Robust Image Watermarking Based on Average and Significant Difference

Dipti Patel, Suprava Patnaik

Abstract— **This paper proposes a blind watermarking technique in the Wavelet domain, with improved robustness against various image processing attacks. Rather than considering state-of art practice of significant frequency pixels with maximum intensity for water marking, two local coefficients with dual constrained of being locally maxima along with less difference between them are considered suitable for watermark embedding. Difference between local maximum and local second maximum values is modified to embed the watermark. A search of coefficients, with local significant value as well as insignificant difference, operates on non-overlapping row vectors of 3-level decomposed high frequency sub-bands of images. Watermark is extracted by comparing the significant difference of every block. Experimental results are shown to justify the improvement achieved by the proposed algorithm against attacks like JPEG compression, Gaussian filtering and different noise. The process is very straightforward and simple to implement.**

Index Terms—**Blind Watermarking, Discrete Wavelet Transform(DWT), Cross correlation,**

I. Introduction

A digital image watermark is a logo/signal embedded into a host image that can be detected or extracted later by means of some operations for authentication purposes. The most important properties of any digital watermarking techniques are security, perceptually inseparable from the *host* image, robust enough to resist many image processing manipulations and acceptable complexity without hampering image quality. Robustness is defined as the recovery of the watermark after the image operations such as filtering, lossy compression, filtering, brightness correction or enhancement and also resistance to malicious attacks. Generally speaking, improving the embedding intensity can increase the resistance capacity for attacks like smoothing, compression, Gaussian low-pass filtering etc.. However, the robustness of sharpen; geometric transform attacks cannot be strengthened. Complexity is described as the effort and time required for watermark embedding and retrieval.

Binary watermark is pattern, generated either by pseudo random number generators, row transformed binary logo image or a biometric extracted for secured identification. In general, watermarking techniques applied to images are classified into two major classes based on the domains of embedding the binary pattern to a host image, namely spatial domain and frequency domain. Spatial domain watermarking modifies the pixel intensity for a subset of image. Modification might include flipping the low-order bits or replacing lower order bit plane with the watermark. Although it may survive transformations such as cropping, any addition of noise or lossy compression is likely to defeat the watermark. Frequency domain watermarking techniques, also called transform domain technique, alters certain frequency components. Some of the algorithms operate using for example DCT, DFT or DWT. Typically frequency alteration are done in the middle frequency range. Alternation of lower frequencies adds perceptual separation between the watermark and the host image. Alteration of high frequencies is likely to loss during lossy compression and filtering. It is also preferred to spread the watermark uniformly over the host image in order to avoid missing retrieval due to cropping. The research on technologies of information hiding and digital watermarking has developed for nearly twenty years and many literatures are available on it. In [1] authors have proposed a spatial domain technique using singular value decomposition and quantization. Blocks having high number of edges are selected for embedding to improve perceptibility. Square diagonal matrix resulted from SVD is used to embed watermark based on quantization. Frequency domain watermarking schemes are more robust to tampering and attacks than those in spatial domain. However, by using this approach embedding capacity reduces as compared to spatial domain. Reference [2] describes a watermarking technique based on two levels DCT and two levels SVD. Original image is divided into non-overlapping blocks of size 8 × 8. Each block is decomposed twice using DCT. SVD is applied to each block. First s-matrix value from every block is collected to form a matrix which is decomposed using SVD again. Watermark is embedded into resulted s- matrix. Ke Luo and Xiaolin Tian [3] proposed DWT based watermarking method that includes multiple embedding in two different frequency ranges to improve robustness. Hamming coded watermark is embedded into lower frequency coefficients to withstand against low-pass filtering and lossy compression attacks. Same watermark is embedded into mid frequency coefficients using spread spectrum technique to improve robustness. In this pare we have adapted a frequency domain local significant selection approach with a motivation to achieve efficient trade-off between capacity and perceptibility.

Paper is organized as follows. In section-II we have described the proposed embedding steps, followed by

Manuscript received August 11, 2011.

Dipti Patel is doing resear at Sardar Vallabhbhai National Institute of Technology ,Surat, GJ 395007, India (e-mail: dipti.patel1987@gmail.com).

Suprava Patnaik is with Sardar Vallabhbhai National Institute of Technology ,Surat, GJ 395007, India ,phone: 9904402677; fax: 91-261-222-7334; e-mail: ssp@ eced.svnit.ac.in

extraction steps described in section-III. Experimental results for various attacks are shown in section-IV. Paper ends with a conclusion in section-V.

II. Watermark Embedding Based on Average and Significant Difference

An advantage of the spatial watermarking techniques is, they can be easily applied to any image. A possible disadvantage of spatial techniques is they do not allow for the exploitation of this subsequent processing in order to increase the robustness of the watermark. In addition to this, adaptive watermarking techniques are a bit more difficult in the spatial domain. For instance, it is generally preferable to hide watermarking information in noisy regions and edges of images, rather than in smoother regions. The benefit is two-fold; 1) Degradation in smoother regions of an image is more noticeable to the HVS, and 2) becomes a prime target for lossy compression schemes. The classic and still most popular domain for image processing is Discrete-Cosine-Transform (DCT). The middle frequency DCT coefficients are chosen for that they minimize or avoid exposing of the watermark in the visual important parts of the image (low frequencies), also removing the risk of removal through compression and noise attacks (high frequencies). One of the many advantages of the wavelet transform is that it is believed to more accurately model aspects of the HVS as compared to the FFT or DCT. This allows us to use higher energy watermarks in regions that the HVS is known to be less sensitive to, such as the high resolution detail bands (LH, HL and HH). Quantization based watermarking technique which aims to modify wavelet coefficients of high magnitude assures embedding the watermark into edge and textured regions of an image. Furthermore, by using the values of the transformed coefficients, the embedding process can be made rather adaptive. This technique improves the resistant to JPEG compression, cropping, and other typical attacks.

In proposed DWT watermarking method**,** significant difference between local maximum and local second maximum value is magnified according to the watermark bit, and is similar to the work proposed in [4]. Original image is decomposed using 3-level DWT. As number of levels increase, robustness and significance of coefficients increase at the cost of payload capacity. As justified earlier, LL3 band cannot be used for embedding as it contains important low frequency information and any minor change in this band coefficients leads to major perceptual distortion in an image. HH1~ HH3 bands are not suitable for embedding as it is very susceptible to compression. HL3 and LH3 can be used for embedding watermark. Proposed method utilizes LH3 and HL3 band for embedding. Use of both the bands handles larger payload, or if required accommodating multiple times embedding for very noisy environment. Fig.1 shows the embedding procedure for LH3 band. Embedding into HL3 band is done using the same steps except that the blocks are selected along the column.

Difference of our work from [4] is in the pixel and block selection process. In [4] the author has considered only positive values as significant coefficients and mentioned that positive coefficients are more robust to different attacks than the negative coefficients. Also the author has imposed the constrained, that larger the block size more will be the payload or embedding capacity. Discrete wavelet transform is a form of finite impulse response filter with time-frequency localization ability. For example the Haar wavelet is the simplest DWT with foundation on simple arithmetic operations like addition and subtraction. It is obvious that accurate synthesis of image coefficient is possible, given the knowledge of sum and difference values. Image coefficients being real and integers, sum always remains positive but difference depends on the phase of wavelet filter. Shifting the filter impulse response by half a time period, will alter the sign of wavelet coefficients. Therefore instead of considering only positive coefficients, we have included all the coefficients irrespective to the sign however marked them as suitable for watermark embedding, provided the difference between the two maxima values is less than some threshold value. Chances of missing all the coefficients for a block, due to high compression type attack is handled by shifting the maximum of low coefficient block to a significant value *T* for embedded a bit one . For a block transmitted with all zeros, or significant difference less than *T/2*, computed embedded bit takes value 0, which is also the required bit. Any attack, drifting the coefficient amount by more than *T/2*, includes chances of erroneous watermark extraction.

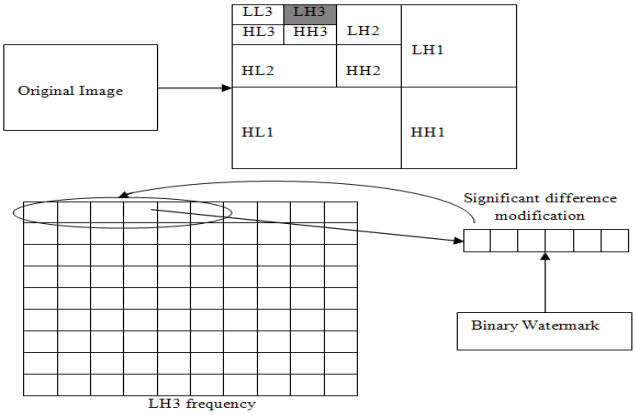


Fig.1. Watermark embedding block diagram

Embedding steps are:

Step-1: Original image is decomposed using 3-level DWT. Watermark is converted into binary bit stream. LH3 band is subdivided into non-overlapped vector blocks along the rows from left to right and then top to bottom. Block size is a trade-off between payload and robustness. A block is counted as adequate for embedding if it satisfies the significant difference requirement described next. It is obvious that considering blocks of smaller size, capacity will increases but at the cost of robustness. For copyright protection, minimum required payload capacity needs to be of 512 bits. So block size of 6 appears to be satisfying the requirement for host images of size 512 x 512. Using both LH and HL sub-bands doubles the capacity and makes room for inclusion of redundancy through error correction coding.

Step-2: The constrained perceptual invisibility is mainly influenced by two factors, image roughness and visual sensitivity. When a smooth surface is stained, it is easier to

ISBN: 978-988-18210-9-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

identify than when the surface is rough. Therefore selection of nodes for watermark embedding is related to intensity difference rather than magnitude. Calculation of significant difference of all the blocks using equation (1) can perform proper block selection.

$$Diff_i = max_i - sec_i \quad \ldots\ldots. (1)$$

Where, $1 \le i \le N$. N is the number of blocks. max_i and sec_i are the maximum and second maximum wavelet coefficients of i^{th} block. Embedding in all the blocks causes distortion in watermarked image. To maintain perceptual excellence only those blocks are selected whose $Diff$ value is lower than a threshold called upper bound.

Step-3: Calculate Average Significant Difference (ASD) value ε of selected blocks using equation (2),

$$\varepsilon = \left\lfloor \frac{1}{N_T} \sum_{i=1}^{N_T} (\max_i - \sec_i) \right\rfloor \quad \ldots\ldots\ldots\ldots (2)$$

Where, $\lfloor \ \rfloor$ is a floor function, ε is average significant difference, N_T is number of blocks which have $Diff$ value less than the upper bound and ($1 \le i \le N_T$). Larger the value of upper bound more will be the capacity but at the cost of perceptual degradation imposed by large coefficient quantization. Experimentally it has been observed 60 as the upper threshold provides good trade-off between robustness and payload capacity.

Step-4: Watermark bit 1 is embedded in a block using equation (3),

$$max_{inew} = max_i + T \ , \quad if \ (max_i - sec_i < maximum(\varepsilon, T))$$
$$= max_i \quad otherwise \quad \ldots\ldots\ldots (3)$$

Watermark bit 0 is embedded in a block using equation (4),

$$max_{inew} = sec_i \quad \ldots\ldots\ldots (4)$$

This confirms $Diff$ value for the block to be either between upper bound (T) and ε or 0 for embedding of 1 and 0 respectively.

Step-5: Repeat step-4 for HL3 band while considering the blocks column wise.

Step-6: Watermarked image is obtained by applying 3-level inverse DWT after replacing modified LH3 and HL3 coefficients for original LH3and HL3 bands.

III. Watermark Extraction

Watermark extraction procedure is very simple and consists of a comparator with binary output, to which the inputs are an adaptively computed threshold and the block $Diff$ values. The steps are as shown in fig. 2.

Extraction steps:

Step-1: Watermarked image with single or multiple attacks is decomposed for 3-levels of DWT.

Step-2: LH3 and HL3 bands are subdivided into non-overlapped vector blocks of size (1x 6) pixels. Only those blocks are selected whose $Diff$ value is lower than upper bound. Unmarked coefficients are unlikely to drift into the range of selected coefficients after an attack. The introduction of the T, to the watermarking algorithm gives a degree of tolerance to the system against attacks.

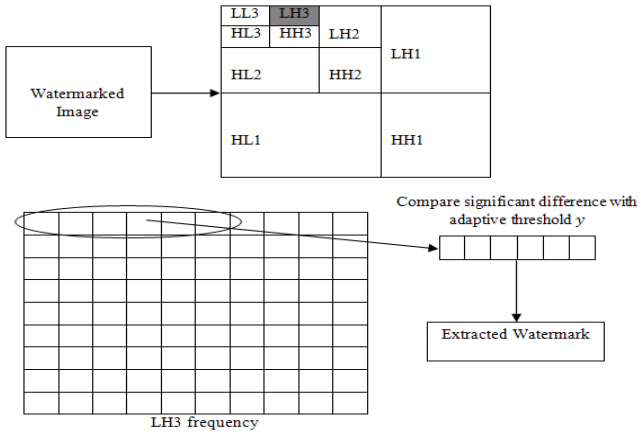


Fig.2. Watermark extraction procedure

Step-3: Threshold value y for the proposed method is attack depended hence estimated adaptively from the DWT coefficients of watermarked image using equation (5). Directly the upper bound used for block selection in the embedding process can"t play the same role in the inverse process. It might happen that $Diff$ for the original block is close to the upper bound and has crossed the upper bound due to some attack. The vice versa is original blocks with $Diff$ greater than upper bound may drift into the acceptable range. α is used to determine how many percentage of the significant difference can be averaged. Setting y equal to T/2 can extract the watermark exactly for no attack.

$$y = \left\lfloor \frac{1}{\alpha N_w} \sum_{j=1}^{\alpha N_w} \varphi(S_j) \right\rfloor$$

Where

$$\varphi(s) = \{Diff_1 < Diff_2 < Diff_3 ..... Diff_N\} \ldots (5)$$

is the set of Diff values arranged in increasing order for all the blocks taken from LH3 or HL3. N_w is the total number of blocks. $\varphi(S_j)$ is the vector with first j values of $\varphi(s)$. α is a scalar and $0 < \alpha < 1$.

Value of α is crucial and deciding parameter for adaptive threshold. Objective is to find the average of block $Diff$ s, excluding the big significant difference blocks which are not considered for embedding. For attacks like compression and Gaussian filtering probability of drift is less and α =0.8 discards the blocks with high $Diff$ value. However for attacks like median filtering percentage of drift is likely to be high and hence α =0.6 delivers a reasonable threshold.

Step-4: Fig.4.shows the sample variations in the cumulative distribution function of $Diff$ without any attack. The plot shows that variations occur for majority blocks for $Diff$ less than 60, which includes approximately 88% of the total blocks. Hence α in the range of 0.8 is well workable for defining y . Watermark is extracted using equation (6),

$$Recovered\ Watermark$$
$$Bit = 1 \ , \ if \ (Diff_i \ge y)$$
$$= 0 \quad otherwise \quad \ldots\ldots\ldots (6)$$

ISBN: 978-988-18210-9-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Where, $1 \leq i \leq Nw$

IV. Experimental Results

Size of test images used for evaluation of algorithm is 512 ×512.Three different types of watermark are used to verify the performance. These are 1) random number 2) a random binary character of size 25 x 21 and 3) binary string of minutia locations extracted from a fingerprint. Value of T is taken as 15and upper bound is set as 60. At receiver, value of α is varied between 0.6 and 0.8. Normalized Correlation (NC) between original and extracted watermark is calculated to compute efficiency of the algorithm. Fig.3. shows the binary string watermarked Lena image. Fig.4. shows the CDF of significant difference of LH3 sub band before and after embedding. It is seen that 85% of the blocks exhibits significant difference lower than 60 before and after embedding. Fig-5 shows sample results for minutia position watermarking when attacks are JPEG compression with Quality Factor(QF) 60 and 3x3 Gaussian filtering.

Fig.3 Watermarked Lena

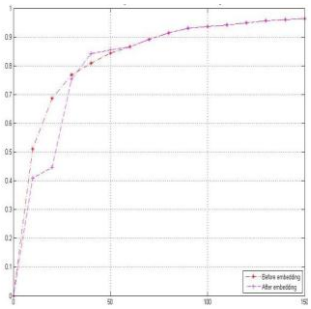


Fig.4 CDF plot with and without embedding

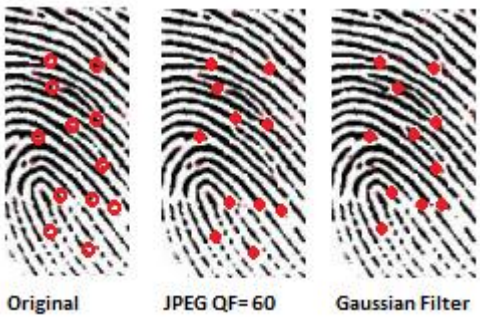


Fig.5 Sample result for minutia position watermarking.

More results are given in the tables 1-3 and also comparison is made with the results published in reference [4]. Normalised cross-correlation (NC) between the embedded and extracted strings is considered as the performance measure parameter.

Table-1 : Result for random sequence

Attack JPEG-QF	Our Method	Ref [4]	Attack	Our Method	Ref-[4]
100-70	1	1	Gaus Filter	.98	.86
60	.99	.99	Gaus Noise	.89	NA
50	.98	.97	Salt-Pepper	.88	NA
40	.97	.95	Hist Equal	.47	.77

Table-2 Normalized Correlation (NC) and retrieved watermark after different attacks for binary logo 'A'

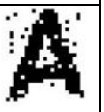
	JPEG 100-70	JPEG QF 60	JPEG QF 50	JPEG QF 40	JPEG QF 30
NC	1	.96	.85	.67	.62
					
	JPEG QF 20	Gau Filter	Histogram Equ	Gau Noise	Salt-Pepper
NC	.72	.99	.67	.54	.77
					

Table 3: NC for finger print minutia watermarking with different attacks

JPEG QF (100-70)	.99	Salt & Pepper Noise	.63
JPEG QF 60	.91	Gaussian Noise	.53
JPEG QF 60	.94	Gaussian Filter	.98

V. Conclusion

Proposed blind watermarking algorithm embeds watermark using the significant difference between local maximum and local second maximum values of DWT coefficients. It modifies coefficients by generating large energy difference between blocks for embedding watermark 1 and removing the difference in order to embed 0. This energy difference is utilized to extract the watermark using adaptive threshold. Experimental results demonstrate the quality of recovered watermark when exposed to various attacks. Increase in capacity allows redundant bits and hence it is comparatively robust. It is seen from experimental results that proposed algorithm gives better robustness for JPEG compression and Gaussian filtering however is not robust against histogram equalization.

References

[1] B.Chandra Mohan, S.Srinivaskumar, B.N.Chatterji, "A Robust Digital Image Watermarking Scheme using Singular Value Decomposition (SVD), Dither Quantization and Edge Detection", ICGST-GVIP Journal, ISSN: 1687-398X , Volume 8, Issue 1, pp. 17-22, June 2008

[2] Feng Liu, Yongtao Qian, "A Novel Robust Watermarking Algorithm Based On Two_Levels DCT and Two_Levels SVD", IEEE CSIP Third International Conference on Measuring Technology and Mechatronics Automation,pp. 206-209, 2011 ..

[3] Ke Luo, Xiaolin and Tian,"A New Robust Watermarking Scheme based on Wavelet Transform", IEEE CISP conference on Image and Signal processing, 2008, vol.1, pp. 312-316.

[4] Lin, W. H., Horng, S. J., Kao, T. W., Fan, P., Lee, C. L., & Pan, Y. (2008), "An efficient watermarking method based on significant difference of wavelet coefficient quantization", IEEE Transactions on Multimedia, 10(5), 746–757

ISBN: 978-988-18210-9-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)