A Robust Multiwatermarking Scheme for Multiple Digital Input Images in DWT Domain

Mahdi Babaei
Faculty of Information & Communication Technology, Limkokwing University of Creative Technology, Malaysia
Email: mahdi.babaei {at} limkokwing.edu.my

Kok-Why Ng
Faculty of Computing and Informatics, Multimedia University, Malaysia

HosseinReza Babaei
Faculty of Information & Communication Technology, Limkokwing University of Creative Technology, Malaysia

Hamid Ghorbani Niknajeh
Faculty of Computing and Informatics, Multimedia University, Malaysia

Abstract—**Digital Watermarking is an encryption technique that protects the ownership of multimedia using algorithms. It has opened a new domain in multimedia security and protection against attacks. In this paper, an experiment is conducted using four inputs images. In order to propose a Multi-Watermarking method using four inputs we have applied an inductive computation that improved the quality of output image from one side; and robustness of trademarks which are extracted from the process on the other side. The process contains four two dimensional trademarks which will be converted and combined into a three dimensional sequence. The next phase is to use sub-digital images in Discrete Wavelet Transform domain and decompose them into non-overlapping blocks and finding the block which contains the most densely packed information pertaining to texture (based on the size of the binary image). The latest stage is to embed the final Multi-Watermark before adjusting the selected block pixels. This will be based on some discrete operation rules, which will later be discussed. The results will be compared to currently available three-input methods.**

Keywords - Digital Watermarking; Wavelet Transform; Gaussian; Image filtering.

I. INTRODUCTION

The rapid development of communication technology and the prevalence of Internet as a worldwide network have facilitated the accessibility to information and media. With the advent of Multimedia-based information technologies, transmission and information sharing among social communities are made possible via audio, music and digitized videos. Since there was a huge demand on information protection and publishing copyright in the market, the information concealment techniques became very popular. It can be divided into various categories. Steganography[2,3] and digital Watermarking[4] are two main categories which are currently available in the market. The art and science of concealing information enable certain information to go undetected called Steganography [1].

The Digital Watermarking is a technique to secure digital contents by combining the original digital image and a watermark [5]. It would be possible to transmit the watermarked image and extract it on receiver side. Watermark images comprise of visible and invisible images. It can be invisible when the range of application is wide. The business logos for most small-sizes businesses use the visible watermark images to ensure copyright protection. In this process, the watermarked images will appear similar to the original images while having one or more hidden watermark images which can be extracted.

The main usage of Watermarking is for identification, content authentication and copyright protection. Such processes require a robust watermark algorithm toward various attacks[6]. Those attacks are mainly related to transformations such as translation, scaling and rotation. The Watermarking techniques against those kinds of attacks can be categorized into Blind and Non-Blind Watermarking. The Blind [7]Watermarking is when the original image is not needed for watermark recognition, and the non-blind is where the original image is needed.

The limitations of Spatial domain-based methods such as [8] or [9] (both Steganography and Watermarking applications), have not made them a favorable choice for a robust Multi-Watermarking technique. They depend a lot on earlier techniques, like cryptography and encryption, whereby their lower capacity and reduced robustness in affining maps and distorting signal processing in the majority of the spatial domain based scheme.

One of the main limitations of the Discrete Fourier transform (DFT) and Discrete Cosine Transform (DCT) [10] is their limit in the amount of tampering and attacks they can withstand. The low capacity of hidden data that Wavelet schemes in [11] and [12] which it can sustain is considered the most important constraint under these methods. In addition, the scheme also lacks robustness with respect to geometric attacks.

In addition to the above lines, all information hiding in the DWT, DCT, and DFT of the carrier images consist of a number of computation and information coding. In order to have good quality stereo images, these methods use the mid to low frequency to embed the hidden data. As a result, it imposes a tradeoff between the size of the hidden data and the quality of the resulting watermarked images. In general, this is another constraint for some of available Watermarking Schemes, aside from their robustness limitation to geometric attacks.

II. LITERATURE REVIEW

A. General Algorithms

The Watermark is an authentication method based on logo(as company or person letterhead), name or even stamp containing lines and texts to show that a certain document has been certified by an authorized person [13]. Transforming from traditional to the digital way has revolutionized Information security techniques which are heavily based on digital technology. This technology embedded into different types of media such as audio, video and photos. The major attempt is to hide a security code quietly in the media and this can be extracted (or recovered) on the receiver side.

In general a digital watermark system consists of two major parts [5]:

I. Embedding the watermark and secret key into the cover image which is basically the original image (Figure1).

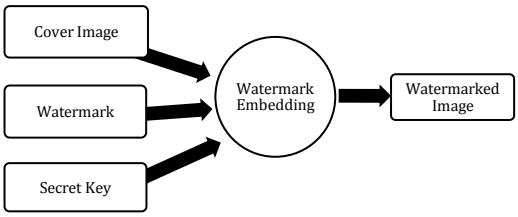

Figure 1-General way to embed watermark

II. The second step is to detect and extract the watermark image with the given secret key and watermarked image in hand. This part executes on the received side after data transmission (Figure2).

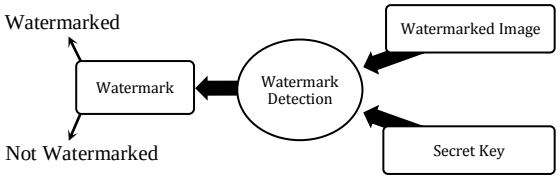

Figure 2-Watermark Detection and Recognition

B. Previous Works

According to [14] the two major categories for digital Watermarking techniques are as follows:

I. Pseudo-Random Gaussian Sequence: This type of Watermarking is more useful when there is a need for objective detection. It is using 1 and -1 to show the watermark.

II. Binary Image or Grey Scale Image Watermarks: This type of watermark is more useful when there is a need for subjective detection. The logo images can turn into a binary or grayscale watermark and used for Watermarking scheme.

Furthermore, an image can be represented in two different domains:

I. Spatial domain: The image is characterized and shown in shape of frequencies.

II. Transform domain: The image represents by pixels. The segmentation of image would be applied based on frequencies. There are several algorithms in this type of Watermarking and the popular ones are shown below:

A) Discrete Cosine Transform (DCT): DCT is a simple image processing procedure. It is fast in transformation and the real output is saved into JPEG. There are two disadvantages with this type of Watermarking: 1.) although they are more robust in comparison to with the Spatial Domain algorithms, they are less effective and secure against simple types of geometric attacks like rotation. 2.) Their weakness extends even to image scaling. These types of techniques can withstand face very simple attacks like pixel brightness or contrast modification and readjustment or blurring. They are not easy to implement and the calculation and infrastructures needed for this type of Watermarking have higher prices compared to others. In fact, they are not much resource efficient. There are two types of DCT Watermarking available: a) Global DCT Watermarking b) Block based DCT Watermarking.

B) Discrete Wavelet Transform (DWT): The main application of this tool is to make multi-resolution decomposition available for both spatial and frequency. The general idea of DWT for Image Data hiding and Watermarking is to split the cover image and decompose it into four sub- graph quarters [15]. In Figure3, HL1, HH1 and LH1 show the best scale wavelet coefficients where the LL1 is the coarse level coefficients. HL1, HH1 and LH1 are the detail sub-images where LL1is considered as the approximation sub-image. It is also possible for LL1 to be decomposed further into HL2, LH2, HH2, and LL2. The process of decomposition continues until the final scale is reached.

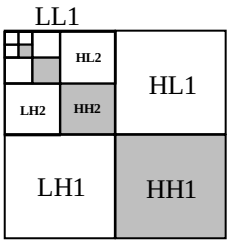

Figure 3- DWT image segmentation

In low frequency image, the stability is enhanced unlike the image processing attack of all other sub-images acquired in Discrete Wavelet Transform. In other words, the decomposition consists of one low frequency zone (at least) and three high frequency sub-graphs. In DWT, each of three high frequency zones shows information about image's edge, image's texture and finally image contour. In this type of Watermarking, the energy of the image is mostly in low frequency. The higher robustness can be achieved through low frequency coefficients.

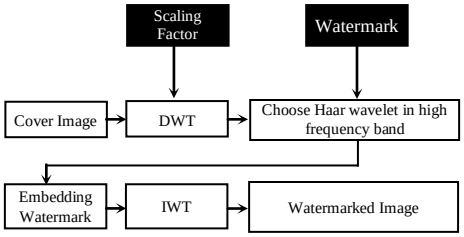

Figure 4-DWT Watermarking

C) Discrete Fourier Transform (DFT): DFT Watermarking had been proposed because of its robustness in facing attacks like rotation, scaling or cropping, which are generally Known as geometric attacks. It is also very effective when faced by frequent attacks. In each Fourier equation, coefficients can be split into two components: 1) Phase and 2) Magnitude. Because of the two components, DFT is considered as complex valued. The complex output of this technique is one of its disadvantages. The strongest part of a DFT is its centered components with low frequency. Based on the experiments, geometric attacks do not change the amount of Phase coefficient. Therefore, this type of Watermarking techniques can bring robustness against translation, rotation, and scaling attacks.

III. PROPOSED SOLUTION

The idea of developing a robust DWT multi-Watermarking scheme was released in 2012 by Y. Zhou and W. Jin[15]. This technique proved that the DWT-domain algorithm is robust, time efficient and reliable against attacks. The limitation of the developed model is the number of watermark images are only three. We set the research goal to improve their techniques and to see the effect of increasing the number of watermark images in final result.

The hypothesis would be the same as [15] but using different number of watermark images. In this paper, we apply the same strategy using four images in order to compare the results and find out the capability of the algorithm in inductive calculations. In case if we use the results analysis for inductive calculus, we would have K number of algorithms with the same steps but with different outputs. The correctness of the first two members shows that it would be possible to prove that this strategy may work for any number of the same algorithm. Let's say:

- K is *True* for the robust DWT algorithm using three input watermark images resulting in a correct output.
- K+1 is *True* for the same robust DWT algorithm as K using four input watermark images and to check for correctness.

We can conclude that:

K + n is *True* for any number of input watermark images. (n is an integer starts from 3)

The proposed method using four watermarks and the six steps in this algorithm are shown as Figure5.

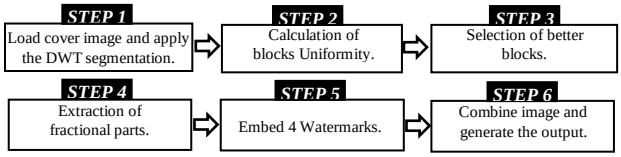

Figure 5- Proposed Solution Steps

A. Watermarking

Step 1

The M x M-size image is imported into the application. As this image is in grayscale, the value of each pixel will be ranged from zero to 255. Based on the basic idea of DWT technique, we split the cover image into quarters. The L-level approximation will be applied on the image and we may say the size of each sub-image would be $M/2^L$ x $M/2^L$.

$$Cover\ image\ size: M \times M \rightarrow F = \{0 \le f(i,j) \le 255\}$$

$$Image\ F_L\ size: M/2^L \times M/2^L$$

M is size in pixel

F is the original grayscale image

$f(i,j)$ *denotes original image dimentions*

L is approximation level

The size for each watermark image (in our scenario four images) would be n x n and it will be an integer multiple of cover image. We may change the multiple 2D watermark images into a 3D using the conditions below:

Watermark image dimension:

$$n \times n \to M / n = r \ (r = \text{int AND } r > 1)$$

$$k\ xw_{T(i,j)} = w_T(\text{i, j, 1 : k}) = w_T(\text{i, j, z}) 1 \le z \le k \qquad (1)$$

Step 2

The cover image has split into smaller images, which are called the sub-images. Each of them needs to be totally separated and there should not be any share pixels existing between them. In this case, the images are called as non-overlapping sub-images.

In next step, we proceed to calculate the uniformity of each non-overlap sub image (block) using the equation below:

$$\textit{Block uniformity}: \ d\ (\mathrm{B}_K) = \frac{1}{n^2} x \sum_{(i,j)\in B_K} \frac{\left| f(i,j) - m_k \right|}{m_k^{1+\alpha}} \qquad (2)$$

B_k *is* $n \times n$ *size block*

m_k *is the average value of Block*

α *is weight correction* (0.6～0.7)

The meaning of block uniformity in here is the uniqueness and visual capacity of an image block. It means that a block with higher number of uniformity will have larger visual capacity. On the contrary, a block with lower visual capacity will be shorter in uniformity magnitude. The reason we take this step is to calculate the visual capacity of blocks in order to be used in next step.

Step 3

The next is to select the blocks with large uniformity number. The selected blocks will be named as BF_L^s. The "S" refers to a non-negative integer which denotes the number of block(s=1, 2,…, S). In addition to that each block has to satisfy a certain criteria to be selected. The requirement of selecting a block is the equality of pixel number of that particular image block and the binary watermark image that will be embedded. So we will have:

BF_L^s : selected block number

The sum of pixel number in the selected blocks is equal to the embedded pixel number in watermarks.

Step 4

The fractional part of each pixel value will be extracted from the selected clocks BF_L^s in this step. At this point, the function floor(x) will be round off element x to the next integer towards minus infinity. Applying the formula below will give us the result of true pixels without fraction. Therefore, we have:

$$\mathrm{BF_L^S} : \mathrm{DBF_L^S}(\text{i, j}) = \mathrm{BF_L^S}(\text{i, j}) - \text{floor}(\mathrm{BF_L^S}(\text{i, j})) \qquad (3)$$

Floor(x):round to nearest integer toward minus

Step 5

In this step, the binary watermark image will be rooted into a selected image field. The value for $DBF_L^s(i,j)$ which denotes the value of that particular pixel minus its fractional part will be modified based on an algorithm shown below. In this algorithm, we have:

Lg: logical table which is returned by the application.

Dec(x): Conversion of a Binary vector to Decimal integer

In this algorithm, the condition will be set based on the value of DBF_L^s in that particular pixel. If the value is positive but less than 0.5, the value will be modified to 0.25 and watermarks would be the Lg output. If the value of DBF_L^s is integer and is greater than 0.5, it will be modified to 0.75. In this case, the Lg output will be based on the remainder amount of division of Decimal to two.

If $0 \le DBF_L^s(i,j) \prec 0.5$,

$DBF_L^s(i,j) = 0.25, \lg(i,j) = Dec\left[w_T(i,j,1:k)\right];$

else

$DBF_L^s(i,j) = 0.75;$

if mod $\left[Dec\left(w_T(i,j,1:k)\right), 2\right] = 0$

$\lg(i,j) = Dec\left[w_T(i,j,1:k)\right] + 1;$

else

$\lg(i,j) = Dec\left[w_T(i,j,1:k)\right] - 1;$

end

end

Step 6

In this step, the original integral part will be recombined with the modified fractional part of $DBF_L^s(i,j)$ and outline the new fields $\mathrm{B\,F'^S_L(i,j)}$. The recombination of the pixels will give us the modified image. In fact the replacement of the original old blocks $\mathrm{B\,F^S_L(i,j)}$ with the new blocks $\mathrm{B\,F'^S_L}$ (i,j) will help us to get a up-to-the-minute approximated sub-image F'L. As a final point, the watermarked image is the outcome of a new approximated sub-image F'L and the original detail sub-images with executing L-level inverse wavelet transform. We will have the below formula to explain what will happen in this step:

$$BF'^S_L(i,j) = DBF_L^S(i,j) + \text{floor}(i,j) \qquad (4)$$

B. Watermark Extraction

Based on this hypothesis that the position of watermark image would be known from the potential of that particular approximated sub-image we would have:

Step 1

In the first step of decomposition of watermarked image, we have approximated on the sub-image. In this step, we test and select an image T_F with M×M in the size. In this condition, we would apply a DWT with L-level, and find an approximated sub-image T_FL.

Step 2

In this step, we would split the watermarked image into multiple blocks. It is important to make the approximation of the sub-image T_FL on the way that none of the blocks overlap each other. The size of each block would be n×n and a particular selected block would

be named as $T\_BF_L^s$ (s=1, 2… S). The selection of those certain blocks would be based on the position of the information recorded in the watermark embedded process.

Step 3

After that, the decimal part of each pixel for the blocks will be extracted. This process may happen by subtracting the fractional part from the true value is each pixel of watermarked image. This would help us to reach and extract the watermarks. The formula that we should apply for that would be:

$$T-BF_L^S : \mathrm{T-DB}\,F_L^S = \mathrm{T-B}\,F_L^S(i,j) - floor\left[\mathrm{T-B}\,F_L^S(i,j)\right]$$
$$(\mathrm{s}=1,2,3,\ldots,\mathrm{S}) \qquad (5)$$

Step 4

In final step, we will recover the multi-watermarks. In order to perform the recovery, we need to follow a discrete operation with refer to the fractional value $T\_DBF_L^s$ of the selected blocks and the logical table Lg.

It is worth mentioning that the function Bin (x) denotes the conversion of decimal integer (x) to a binary vector.

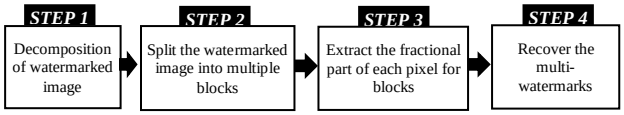

Figure 6- Extraction Steps

IV. RESULTS AND ANALYSIS

An experiment had performed using four base-2 images with the size of 32×32(shown in figure 7), a cover image (figure 8) and the developed application. The final result is a watermarked image which is shown in Figure 8.

Figure 7- Four watermark Images

In this application, the watermark images are named as w_1, w_2, w_3 and w_4. The 8-bit cover image would be a grayscale person image with 512×512 in size. In this simulation, the fourth level of wavelet decomposition and reconstruction is used for the person image.

The ratio of peak signal to noise (PSNR) is a major factor to measure and determine the quality of watermarked image. In this case we will have an error rate in extraction of watermarks. This rate will be evaluated by ρ_b. The definition of these rates would be the formulas below based on[15]:

$$PSNR = 10\times\log_{10}^{\left(\frac{1^2}{MSE}\right)}(dB) \qquad (6)$$

$$\mathrm{MSE} = \sum_{i=1}^{n}\sum_{j=1}^{n}\left(f(i,j)-f^*(i,j)\right)^2 \Big/ N^2 \qquad (7)$$

$$\rho_b = T_{error}/T_b \qquad (8)$$

∴

▹ $f(i,j)$ *and* $f^*(i,j)$ *is the pixel values of the original and watermarked image*

▹ T_b *is the total pixel number of the embedded digital watermark.*

▹ T_{error} *is the total error pixel occurred in extracted watermark.*

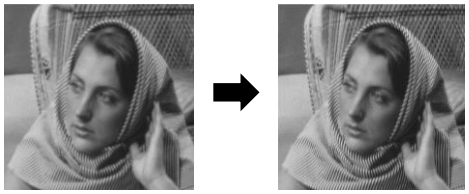

Figure 8- Cover Image and Final Watermarked image (using four watermark images)

The best comparison of results with the previous researches in area would be based on our method in compare to [15]. There are two series of experiments been done using each method and the results show less error rate in extraction and higher quality of watermarked images in proposed method overall.

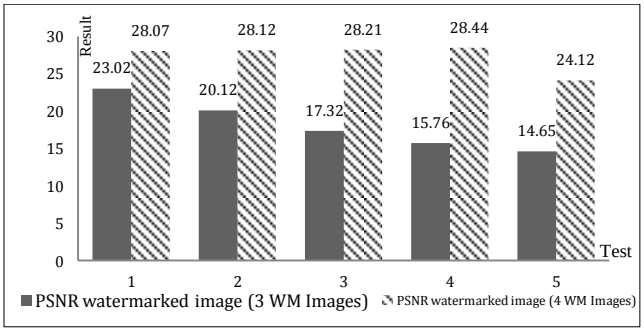

Figure 9 - Quality comparison of Proposed Method Vs. Previous works

PSNR watermarked image	Error extracted logo (3 WM Images)	PSNR watermarked image	Error extracted logo (4 WM Images)
23.02	0	28.07	0.1230
20.12	0.42	28.11	0.1294
17.32	2.34	28.21	0.1201
15.76	5.72	28.44	0.1218
14.65	7.973	24.11	0.1262

Table 1-Watermarked Image Quality comparison

The simulated results indicate that the proposed scheme has ideal imperceptibility and capacity, which are independent of the embedded Watermarking number; especially the scheme can guarantee the embedded multi watermarks. Not only the error rate has reduced but also the quality of watermarked image has increased.

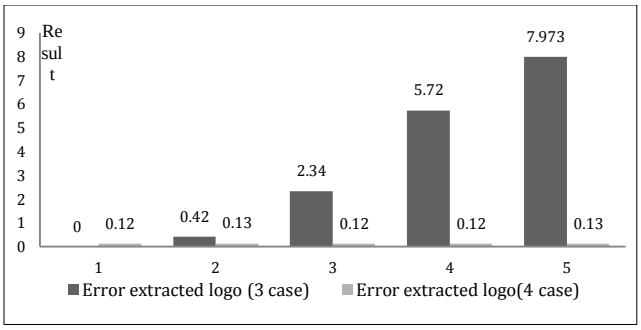

Figure 10-Error rate in extraction of logo comparison

A. Attack testing I- Gaussian Noise

Testing the reliability of the anticipated method alongside Gaussian noise attacks with mean of 0 and variance of 0.01 are applied. The PSNR of the original watermarked image reduces to 28.1168dB from 34.8219dB with an error rate ρ_b of 1.294%. The detailed simulated results under different intensity noise addition are presented in Figure 12, indicating the watermark robustness against noise attack.

B. Attack testing II- Median filter

With the purpose of testing the reliability of proposed method against the other types of attacks, a watermarked woman image filtered by median filter by [7×7] in size window has been tested with low-pass filtering. In this case, there are lot of missing details and high amount of PSNR been reduced in watermarked image from 34.8219 dB to 25.5110dB. Figure 13 shows the detailed simulated results under median filtering with different window size.

C. Attacks testing results and analysis

Figure 12 and 13in below show the result of using Gaussian Noise and median filter.

Gaussian Noise (Variance)	PSNR Watermarked image	Error extracted logo (4 WM Images)
Noise = 0	34.82	0
0.005	28.07	0.1230
0.01	28.11	0.1294
0.02	28.21	0.1201
0.03	28.44	0.1218
0.04	24.11	0.1262

Table 2-Result of Gaussian noise attack testing

Median Filter windows size	PSNR watermarked image	Error extracted logo (4 WM Images)
Without median	34.82	0
5 * 5	22.29	0.1267
7 * 7	25.51	0.1277
9 * 9	28.88	0.1250
11 * 11	27.04	0.1191
13 * 13	26.89	0.1277

Table 3-Result of Median Filter attack testing

D. Comparison of PSNR in Gaussian noise attack

The results of Gaussian noise attack had been shown in Table 4 shows the improvement of PSNR in our algorithm in compare to what had existed before. The results also show an increasing PSNR ratio percentage by increasing Gaussian noise variance.

Gaussian Noise (Variance)	PSNR Watermarked image (3 WM Images)	PSNR Watermarked image (4 WM Images)
0	34.82	34.82
0.005	23.02	28.07
0.01	20.12	28.11
0.02	17.32	28.21
0.03	15.76	28.44
0.04	14.65	24.11

Table 4-Comparison of PSNR in Gaussian noise attack testing using 3 and 4 input watermarks

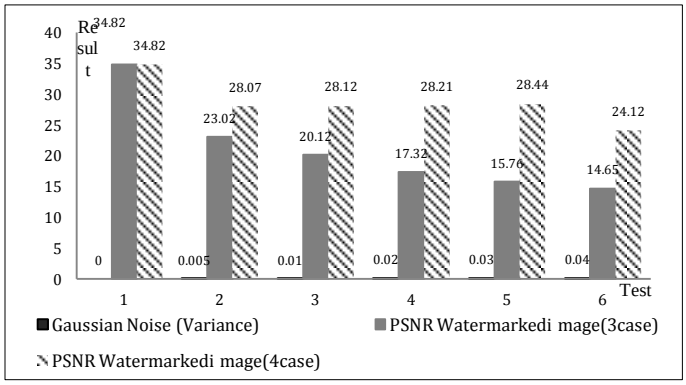

Figure 11-Comparison of PSNR in Gaussian noise attack testing using 3 and 4 input watermarks.

V. CONCLUSION

We have researched on four-binary Watermark input images embedded them together into a grayscale digital image. The system is derived from the novel discrete operation. The application operation and simulation results signify that the anticipated scheme has ideal imperceptibility and capacity, which are not dependent on the embedded Watermarking number, in particular, the scheme is able to undertake the embedded Multi-Watermarks, as well as, the one having protected from all kind of attacks. The results shown in Section IV can clearly certify that the proposed method can generate a robust Multi-Watermarking method in DWT domain and can even certify that the general image processing attacks are not harmful to this Watermarking technique.

The results show that there is an improvement in image quality in compare to [15], and the error rate in watermark extraction is reduced as well. The comparison of the results to earlier studies with three input watermark images shows that the robustness has increased. This result with increment of image quality and error extraction rates has boosted the immunity against the attacks. The low rate of error and high

quality in reducing the attacks show that this can perform better than what had existed before.

Based on what we have for the four input images, we can say that the results are well accepted. The truthfulness of K=4 watermark images and the previous works in this field (using K=3) can certify the hypothesis that this algorithm can effectively work for K=n (n is a non-negative integer). It seems that adding the number of input watermark images will reduce the error rate and increase the accuracy of the algorithm.

As for future work, it can further be improved on its accuracy by using higher number of watermarks. However, this will consume a lot of processing power.

REFERENCES

[1] F. A. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding-a survey," *Proceedings of the IEEE,* vol. 87, pp. 1062-1078, 1999.

[2] D. Artz, "Digital steganography: hiding data within data," *internet computing, IEEE,* vol. 5, pp. 75-80, 2001.

[3] A. Martin, G. Sapiro, and G. Seroussi, "Is image steganography natural?," *Image Processing, IEEE Transactions on,* vol. 14, pp. 2040-2050, 2005.

[4] I. Cox, M. Miller, J. Bloom, and M. Miller, *Digital watermarking*: Morgan Kaufmann, 2001.

[5] M. Abdullatif, A. M. Zeki, J. Chebil, and T. S. Gunawan, "Properties of Digital Image Watermarking."

[6] S. Elshoura and D. Megherbi, "Analysis of Noise Sensitivity of Tchebichef and Zernike Moments with Application to Image Watermarking," *Journal of Visual Communication and Image Representation,* 2013.

[7] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, *Digital watermarking and steganography*: Morgan Kaufmann, 2007.

[8] C.-H. Yang, C.-Y. Weng, S.-J. Wang, and H.-M. Sun, "Adaptive data hiding in edge areas of images with spatial LSB domain systems," *Information Forensics and Security, IEEE Transactions on,* vol. 3, pp. 488-497, 2008.

[9] W.-L. Tai, C.-M. Yeh, and C.-C. Chang, "Reversible data hiding based on histogram modification of pixel differences," *Circuits and Systems for Video Technology, IEEE Transactions on,* vol. 19, pp. 906-910, 2009.

[10] K. Solanki, O. Dabeer, U. Madhow, B. Manjunath, and S. Chandrasekaran, "Robust image-adaptive data hiding: Modeling, source coding and channel coding," in *Proceedings of the Annual Allerton Conference on Communication Control and Computing*, 2003, pp. 829-838.

[11] J. Xie, C. Yang, and D. Huang, "High Capacity Information Hiding Algorithm for DCT Domain of Image," in *Intelligent Information Hiding and Multimedia Signal Processing, 2008. IIHMSP'08 International Conference on*, 2008, pp. 269-272.

[12] D. Zou, Y. Q. Shi, Z. Ni, and W. Su, "A semi-fragile lossless digital watermarking scheme based on integer wavelet transform," *Circuits and Systems for Video Technology, IEEE Transactions on,* vol. 16, pp. 1294-1300, 2006.

[13] S.Paul. "*What is Digital Watermarking?"* Available: http://www.legalzoom.com, 2007

[14] V. M. Potdar, S. Han, and E. Chang, "A survey of digital image watermarking techniques," in *Industrial Informatics, 2005. INDIN'05. 2005 3rd IEEE International Conference on*, 2005, pp. 709-716.

[15] Y. Zhou and W. Jin, "A robust digital image multi-watermarking scheme in the DWT domain," in *Systems and Informatics (ICSAI), 2012 International Conference on*, 2012, pp. 1851-1854.