. 2, pp. 1508-1512.

[5] J. Du, C.H. Lee, H.K. Lee and Y. Suh, "BSS: a new approach for watermark attack," in *Proc. Fourth International Symposium on Multimedia Software Engineering*, 2002, Dec. 2002, pp. 182 – 187.

[6] C. S. Lu, and H. Y. M. Liao, "Multipurpose watermarking for image authentication and protection," *IEEE Trans. Image Processing*, vol. 10, pp. 1579-1592, Oct. 2001.

[7] G. C. Langelaar and R. Lagendijk, " Optimal differential energy watermarking of DCT encoded images and video," *IEEE Trans. Image Processing*, vol. 10, pp. 148-158, Jan. 2001.

[8] Y. J. Zhang, T. Chen, and J. Li, "Embedding watermarks into both DC and AC components of DCT," in *Proc. SPIE Security and Watermarking of Multimedia Contents III*, Jan. 2001, pp. 424-435.

[9] J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia, "*IEEE Trans. Image Processing*, vol. 6, pp. 1673-1687, Dec. 1997.

[10] C. T. Hsu, and J. L. Wu, "Hidden digital watermarks in images," *IEEE Transactions on Image Processing*, vol. 8, pp. 58-68, Jan. 1999.

[11] Y. Choi and K. Aizawa, "Digital watermarking using inter-block correlation: extension to JPEG coded domain," in *Proc. IEEE Int. Conf. Information Technology: Coding and Computing*, Mar. 2000, pp. 133-138.

[12] W. Loo, G.L. Heileman, and C. E. Pizano, "Fast and robust watermarking of JPEG files," in *Proc. IEEE 5th Southwest Symp. Image Analysis and Interpretation*, April 2002, pp. 158-162.

[13] J. Huang, Y. Q. Shi, and Y. Shi, "Embedding image watermarks in DC components," *IEEE Trans. Cirsuits Syst. Video Technol*., vol. 10-6, pp. 974-979, Sep. 2000.

[14] J. Huang, and Y.Q. Shi, "An adaptive image watermarking scheme based on visual masking," *Electron. Lett*., vol. 34, pp. 748-750, Apr. 1998.

[15] D. Kundur, D. Hatzinakos, "Digital watermarking for telltale tamper proofing and authentication", *Proceedings of the IEEE*, vol. 87-7, pp.1167 – 1180, July 1999.

[16] G. Strang, and T. Nguyen, *Wavelets and filter banks, Wesley-Cambridge Press*, 1996, pp.14-64.

[17] ---- (2004, July), DataMatrix Java Bar Code Package User Guide, [online]. Available: http://www.idautomation.com/DataMatrixJavaBean/UserGuide.

0-7695-2841-4/07 $25.00 © 2007 IEEE