Robust Phase Watermarking Algorithm using Complex Hadamard Transform

Abstract-

In this paper, a robust phase watermarking algorithm for still images is presented where the watermark information is conveyed in the phase spectrum in the transform domain. Phase watermarking algorithm that uses multi-polarity Walsh-Hadamard and Complex Hadamard transform is developed. The robustness of presented algorithm is investigated by its uniqueness, JPEG encoding and successive watermarking.

Index terms-Unified complex Hadamard transform,Multi-polarity complex Hadamard transform, Multi-polarity Walsh-Hadamard transform, Phase watermarking, Spectral techniques.

1. Watermarking

With the explosive growth of the Internet, the use of digital images is becoming more widespread as digital images are easily transmitted over networked systems. However, this has also heightened the problem of copyright protection. The owners of digital images are reluctant to allow the distribution of their works in a networked environment as exact copies can be obtained easily. Although encryption can be applied to limit access to only valid key-holders, there is no way to trace the reproduction or retransmission of the decrypted images. The characteristics of an effective image watermark are as follows:

(a) It should be perceptually invisible and should not result in artifacts that are different from those that may be seen in the original image.
(b) It should be robust to common signal processing operations such as sharpening, resizing, lossy compression, etc since operations that damage the watermarked images also damage the embedded data. Pirates may also attempt to remove the embedded watermark through other modifications to the watermarked images.

A novel hybrid watermarking technique for grey scale images based on the modified multi-resolution multi-polarity Walsh-Hadamard and Complex Hadamard transforms has been proposed and implemented in the MATLAB. A series of tests to gauge the robustness of the watermark is performed and the experimental results are also presented. The new watermarking technique based on multi-polarity Walsh- Hadamard and Complex Hadamard transforms can also be used in digital and color image processing.

2. Technique for insertion of Watermark

The design and implementation of a novel hybrid transform domain based watermarking technique for grey scale images is described in this section.
Figure 1 illustrates the stages involved in the insertion of watermark. It should be noticed that the secret key could be added easily in our watermarking scheme

.

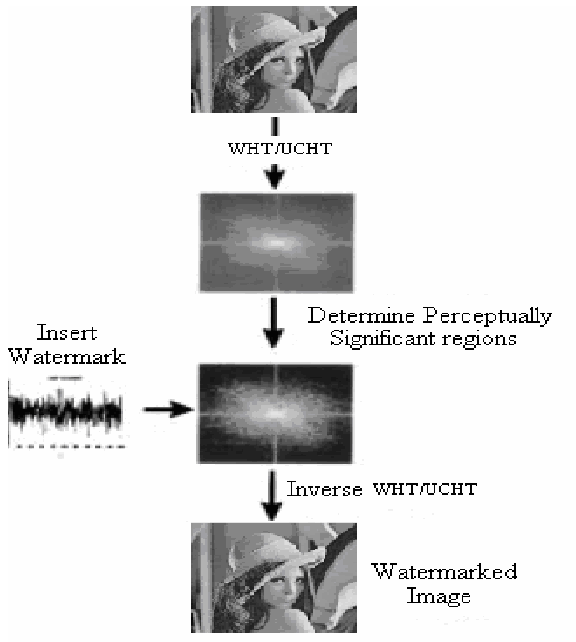

Fig 1. Insertion of watermark

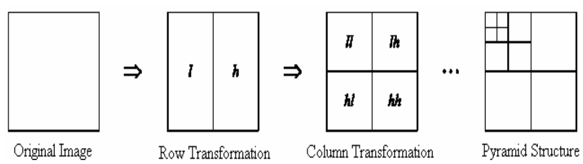

Fig.2 Multi Resolution decomposition of an Image

The insertion of the watermark consists of the following steps:

(a) The raw pixels are extracted from the BMP image and stored in a two-dimensional array. The dimensions of the image are adjusted to the next higher multiple of 8 to handle images of different sizes. For example, the original dimensions of an image are 500 × 300 pixels. The dimensions of the image are adjusted to 504 × 304 pixels, where the additional pixels are filled with 0.

(b) The modified multi-resolution integer-valued multi polarity WHT is applied to decompose the image into a pyramid structure with various bands such as the low low frequency band, low-high frequency band, high high frequency band etc. The modified multi-resolution integer-valued multi-polarity WHT is implemented in two steps and applied three times. The decomposition is performed as follows:

$$T_1[:,x] = \left\lfloor \frac{I[:,2x] + I[:,2x+1]}{2} \right\rfloor,$$

$$T_1\left[:,\frac{width}{2}+x\right] = I[:,2x] - I[:,2x+1],$$

$$T_2[y,:] = \left\lfloor \frac{T_1[2y,:] + T_1[2y+1,:]}{2} \right\rfloor,$$

$$T_2\left[\frac{height}{2}+y,:\right] = T_1[2y,:] - T_1[2y+1,:]$$

Where I [y, x], T_1[y, x] and T_2[y, x] refer to pixels in the original, temporary and transformed images, respectively. The symbol ":" on the left hand side of the comma refers to the rows of the image. When the symbol ":" appears after the comma, it refers to the columns. Width and height denote the dimensions of the ll quadrant and $\lfloor \cdot \rfloor$ represents the downward truncation. y and x denote the rows and columns of the images, respectively. The two-dimensional transformation is performed by applying the transformation on the rows followed by the columns of the image. The *ll* quadrant in Fig. 2 forms another image with half the resolution. The same transformation is applied to this reduced resolution image twice to form the pyramid structure.

(c) The lowest frequency band (LFB) is segmented into n 8×8 blocks.

(d) The two-dimensional multi-polarity CHT is performed on the segmented 8 × 8 blocks by applying the one dimensional multi-polarity CHT on the rows followed by the columns. The CHT coefficients of a real image are complex-valued which leads to a magnitude and phase representation for the transformed image.

(e) Similar to the DFT-based watermarking technique [5], the phase components of the selected CHT coefficients are altered to convey the watermark information. In phase watermarking, the condition that the image is real imposes the following constraint of the CHT coefficients:

$$P(k1, K2) = P^{*}(N1 - k1, N2 - K2)$$

Where $P(k1, K2)$ and

$P(N1 - k1, N2 - K2)$ are the CHT coefficients, * denotes the complex conjugate, N1 = N2 = 7 and $0 \leq$ k1, K2 ≤ 7 for an 8 × 8 block. Therefore, changes to the phase (δ) must preserve negative symmetry:

$$\angle P(k1, K2) \rightarrow \angle P(k1, K2) + \delta,$$
$$\angle P(N1 - k1, N2 - k2)$$
$$\rightarrow \angle P(N1 - k1, N2 - K2) + \delta,$$
$$\delta = (1 + G1 \times COV) \times G2 \times \Delta \times x_i$$

Where G1 and G2 are empirical constants set to 0.75 and 0.0075, respectively.

COV is the coefficient of variance of the pixels in the 8 × 8 block before the CHT and is defined as the standard deviation divided by the mean value. Δ is equal to 3°. The watermark $X = \{x_1, \ldots\ldots x_{n-1}, x_n\}$ is a pseudo random sequence

Where the values of xi are as follows:

$$x_i = -199 \text{ to } -50 \text{ for } x_i < 0,$$
$$50 \text{ to } 200 \text{ for } x_i > 0,$$

δ depends on the coefficient of variance as described in order to insert the maximum possible watermark in every block. If the COV of the 8 × 8 block is very small, the intensities of the pixels are close and it is not advisable to alter the CHT coefficients by a large amount. On the other hand, if the COV is large, the selected CHT coefficients can be altered by a larger amount without affecting the visual quality of the image. This approach of altering the selected CHT coefficients of the LFB ensures that the watermark is robust and secure as it is placed in the most significant components of the data. Hence, an attacker must target the fundamental structural components of the data, thereby increasing the chances of fidelity degradation.

The reasons for selecting the phase components are as follows:

(1) A watermark that is embedded in the phase of the CHT coefficients is more robust to tampering.

(2) From communications theory, it is well known that phase modulation possesses superior noise immunity when compared to amplitude modulation.

(f) After altering selected CHT coefficients, an inverse two-dimensional multi-polarity CHT is applied by performing the one-dimensional multi-polarity CHT on the columns followed by the rows.

(g) The inverse modified multi-resolution multi-polarity WHT is applied three times. The construction of the watermarked image from the altered transformed image is performed using the following inverse transformation:

$$T_1[2y,:] = T_3[y,:] + \left\lfloor \frac{T3[\frac{height}{2} + y,:] + 1}{2} \right\rfloor,$$

$$T_1\left[2y+1,:\right] = T_1[2y,:] - T3[\frac{height}{2} + y,:],$$

$$I_1[:,2x] = T_1[:,x] + \left\lfloor \frac{T_1[:,\frac{width}{2} + x] + 1]}{2} \right\rfloor,$$

$$I1\left[:,2x+1\right] = I_1[:,2x] - T_1[:,\frac{width}{2} + x]$$

Where $I_1[y, x]$, $T_1[y, x]$ and $T_3[y, x]$ refer to pixels in the reconstructed, temporary and altered transformed images, respectively.
(h) BMP file format is applied to create the watermarked copy of the original image.

3. Recovery of the Watermark

Figure 3 summarizes the stages involved in the extraction of watermark. It should be noticed that the watermark detector does not need the original image when a hash of the original image is used as a watermark.
The steps to extract the embedded watermark are performed as follows:

(a) The raw image pixels are extracted from the original and test images in BMP format. The dimensions of the images are adjusted to the next higher multiple of 8 to handle images of different sizes.
(b) The following steps are performed for the original image:

(1) The original image is decomposed into the pyramid structure using the modified multi-resolution multi polarity WHT.
(2) A forward multi-polarity CHT is performed on the segmented 8×8 blocks of the LFB.
(3) The watermark is inserted.
(4) An inverse multi-polarity CHT is performed and all the imaginary parts are set to zero.
(5) An inverse modified multi-resolution multi-polarity WHT is computed and the results of the inverse transformation are limited in the range from 0 to 255.
(6) A modified multi-resolution multi-polarity WHT is performed again followed by the forward multipolarity CHT of the segmented 8 × 8 blocks of the LFB.

(c) A modified multi-resolution multi-polarity WHT is performed on the test image followed by the forward multipolarity
CHT of the segmented 8 ×8 blocks of the LFB.
(d) A comparison of selected CHT transform coefficients of both images is performed.

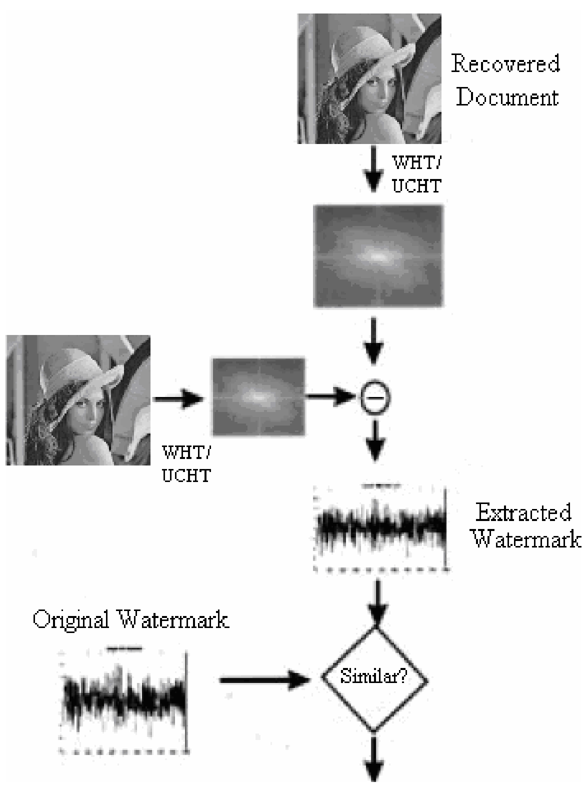

Fig.3 Extraction of watermark

4. Results

The proposed watermarking technique has been implemented in the MATLAB. In order to evaluate the proposed technique, the original grey scale image of 256 × 256 pixels shown in Fig. 4(a) is watermarked using the proposed scheme. The watermarked version is shown in Fig. 4(b). The robustness of the watermark depends directly on the embedding strength, which in turn influences the visual degradation of the image. The PSNR of the watermarked image with respect to the original image is 41.34 dB.

The watermarked image is subjected to a series of attacks to gauge the robustness of the embedded watermark:

(a) Uniqueness of Watermark: Fig.5 shows the response of the watermark detector to 1000 randomly generated watermarks of which only one matches the watermark embedded in Fig. 4(b). The positive response due to the correct watermark is very much stronger than the response due to incorrect watermark.

(a)Original (b) Watermarked

Fig.4 Original and watermarked versions of Lena

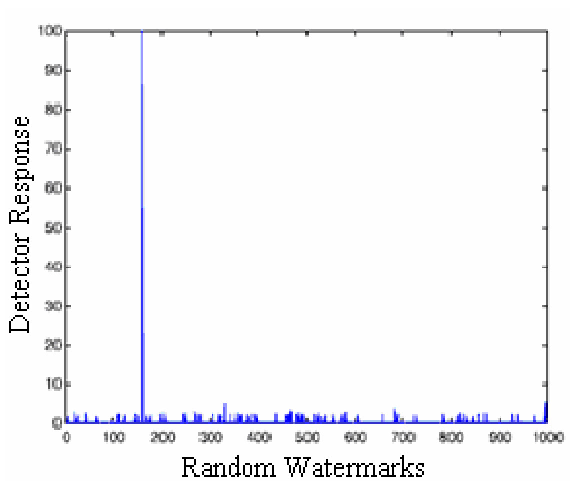

Fig.5 Watermark detector response

(b) JPEG Compression: In this test, the watermarked image is compressed using the standard JPEG encoding [9]. Figure 6 shows a JPEG encoded version of Lena at 10% quality factor and 0% smoothing. The embedded watermark is still detected even though the JPEG encoded image is clearly distorted. Table 1 lists the results for the JPEG compression tests from 10% to 100% quality factor.

Fig.6 JPEG Encoded version of Lena at 10% quality

JPEG coding Quality	PSNR (dB)	Detected
100	58.43	Yes
90	40.66	Yes
80	37.31	Yes
70	35.63	Yes
60	34.48	Yes
50	33.67	Yes
40	32.84	Yes
30	31.92	Yes
20	30.66	Yes
10	28.30	Yes

Table1 . Results of JPEG Compression tests

(c) Successive watermarking: The original image is watermarked, the watermarked image is then watermarked and so on. This can be considered as another form of attack in which it is clear that significant image degradation eventually occurs as the process is repeated. After five successive watermarking operations, the five watermarks are still detected in the resulting image (PSNR = 31.18 dB) shown in Fig. 7. In the response of the watermark detector given in Fig.8, the five spikes clearly indicate the presence of the watermarks and demonstrate that successive watermarking does not remove the embedded watermarks.

Fig.7 Image of Lena after five successive watermarking operations

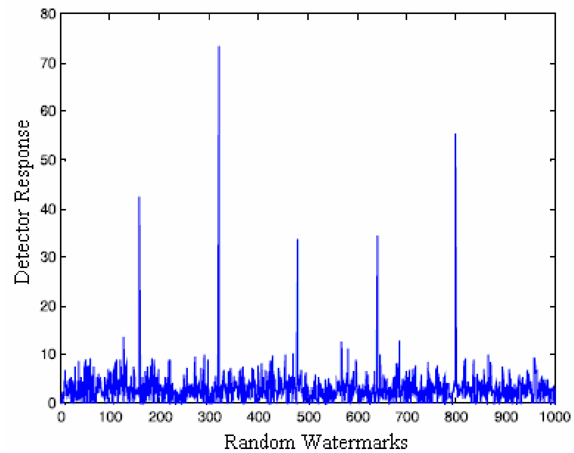

Fig.8 Watermark Detector response (Successive watermarking)

5. Conclusions

A new hybrid technique for watermarking grey scale images based on the multi-resolution modified multi-polarity WHT and CHT is proposed and developed. The quality of the watermarked image is very good. The proposed technique also exhibits robustness to JPEG compression up to 10% quality factor, successive watermarking of the original image.

6. References

1. Cox, I.J., Killian, J., Leighton, F.T., Shamoon, T.: Secure spread spectrum watermarking for multimedia. IEEE Trans. Image Process. 6(12), 1673–1687 (1997)
2. Falkowski, B.J.: Properties and ways of calculation of multipolarity generalized Walsh transforms. IEEE Trans. Circuits Syst. II: Analog Digit. Signal Process. 41(6), 380–391 (1994)
3. Falkowski, B.J.: Family of generalized multi-polarity complex Hadamard transforms. IEE Proc. Vis. Image Signal Process. 145(6), 371–378 (1998)
4. Ó Ruanaidh, J.J.K., Dowling, W.J., Boland, F.M.: Watermarking digital images for copyright protection. IEE Proc. Vis. Image Signal Process. 143(4), 250–256 (1996)
5. Ó Ruanaidh, J.J.K., Dowling, W.J., Boland, F.M.: Phase watermarking of digital images. In: Proc. IEEE Int. Conf. on Image Processing, pp. 239–242 (1996)
6. Rahardja, S., Falkowski, B.J.: Family of unified complex Hadamard transforms. IEEE Trans. Circuits Syst. II: Analog Digit. Signal Process. 46(8), 1094–1100 (1999)
7. Rahardja, S., Falkowski, B.J.: Complex composite spectra of unified complex Hadamard transform for logic functions. IEEE Trans. Circuits Syst. II: Analog Digit. Signal Process. 47(11), 1291–1297 (2000)
8. Rahardja, S., Ser, W., Lin, Z.: UCHT-based complex sequences for asynchronous CDMA system. IEEE Trans. Commun. 51(4), 618–626 (2003)
9. Wallace, G.K.: The JPEG still picture compression standard. Commun. ACM 34(4), 30–44 (1991)
10. Xie, S., Rahardja, S.: Performance evaluation for quaternary DSSSMA communications with complex signature sequences over Rayleigh-fading channels. IEEE Trans. Wirel. Commun. 4(1),266–277 (2005)