www.ijmer.com Vol.1, Issue.2, pp-729-732 ISSN: 2249-6645

Watermarking in Binary Images for Authentication

Aditi Jahagirdar[1], Dr. Manoj Nagmode[2]
[1](Dept of Information Technology, MITCOE, Pune, India)
[2](Dept. of E&TC, MITCOE, Pune, India)

ABSTRACT

Watermarking is a technique of hiding information in image including scanned text, figures, and signatures in such a way that it is difficult to intercept. In this paper, we discuss hard authentication for detecting tampering in binary images. Morphological transform domain is selected to avoid quantization errors introduced in real valued transform domain. Instead of using Detail coefficients as location map for data hiding locations, flipping of an edge pixel in binary image is viewed as shifting of edge location one pixel vertically and horizontally. To track these edges, algorithm based on Interlaced Morphological Binary Wavelet Transform (IMBWT) is used. We process an image as 2x2 pixel blocks called main processing blocks. This allows flexibility in tracking edges and reduces computational complexity. Flip ability of a coarse signal is determined by considering 3x3 blocks which consist of both main processing block and subsidiary blocks. In Single Processing Case (SPC), a coarse signal is considered flippable if both horizontal and vertical edges exist. Orthogonal embedding i.e. flipping the candidates of one does not affect the flippability conditions of another is used in Double Processing Case(DPC) and DPDC. This increases capacity of data hiding. RSA public key algorithm is used to generate hard watermark. Experimental results demonstrate validity of our argument. Also it is seen that tampering in watermarked image can be detected efficiently using this method.

Keywords- Authentication, Morphological Binary Wavelet Transform, Orthogonal embedding, watermarking

1. INTRODUCTION

Authentication of digital documents has aroused great interest due to their wide application areas such as legal documents, certificates, digital books and engineering drawings. In addition, more important documents such as fax, insurance and personal documents are digitized and stored. It is becoming important to ensure the authenticity and integrity of digital documents as the availability of the powerful image editing software has made copying and editing an image easier [1]. Detection of tampering and forgery are thus of primary concerns. Data hiding or watermarking for binary images authentication has been a promising approach to alleviate these concerns.

Many data hiding techniques have been proposed for color or grayscale images in which the pixels may take on wide range of values. Most of gray or color image data hiding schemes cannot be directly applied to binary images. Binary images can only take two values: either "1" or "0." The difficulty lies in the fact that changing pixel values in a binary image can cause irregularities that are very visually noticeable [2]. So hiding data in binary images is more challenging than in images of other formats. The goal of authentication is to ensure that a given set of data comes from a legitimate sender and the content integrity is preserved Authentication watermarking can be further classified into hard authentication and soft authentication.

The paper is organized as follows. Classification of watermarking techniques is given in section 2. In section 3 we discuss the Interlaced Binary Wavelet transform algorithm. Section 4 gives the actual steps implemented for embedding and extraction of watermark. Experimental results are discussed in section 5. Paper is concluded in section 6.

2. CLASSIFICATION OF WATERMARKING TECHNIQUES

2.1Classification Based On Robustness

A watermarking scheme can be classified as visible and invisible. Invisible watermarking can be either *robust* or *fragile*. Robust watermarks are generally used for copyright and ownership verification. High robustness is a requirement for copyright protection to provide ownership in any kind of attacks. On the other hand, a fragile watermark is a watermark that is readily altered or destroyed when the host image is modified through a linear or non-linear transformation. The sensitivity of fragile marks to modification leads to their being used in image authentication [3][4]. Fragile watermarks are useful for purposes of authentication and integrity attestation [5].

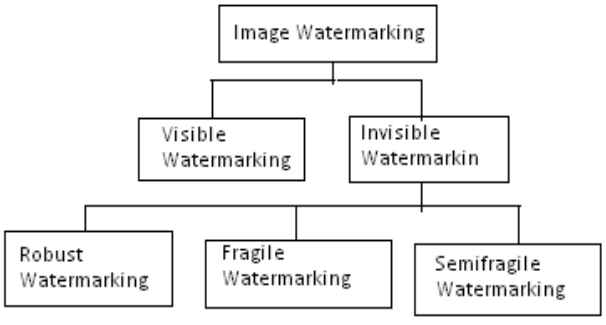


Fig: 1 Types of watermarking

A secure authentication system is useful in showing that no tampering has occurred during situations where the credibility of an image may be questioned [6].

It provides a guarantee that the image has not been tampered with and comes from the right source. The fragile watermark method is useful to the area where content is so important that it needs to be verified for it being edited, damaged or altered such as medical images. There exist also semi-fragile watermarking techniques, where some manipulations are allowed (for example JPEG compression to a pre defined quality factor) but other data manipulations are detected as tampering [7].

2.2 Classification Based On Domain Used

Images can be represented in spatial domain or in transform domain. The transform domain image is represented in terms of its frequencies; whereas, in spatial domain it is represented by pixels. In case of spatial domain, simple watermarks can be embedded in the images by modifying the pixel values. In transform domain, the image is segmented into multiple frequency bands, using various reversible transforms like Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), or Discrete Fourier Transform (DFT). Each of these transforms has its own characteristics and represents the image in different ways. Watermarks can be embedded within images by modifying these values, i.e. the transform domain coefficients.

From the implementing point of view, the digital watermarking algorithm can be divided into two domains, the space domain and the frequency domain. LSB and Patchwork are typical algorithms in space domain. The capacities of the special domain algorithms are not large enough, especially for small images. In frequency domain algorithms, DFT (Discrete Fourier transform), DCT (Discrete Cosine Transform) and DWT (Discrete Wavelet transform) are the most widely used three frequency transforms. General comparison of spatial domain watermarking algorithms and transform domain algorithms as giveby Mahmoud El-Gayyar[8] can be given as follows.

Table1: Comparison Of Watermarking Techniques

	Spatial Domain	Frequency Domain
Computation Cost	Low	High
Robustness	Fragile	More robust
Perceptual Quality	High Control	Low Control
Capacity	High (Depends on size of image)	Low
Application	Authentication	Copy right

Transform domain methods have dominated the watermarking field from its early stages. In these methods some coefficients are selected and modified according to certain rules. The two most important numbers in this process are the length and the position of the watermark. These are usually heuristically chosen. In order to handle this problem, an adaptive scheme for the selection of the proper coefficients is analyzed in the present communication.

Transform domain watermarking generally include the following steps:

• Determine a frequency transform.
• Select transformed coefficients.
• Alter selected coefficients according to some rule.
• Inverse transforms.
• Save watermarked image.

Among the several categories of watermarking schemes, watermarking algorithms based on Discrete Wavelet Transform (DWT) usually produce watermark images with the best balance between visual quality and robustness due to the absence of block artifacts, and have been applied in various areas.

In this paper, an algorithm of digital image watermarking based on discrete wavelet transform (DWT) is discussed. RSA private key and encryption algorithm is used to generate hard watermark [9][10].

3. INTERLACED MORPHOLOGICAL BINARY WAVELET TRANSFORM FOR 2-D SIGNAL

Morphological wavelet transform gives detail coefficients which can be used as location map for data hiding in images [11]. Flipping a pixel involves changing the coefficients and thus shifts the edges horizontally and vertically. As a result, the edges used for finding data hiding locations can't be found in watermarked image and so are not useful for blind watermark extraction. To overcome this problem Interlaced Binary Wavelet Transform is used which keeps track of shifted edges. For this coarse signal is considered in 2x2 blocks as shown in Fig.2.

S(2m,2n)	S(2m,2n+1)
S(2m+1,2n)	S(2m+1,2n+1)

Fig 2: Designations of the samples in a 2 x 2 block

To define a 2-D transform, one sample in the 2 *x* 2 block can be sub-sampled as the coarse signal. The difference between the sub-sampled sample and its vertical, horizontal, and diagonal neighbors gives the horizontal, vertical and diagonal detail signals. The resultant transformed signal remains binary and the coarse and detail signals will each be 1⁄4 the size of the original signal. Based on the starting coordinates in the top left position, each 2x2 block in 2D image is classified as

1. Even-Even Block (EEB).
2. Even-Odd block (EOB).
3. Odd- Even (OEB).
4. Odd-Odd (OOB)

The transform for all these four groups collectively called as IMBWT [11]. Depending on these blocks four single processing cases can be defined where anyone will be main processing block and others will be subsidiary blocks.

Here for finding the flip ability conditions of pixels, three different methods are considered. They are

1) SPC (Single Processing Case)
2) DPC (Double Processing Case)
3) DPDC (Double Processing with Distortion control)

3.1 Single Processing Case

In SPC only one from EEB, OOB, EOB and OEB is considered as a main processing block. Flipping an edge pixel in binary images is equivalent to shifting the edge

www.ijmer.com Vol.1, Issue.2, pp-729-732 ISSN: 2249-6645

location horizontally one pixel to the left or right and vertically one pixel up or down as shown in Fig.3

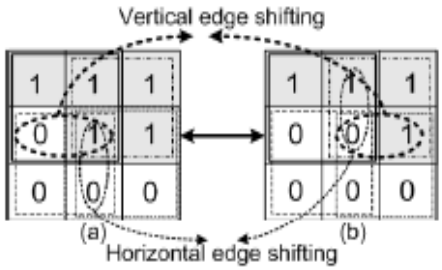


Fig 3: Illustration of edge shifting phenomenon

"1" and "0" represent the black and white pixels, respectively. A horizontal edge exists if there is a transition between two neighboring pixels vertically and a vertical edge exists if there is a transition between two neighboring pixels horizontally. In SPC, Flip ability condition is define such that a coarse signal is flippable if both horizontal and vertical edges exist.

3.2 Double Processing Case

The capacity of the proposed scheme can be increased significantly by combining two single processing cases, Even-even and odd-odd, namely Double processing case (*DPC)* algorithm. This is called as Orthogonal Embedding as described earlier. The maximum number of candidate pixels increases from
[1/4 x M x N] to [1/2 x M X N] for M x N sized image.

3.3Double Processing With Distortion Control

It is possible to minimize the distortion for *DPC*, using double processing with distortion control algorithm (*DPDC*). Each time when a *block* is processed, an embedder is chosen such that the visual distortion between the original and watermarked patterns is minimum.

4. AUTHENTICATION-VERIFICATION PROCESS

4.1 Steps for Watermark Embedding

The steps for hard authenticator watermark embedding process can be described as follows
1) Find the embeddable locations in Image Y using IMBWT for SPC, DPC or DPDC.
2) Clear the 'embeddable' locations by setting them to '0's to generate the intermediate image Y1.
3) Feed the intermediate image Y1 into a hash function H() to generate hash value Ho = H(Y1).
4) Employ the RSA private key to generate Ws = Ek(Ho, Ks)Where Ks is a private key and Ek() is encryption algorithm.
5) Perform XOR of Ws with payload watermark Wp to generate hard authenticator watermark Wr.
6) Embed Wr in the embeddable blocks by flipping the candidates found in step1.
7) Obtain the watermarked image Yw by computing inverse IMBWT for main processing blocks to reconstruct the candidate pixels.

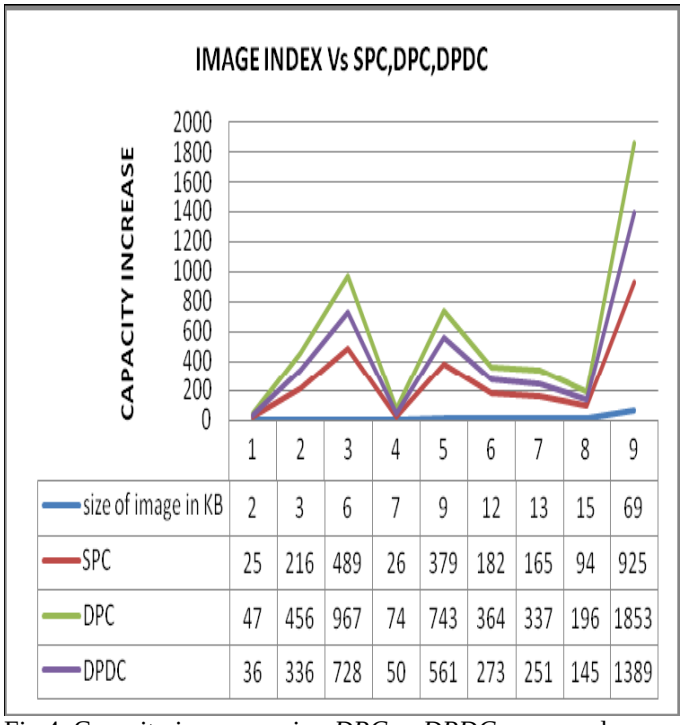
4.2 Steps for watermark extraction

1) The first three steps, i.e. find the embeddable locations, generate the intermediate image y1'and generate the hash value of the watermarked image are same as steps 1 to 3 of embedding process.
2) Extract the watermark Wr' and split it into two parts Ws' and Wp'.
3) Employ public key Kp to decrypt Ws' to obtain the hash value of original image.
3) Compare Wp' with Wp to check the authenticity of image.

5. EXPERIMENTAL RESULTS

5.1 Embedding capacity comparison

To show the capacity increase by employing DPC and DPDC compared with that of SPC, various images of a variety of sizes are used. These images are of different types (e.g., lena, text, handwritten text in different languages and sizes etc.). The capacity increase for different sizes of images obtained from SPC, DPC and DPDC for different images is shown in Fig. 4.



	1	2	3	4	5	6	7	8	9
size of image in KB	2	3	6	7	9	12	13	15	69
SPC	25	216	489	26	379	182	165	94	925
DPC	47	456	967	74	743	364	337	196	1853
DPDC	36	336	728	50	561	273	251	145	1389

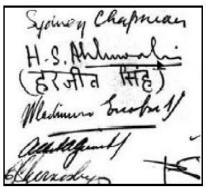
Fig 4: Capacity increase using *DPC* or *DPDC* compared with that of *SPC*.

It is seen that embedding capacity is maximum in DPC but visual quality of the image is not up to the mark. DPC gives more capacity as compared to SPC and good visual quality than DPDC. It is also observed that embedding capacity depends on contents of the image than size.

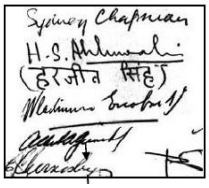
5.2 Watermark embedding and extraction for application "signature in signature"

In this application, authenticity of signature can be checked by adding a small signature in main signature. If extracted watermark matches with original watermark then signature is treated as authentic.

Fig.5 shows the result of embedding signature image of pixel size 26 x 27 in the host image again of signature of pixel size 231x 211. It is seen that visual quality of image after watermarking is satisfactory and extracted watermark also matches with original watermark.



(a)Input Image (b) Watermark

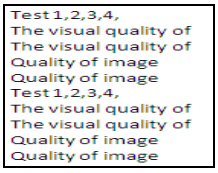


(c) Watermarked Image (d) Retrieved watermark

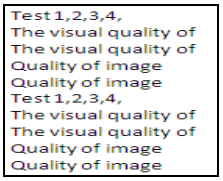
Fig: 5 Watermark embedding and extraction

5.3 Tampering detection

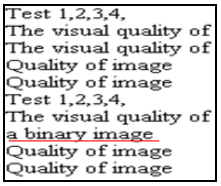
In the following example, in Fig. 6, a logo (b) is added to the text image (a) to generate the watermarked image (c). Extracted watermark is shown in (d). To test the algorithm for tampering detection, some text is added to the watermarked image (e). It is observed that the extracted watermark (f) is distorted proving that the image is tampered. Thus it can be seen from the results that logo image can be reconstructed perfectly when no tampering occurs where as looks like a random noise pattern when watermarked image is tampered.



(a)Original image (b)original watermark



(c)watermarked image (d)Extracted watermark



(e) Tampered Image (f) Watermark extracted from tampered image

Fig 6 : Tampering Detection in text image

6. CONCLUSION

A high-capacity data-hiding scheme for binary images authentication is developed based on the interlaced morphological binary wavelet transforms. Embedding capacity of image is increased considerably by using orthogonal embedding in DPC and DPDC as compared to SPC. Visual quality of the watermarked image is satisfactory. Experimental results show that this method detects the tampering done in image efficiently. The present scheme is superior in being able to attain larger capacity while maintaining acceptable visual distortion.

REFERENCES

[1] M. Wu and B. Liu, "Watermarking for Image Authentication", *Proceedings of IEEE International Conference on Image Processing, 1998, vol.2*, pp. 437-441

[2] H. Yang and Alex C. Kot, "Pattern-Based Date Hiding for Binary Images Authentication by Connectivity-Preserving", *IEEE Trans. On Multimedia, vol. 9, no. 3*, pp. 475-486, April 2007

[3] B. Chen and G.W.Wornell, "Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding," *IEEE Trans. on InformationTheory, vol. 47, no. 4*, pp. 1423-1443, May 2001.

[4] Y. Zaho, "*Dual Domain Semi-Fragile Watermarking for Image Authentication*", Master Thesis, University of Toronto, 2003.

[5] Min Wu, and Bede Liu, "Data Hiding in Binary Images for Authentication and Annotation", *IEEE Trans. on Multimedia, vol. 6, no. 4*, pp. 528-538, August 2004

[6] M. Fridrich and A. Baldoza, "New fragile authentication Watermark for Image", *ICIP 2000*, Vancouver, Canada (2000).

[7] R. Swierczynski, "Fragile Watermarking Using Subband Coding", *Institute of Electronics and Telecommunication Poznan University*, Sept. 2002.

[8] Mahmoud El-Gayyar, "Watermarking Techniques Spatia Domain Digital Rights Seminar *Media Informatics University of Bonn Germany*, May 2006

[9] P.S.L.M. Barreto, H.Y. Kim, V. Rijmen, "Toward a Secure Public-key Blockwise Fragile Authentication Watermarking", University of São Paulo, Brazil and B-3000 Leuven, Belgium.

[10] P.W. Wong, " A PublicKey Watermark for Image Verification and Authentication" *Proceedings of IEEE International Conference on Image Processing,1998, Vol.1*, pp. 455-459,(MA 11.07).

[11] Henk J. A. M. Heijmans, and J. Goutsias, "Nonlinear Multiresolution Signal Decomposition Schemes-Part II: Morphological Wavelets" *IEEE Trans. on Image Processing, vol. 9*, no. 11, pp.1897-1913, Nov. 2000

[12] Huijuan Yang, Alex C. Kot, "Orthogonal Data Embedding for Binary Images in Morphological Transform Domain-A High-Capacity Approach" *IEEE Transactions On Multimedia, Vol. 10, No. 3*, April 2008 339.