Digital Watermarking Using Complex Hadamard Transform and Phase Modulation

Roumen Kountchev [1], Vladimir Mirchev [2]

Abstract - **Image digital watermarking is the process of secretly embedding a short sequence of information inside the image without changing its perceptual quality. The bit sequence is embedded in a way that is difficult to find, modify or erase without a secret key. Standard image processing operations such as low pass filtering, JPEG compression, cropping, etc. should not remove the m[1]ark. We present a new digital watermarking method algorithm for copyright protection of still images. Watermark detection is done by comparing the watermarked image with the original one. The robustness to a JPEG image compression attack is demonstrated.**

Keywords - **watermarking, Complex Hadamard Transform, phase modulation**

I. INTRODUCTION

Image watermarking is an important technique for intellectual property protection of digital image information. Since the early 90's the area of watermarking has received a lot of attention from researchers in the signal, processing, security and multimedia communication communities. The rapid evolution of the Internet has lead to a growing concern about the protection of intellectual property. Since digital signals can easily be copied and reproduced in a way that is perceptually identical to the original, the chance of piracy of intellectual property has increased.

There are some requirements a good digital watermark must satisfy – robustness, perceptual invisibility and unambiguity. While this set of requirements is a must, others are also very important - high bit rate, security, constant bit rate, etc. There are a variety of watermarking techniques that have been proposed in the image digital watermarking literature. An overview of these techniques can be found in [4, 5].

It is known that much of the information that characterizes an image is contained in its phase. Most of the proposed algorithms use amplitude modulation techniques in order to embed the watermark bit sequence. Few of them use phase modulation [3].

In this article we describe a watermarking algorithm using phase modulation after applying a complex Hadamard transform. Similar to the watermarking technique described in [3], the phase components on selected transform coefficients are altered to convey the watermark information. It is well known that phase modulation possesses superior noise immunity when compared to amplitude modulation. One of the main differences between the algorithm described in [3] and the one proposed here is the choice of the CHT matrix used to perform the transform.

II. PROPOSED WATERMARKING ALGORITHM

In this section, a new watermarking algorithm is described. The technique is based on modifying the phase of image transform coefficients. The transform we are using in this article is Complex Hadamard Transform applied to 16×16 non-overlapping subblocks of the image. The basic principle of our watermarking technique is to set the phase of a coefficient according to value of the bit to be embedded. The choice of the coefficients is based on their type and amplitude – the coefficient must be complex, its module must be the highest one in the subblock and its module must be bigger than a chosen threshold. The calculation of the value of the threshold is done adaptively in order to increase the watermark detector's performance.

The Complex Hadamard transform we use in this algorithm is a rather new one. Although there are a few researches [1, 2, 3], its properties for the needs of digital signal and image processing are not studied well yet. The CHT matrices fulfill all the basic requirements expected from orthogonal transforms, such as linearity, uniqueness, complex convolution, etc. The CHT is confined to four complex values (±1 and ±j). In total, there are 64 CHT matrices that can be generated. The CHT matrix we use in our algorithm has several properties – all of the coefficients with both indexes even, have real values, the rest of the coefficients have complex values. Half of the complex coefficients are complex conjugates of the other half. This should be satisfied when altering a complex coefficient. The presence of real coefficients simplifies the calculations needed to perform the Hadamard transform. The integer arithmetic used in this transform is a big advantage compared to other complex transforms (e.g. DFT).

1	1	1	1
1	j	-1	-j
1	-1	1	-1
1	-j	-1	j

Fig. 1. $[CH_4]$ - Complex Hadamard Matrix 4x4

$[CH_2^{n-1}]$	$[CH_2^{n-1}]$
$[CH_2^{n-1}]$	$-[CH_2^{n-1}]$

Fig. 2. $[CH_2^n]$ - Complex Hadamard Matrix 2^n

[1] Roumen Kountchev, Dr. Sc., Professor is with the Faculty of Communications and Communication Technologies, Technical University of Sofia, Climent Ochridski 8, Sofia, Bulgaria, E-mail: rkountch@tu-sofia.bg

[2] Vladimir Mirchev, PhD student is with the Faculty of Communications and Communication Technologies, Technical University of Sofia, Climent Ochridski 8, Sofia, Bulgaria, E-mail: vsmin@mail.bg

Fig. 2 shows how to generate the complex matrices used to perform the CHT. We start with 4x4 matrix [CH_4], shown in Fig. 1 and calculate higher order matrices [CH_2^n] recursively from the previous ones.

The block scheme of our watermark embedding algorithm is shown in Fig. 3.

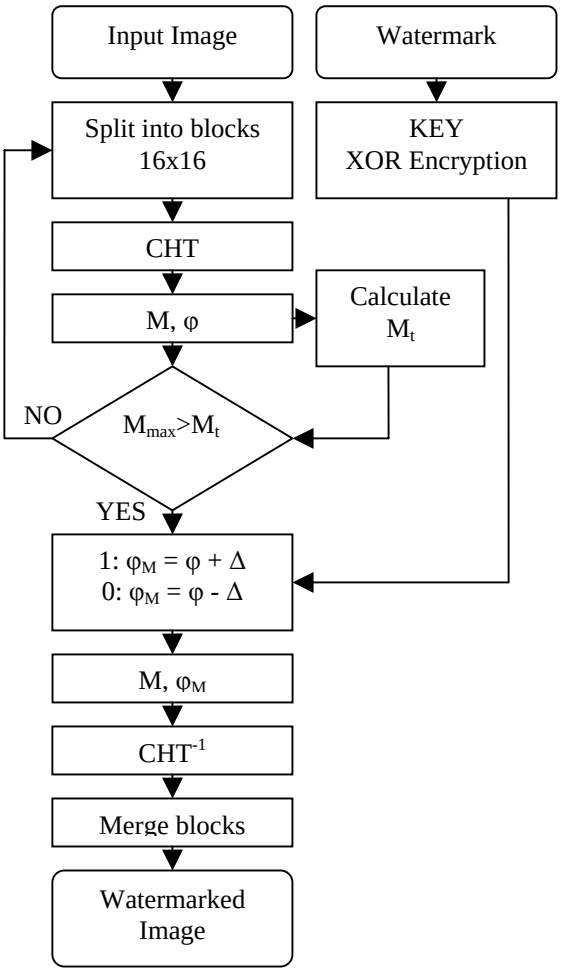

Fig. 3. Watermark encoder

First, we divide the input image into subblocks. We choose 16x16 pixels blocks so we can achieve high resistance to the popular JPEG image compression. Each subblock is processed by applying complex Hadamard transform. A translation from Decart to polar coordinate system is made. Then we find the complex coefficient *X[i, j]* with the highest module. If its magnitude is satisfies the chosen threshold value M_t, then an alteration of its phase is made according to the value of the current bit to be embedded. Higher magnitude transform coefficients are more immune to image processing operations than low magnitude coefficients. Furthermore, these coefficients preserve the most important information of the image and its integrity. The value of the threshold is adaptively calculated as an average value of the magnitudes of all complex coefficients in all of the previous blocks till and including the current one. The threshold condition guarantees that we will modify a coefficient in none homogenic image subblock. This leads to higher visual perceptibility. Alteration of the phase is made according (1):

$$\begin{cases} \varphi_M = \varphi + \Delta, \ represents\ binary\ 1 \\ \varphi_M = \varphi - \Delta, \ represents\ binary\ 0 \end{cases} \quad (1)$$

Where Δ is the depth of the watermark we embed. Choosing a bigger value for this parameter leads to higher robustness of the watermark, but also increases its visual perceptibility in the image and lowers the resulting PSNR.

The watermark bit sequence is encrypted by using a simple XOR operation with a randomly generated key. This insures that the information to be embedded has uniform probability distribution. This improves our algorithm in two aspects: first, one has to know both the encryption key and the watermark message in order to read the watermark, so the security of the watermark is higher; second, the potential autocorrelation in the watermark message is removed, thus improving the watermark resistance against various correlation detection attacks [4].

After that, an inverse CHT transform is made and the current subblock is replaced by the modified one.

The described process is successively made for all subblocks of the image. The result is a new watermarked image. The number of the subblocks that will stay unchanged due to the threshold condition can not be predetermined. That is, our watermark technique does not have the constant bit rate property and the amount of the embedded bits depends highly on the nature of the image to be watermarked.

The process of the watermark detection is shown in Fig. 2. The watermark extraction algorithm is very similar to the embedding one. The CHT transform is made twice – once for the subblock of the watermarked image and once for the corresponding subblock of the original image. The decision whether the current subblock is marked or not is made by taking the coefficient values from the original image, thus making it independent from the attacks applied to the watermarked image. If a subblock is found to be marked, the phase difference of the corresponding coefficients is calculated. According to the sign of the result the value of the current bit to be extracted is set (2).

$$\begin{cases} \varphi_M - \varphi > 0, \ extracted\ binary\ 1 \\ \varphi_M - \varphi < 0, \ extracted\ binary\ 0 \end{cases} \quad (2)$$

The resulting bit sequence is checked against the original one. If an error rate smaller than 25% is found, then the input image is claimed to be watermarked and the watermark message could be restored.

The decoding process in presence of geometric attacks is more involved. These attacks do not destroy the watermark, but rather disrupt the watermark synchronization. With the presence of the original image, an iterative search of set of inverse geometric operations can be made. Unfortunately, the iterative search approach is very computationally expensive and becomes even more so when the geometric attack does not introduce visible changes in the watermarked image. That's why, we often declare watermark is not present, when geometric attacks are applied.

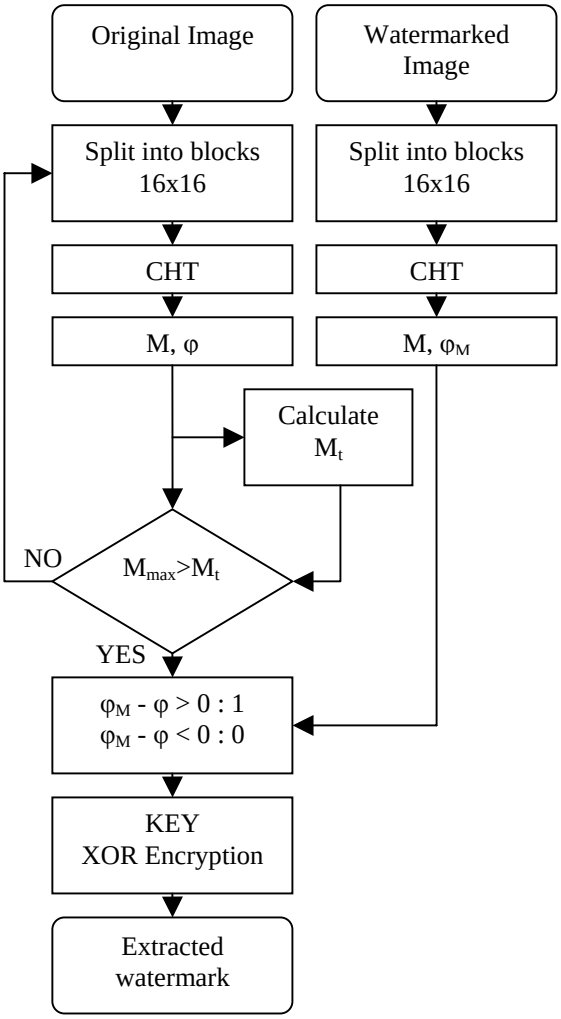

Fig. 4. Watermark decoder

III. SIMULATION AND RESULTS

A standard image was watermarked using the suggested algorithm. Figure 5 shows the original grey-scale image of 256×256 pixels. A block size of 16×16 pixels was used by the watermarking algorithm. The watermarked image is shown in Fig. 6. A total amount of 184 bits is embedded. Table 1 shows the amount of the embedded bits for four standard images. It proves that the watermark is embedded only in none homogenic areas of the image. Despite of the presence of the watermark no visible changes are made.

TABLE 1.
AMOUNT OF EMBEDDED BITS IN DIFFERENT IMAGES

Image name	Amount of embedded bits
Lena 256x256	184
Baboon 256x256	182
Camera 256x256	105
Peppers 256x256	179

Fig. 5 Original image “Lena”

Fig. 6. Watermarked image “Lena” at $\Delta = 12$

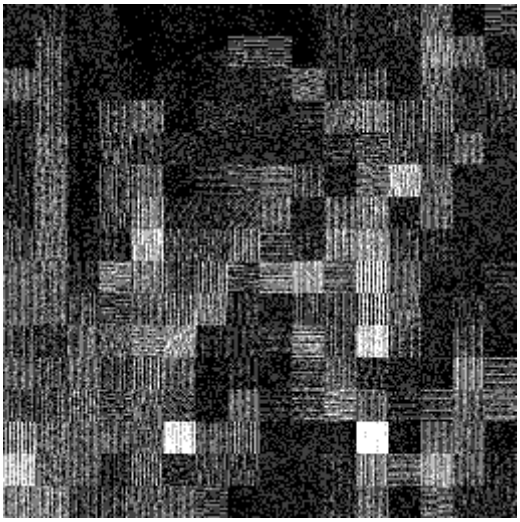

Fig. 7. Absolute difference image at scale factor 64

Figure 7 shows the absolute difference between the original image and the watermarked image “Lena” scaled by 64. As expected, the biggest difference occurs around edges.

In experiments the watermarked image is compressed using a JPEG encoder. Experimental results are shown in Fig. 8 and Fig. 9. Figure 8 shows the resulting PSNR at different values of the parameter delta. Bit error rate at different values of Δ and different JPEG quality factors is shown in Fig. 9.

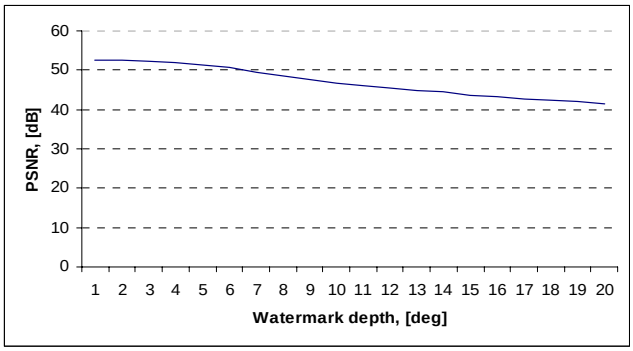

Fig. 8. PSNR results at different Δ

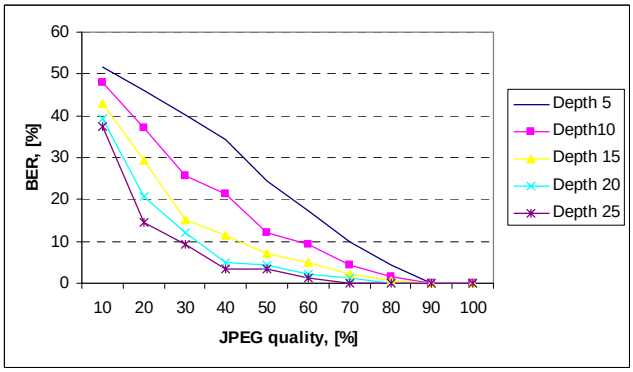

Fig. 9. BER versus JPEG quality

IV. Conclusion

In this paper, we present a new digital watermarking algorithm based on modifying the phase component of the selected coefficients. There is a lot of work to be done, but the test results indicate that using image phase information can lead us to designing very robust watermarks. In our algorithm we emphasize on achievement of low computational complexity, thus making it possible to perform real-time watermark embedding and detection.

Future work will concentrate in applying the phase alteration in more than one coefficient and at different phase steps, thus improving the amount of bits to be embedded in the image. In addition, novel techniques will be devised to make it possible to detect a watermark without requiring the original unmarked image.

There is a need of making an extended research on the properties of CHT transform. Finding algorithms for fast complex Hadamard transform is extremely important in order to lower the computational complexity, which will allow us to use CHT in pyramidal image decomposition. A pyramidal image decomposition using CHT will make it possible to embed different watermarks in each layer of the pyramid achieving the multilayer watermark property [6].

Another important research, that will be made, is the resistance of the watermark against various attacks – geometric transforms, filtering etc. In addition, a research on watermaking color images using the described algorithm will be made.

References

[1] S. Rahardja, B. Falkowski, Family of Unified Hadamard Transforms, IEE Transactions on circuits and systems-II: Analog and Digital Signal Processing, Vol. 46, No. 8, August 1999

[2] S. Rahardja, B. Falkowski, Complex Hadamard Transforms: Properties, Relations and Architecture, IECIE Trans. Fundamentals, Vol. E87-A, No. 8, August 2004

[3] S. Rahardja, B. Falkowski, Complex Composite Spectra of Unified Complex Hadamard Transform for Logic Functions, IEEE Transactions on circuits and systems-II: Analog and Digital Signal Processing, Vol. 47, NO. 11, November 2000

[4] M. D. Swanson, M. Kobayashki, and A. H. Tewfik, Multimedia data embedding and watermaking technologies, Proceedings of IEEE, vol. 86, no. 6, pp. 1064-1087, June 1998

[5] P. W. Wong, E. J. Delp, Security and Watermarking of Multimedia Contents, The International Society for Optical Engineering, San Jose, California, USA, 1999.

[6] R. Kountchev, M. Milanova, C. Ford, S. Rubin. Multimedia Watermarking with Complex Hadamard Transform in the Inverse Pyramid Decomposition. Proc. of the 2003 IEEE Intern. Conf. on Information Reuse and Integration, Las Vegas, USA, October 2003,pp.305-310