Robust Logo Watermarking Based on Wavelet Transform Modulus Maxima

Mohammad Barr
School of Engineering & Sustainable Development
De Montfort University
Leicester, UK
mohammad.barr@my365.dmu.ac.uk

Dr. Cristian Serdean
School of Engineering & Sustainable Development
De Montfort University
Leicester, UK
cvs@dmu.ac.uk

***Abstract*— In this paper, a novel blind logo image watermarking technique is presented which can be used to protect the copyright of digital images. Our technique uses two different watermarks. One is a high capacity multi-bit watermark used to embed a logo and the other is a low capacity single-bit watermark used for the detection of geometrical attacks. Both watermarks are embedded into the red, green, and blue components of an RGB image, weighted based on human visual system considerations. Each non-overlapping watermark is embedded using a spread spectrum approach, based on a pseudo-random noise (PN) sequence and a unique secret key. Robustness against geometric attacks is achieved with the help of wavelet transform modulus maxima, which is shift invariant, and by embedding it in different sub-bands of the wavelet transform. The experimental results show that our proposed watermarking scheme is robust to geometric attacks such as rotation, scaling, and translation and compares favourably against existing techniques.**

Keywords—Discrete Wavelet Transform; wavelet transform modulus maxima; watermark embedding; watermark detection; watermarking

I. INTRODUCTION

Nowadays, digital multimedia content (in particular, image data) is widely available and is frequently distributed over the Internet. Copyright protection of such content is important to ensure its rightful ownership and legal distribution. Thus, storing the ownership information along with the digital data has emerged as an active area of research.

Digital Watermarking is a tool which enables the hiding or embedding of a signal (usually containing ownership information) into another signal (usually image or video content) in a robust fashion. It is used to protect digital data against copyright infringement [1]. Important applications of watermarking include broadcast monitoring, owner identification, proof of ownership, authentication, fingerprinting, copy control, and covert communication [2].

An important problem related to watermarking is that it is not sufficient just to store the ownership information but also to hide it and separate it from the real data and to protect it against tampering. It is to be noted that watermarking is different from encryption. While, they both provide protection of the data, encryption only provides protection during transmission. The data is no longer protected once it is decrypted. On the other hand, a watermark is always present in the data [3].

A watermark exhibits several important characteristics. Among others, these include: robustness, tamper resistance, fidelity, and computational cost [2]. Robustness is the characteristic of a watermark that indicates how well the watermark can survive common signal processing operations such as lossy compression. Tamper resistance can be further classified into four types: resistance against active, passive, collusion or forgery attacks. Fidelity refers to the ability of a watermark to embed into another signal without visibly changing that signal. Lastly, computational cost usually determines the computational resources, speed, or time required to embed the watermark or to determine the authenticity of the watermark. An ideal watermark should be robust, tamper resistant, have high fidelity, and a small computational cost. Achieving these conflicting requirements simultaneously is rarely possible in practice and usually requires a trade-off between one or more of these characteristics.

To address the above considerations, many different methods have been proposed in the literature. Most techniques tend to focus on watermarking grey level images. In this paper we focus on embedding the watermarks in the RGB domain, which in comparison has been far less used in image watermarking. A novel wavelet transform based robust watermarking scheme is proposed, that embeds two orthogonal watermarks, both in the wavelet domain. Our scheme makes use of the properties of the wavelet transform modulus maxima (WTMM) [8, 9, 10] to provide robustness against geometric attacks and protect the embedded logo.

The rest of the paper contains the following sections. In Section II, a brief literature survey of relevant robust watermarking methods is presented. These include both spatial and transform domain techniques. Moreover, popular spread spectrum techniques have also been reviewed and the differences between the existing spread spectrum techniques and the proposed technique have been highlighted. In Section III, the proposed novel robust logo watermarking technique is presented. The experimental results of the proposed method are

978-1-5386-0821-0/17/$31.00 ©2017 IEEE

discussed in Section IV. Finally, conclusions are presented in Section V.

II. LITERATURE REVIEW

In this section, a review of the popular watermarking schemes is presented. In order to better understand the schemes, they have been divided into two broad categories of spatial domain and transform domain techniques. While spatial domain techniques are simple to implement, they are not as robust as the more complex transform domain techniques. Several transforms have been used over the years for watermarking, each offering a different set of strengths and weaknesses. Commonly used transforms include Fourier transform (FT), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) etc. Among these, due to its many advantages, the DWT has emerged as the transform of choice for many researchers. Hence, in this section we focus on DWT based watermarking schemes.

Chou and Liu [4] used the discrete wavelet transform to embed a watermark in colour images that satisfies two conflicting characteristics of a watermark i.e., transparency and robustness. Their proposed watermarking scheme enables creation of watermarks that are transparent and robust against various attacks such as cropping, low-pass filtering, scaling, median filtering, the addition of white noise, and JPEG and JPEG2000 compressions at high compression ratios. The idea is to embed watermark as perceptually redundant information. A drawback of this method is that it is not completely blind i.e., though it can work without requiring the original image to be present, but it requires a small amount of information including the locations of qualified coefficients and the data associated with coefficient quantization is needed for watermark extraction.

Kumar et al. [5] combined DWT with rough set theorem and singular value decomposition (SVD) for efficient watermarking of grey scale images. SVD was used to make the watermarking scheme robust while rough set theorem was used to enhance the perceptual quality of the watermark. The problem with this method is that its robustness to rotation is limited. Moreover, this method only addresses the problem of watermarking of grey scale images and it is computationally complex.

Hu, Shao, and Ma [6] exploit the human visual system (HVS) and DWT in their proposed watermarking scheme. They first scramble the watermark using a logistic map. The scrambled watermark is then embedded into the DWT coefficients. To improve the robustness and transparency of the watermark, the authors expand the contrast sensitivity function (CSF) to the spatial frequency plane to determine the perceptual weight of the embedding strength in the DWT sub-bands. The experimental results show that the proposed method not only results in a high quality watermarked image but is also resistant to compression, filtering, noise (Gaussian and Salt & Pepper), enhancement, and geometric attacks. However, the results have only been demonstrated using a grey scale host image and a binary watermarked image. It is not clear how the algorithm will perform in the case of coloured images.

Another watermarking scheme was recently introduced by Maqbol et al. [7]. In this scheme, they employ both singular value decomposition (SVD) and DWT. They also take into consideration the human visual system and test the robustness of their scheme against rotation, scaling, and translation attacks. However, this scheme only targets watermarking of grey scale images. Moreover, the experimental results presented for this scheme are not very encouraging.

Hence, to address the problem of robust watermarking of colour images, we introduce a novel method which uses the shift-invariant WTMM [9] as a tool against geometric attacks. The proposed logo image watermarking scheme is presented in the next section and operates on RGB images.

III. PROPOSED METHOD

A. Watermark Embedding

Our proposed watermark embedding technique is shown in Fig. 1. Its main features are the embedding of two different watermarks in different DWT sub-bands of the same host image and the use of the shift invariant wavelet transform modulus maxima for achieving robustness against geometric attacks. The first watermark is a robust 1-bit watermark which is embedded in the Low-High (LH) and High-Low (HL) sub bands of the DWT of the original image while the second watermark is a high capacity multi-bit watermark (a logo image) which is embedded in the High-High (HH) sub bands of the DWT of the watermarked image already containing the 1-bit watermark.

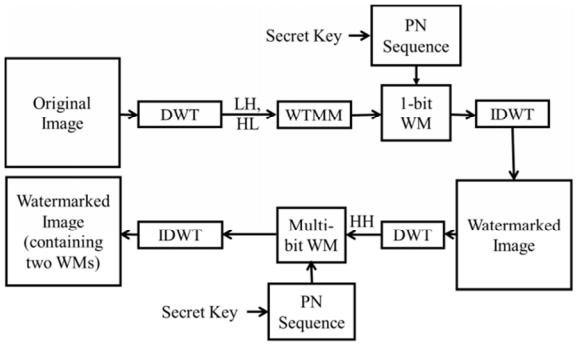

Figure 1 The overall watermark embedding process

As shown in Fig. 1, the overall embedding process includes computing the DWT of the original image first, as in [8]. Then, the LH and HL sub bands are extracted from the DWT of the original image. The magnitude function ($Mf(u,2^j)$) and the angle function ($Af(u,2^j)$) of WTMM are then calculated from the extracted LH and HL sub bands using Eq. (1) and Eq. (2) respectively.

$$Mf(u,2^j) = \sqrt{|W^1 f(u,2^j)|^2 + |W^2 f(u,2^j)|^2} \quad (1)$$

$$Af(u,2^j) = \begin{cases} \alpha(u), & if\ W^1 f(u,2^j) \geq 0 \\ \pi + \alpha(u), & if\ W^1 f(u,2^j) < 0 \end{cases} \quad (2)$$

Here,

$$\alpha(u) = tan^{-1}\left(\frac{W^2 f(u,2^j)}{W^1 f(u,2^j)}\right) \quad (3)$$

The details about the functions $W^1 f(u, 2^j)$ and $W^2 f(u, 2^j)$ and the calculation of the WTMM can be found in [8-10]. A 1-bit watermark is embedded in the WTMM coefficients using a PN sequence generated based on a secret key. The chip rate and by implication the robustness of the watermark is maximised by embedding just one single bit of data. The logo (i.e. the multi-bit watermark) is then embedded in the HH sub-band, again based on a PN sequence generated by a second secret key. The overall watermarked image contains two orthogonal watermarks (both the 1-bit and the multi-bit watermarks) embedded in different sub-bands and used for different purposes.

The motivation behind using two different watermarks is that the 1-bit watermark can be used to determine if the watermarked image has been attacked using any geometric attack. While spread-spectrum techniques possess many appealing properties [2], their main disadvantage is their sensitivity to any geometric attack that leads to 'desynchronization' between the resulting image and the generated PN sequence. We therefore rely on the shift invariance property of the WTMM to embed a robust 1-bit watermark which is solely as an attack detection mechanism, allowing us to undo the geometric transformation and 'resynchronise' the image. If the 1-bit watermark cannot be instantly recovered, this signals the presence of a geometric attack. In such a case, the geometric attack is first identified and then undone, allowing us to then recover the multi-bit logo (watermark).

The multi-bit and 1-bit watermark embedding processes are illustrated in more detail in Fig. 2 and Fig. 3 respectively.

As it can be observed in Fig. 2 and Fig. 3, the DWT is applied separately to each of the red, green, and blue components of an image. It is worth noting that by embedding the watermark into the RGB domain, the effective chip rate of the system is trebled.

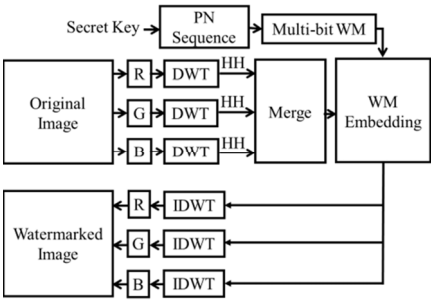

Fig. 2. The multi-bit watermark embedding process

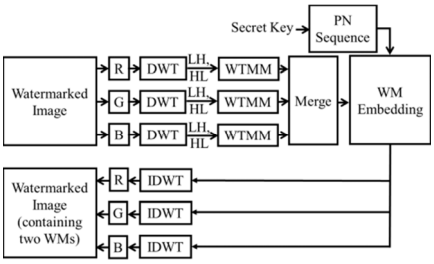

Fig. 3. The 1-bit watermark embedding process

B. *Watermark Recovery*

The overall watermark recovery process is shown in Fig. 4.

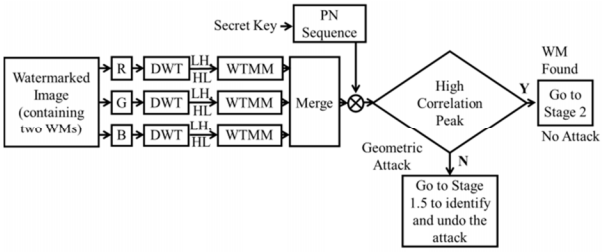

Fig. 4. Watermark recovery process

In the recovery process, the watermarked image (containing both the 1-bit and the multi-bit watermarks) is first split into its respective red, green, and blue components. The DWT of each colour component is then computed. The WTMM of the LH and HL sub bands is then obtained based on Eq. (1 – 3). Watermark detection is achieved by cross-correlation of the WTMM coefficients with the PN sequence generated locally using the same secret key used during embedding. If the result is a high cross-correlation peak, then this points to the scenario in which no geometric attack has taken place and the logo watermark can be safely recovered during Stage 2 as shown in Fig. 5.

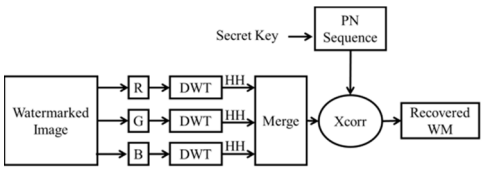

Fig. 5. Watermark recovery Stage 2.

It should be noted that in Stage 2, the multi-bit watermark is blindly recovered via cross-correlation from the HH sub-bands of the red, green, and blue components of the watermarked image.

On the other hand, if a high cross-correlation peak is not found, then this points to the scenario in which a geometric attack has taken place and the watermark recovery process enters an intermediate stage (Stage 1.5, shown in Fig. 6). During this intermediate stage, the attack is first identified and undone before the multi-bit watermark is finally recovered during Stage 2.

IV. RESULTS AND DISCUSSION

In this section, we present and discuss our experimental results. For the purposes of this paper we used two popular test images: Lenna and Pepper. The resolution of each host image is 512×512 pixels. As, generally, logo images are much smaller in size compared to the host image, a logo image of size 50×20 pixels is used (see Fig. 7). This size is considered

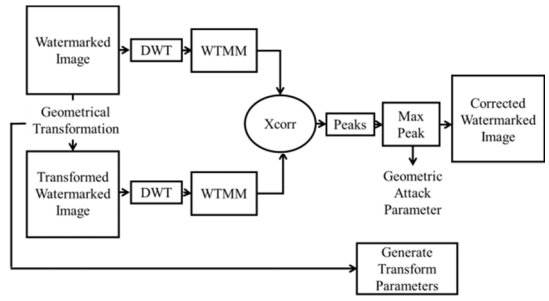

Fig. 6. Watermark recovery Stage 1.5.

sufficient to convey a meaningful enough visual message while ensuring a good trade-off between robustness and watermark capacity. Haar wavelet was used to produce the wavelet coefficients. All the experiments were performed in MATLAB. As a performance evaluation metric, we use the normalized cross-correlation of the original and the attacked image.

Figure 7 – The logo image.

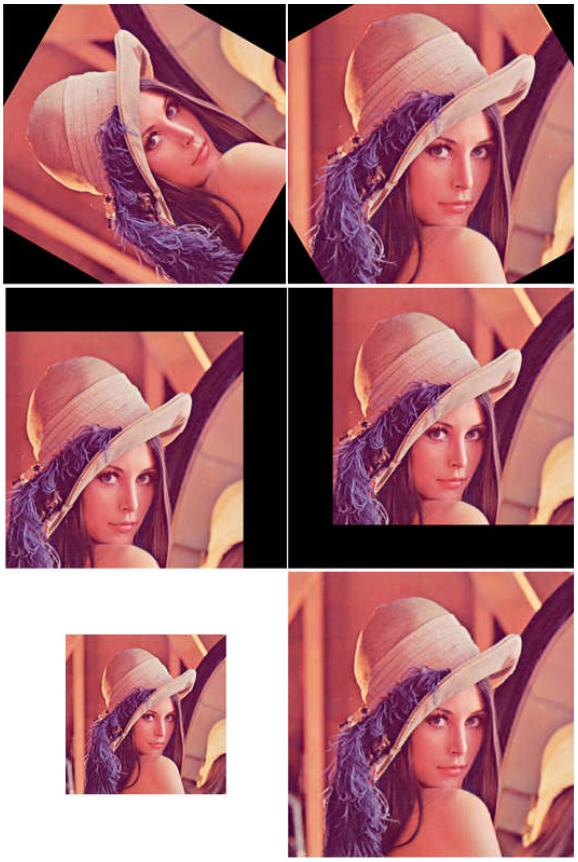

Figure 8 – left column: the Lena image rotated by 60 degrees (top), translated by pixels offset (80, -80) (center), and scaled down by factor 0.5 (bottom); right column: the recovered Lena image after rotation (top), translation (center), and scaling (bottom).

The focus of our experiments was on demonstrating the robustness of our proposed algorithm against geometric attacks. These attacks include rotation, scaling, and translation. For testing robustness against rotation, we rotate the image by different angles from 1 degree to 359 degrees and try to detect and recover the watermark. Similarly, for testing robustness against translation, we shift the image using different pixel offset values and try to detect and recover the watermark in each case. The three examples illustrated in this paper are: $(+10,-10)$, $(+10,-20)$, and $(+30,-40)$. Lastly, to test the robustness of our proposed algorithm against scaling, a similar approach to rotation is taken. In the example provided in this paper we scale down the image by a factor of 0.5 and then try to detect and recover the watermark. Fig. 8 shows some examples of the Lena image undergoing different geometric transformations (rotation, translation, and scaling) and then getting recovered.

To demonstrate the efficiency of our algorithm, we also compare the performance of our proposed algorithm with that of a benchmark watermarking scheme [7].

The results of our proposed method compared to the method described in [7] are shown in Fig. 9 – Fig. 14. Fig. 9 and Fig. 10 show the results of our proposed algorithm compared to [7] with respect to robustness against rotation. These results are derived using the Lena and the Pepper images respectively. From these results, we can see that our proposed algorithm achieves a normalized cross correlation value which is almost twice as that obtained in [7].

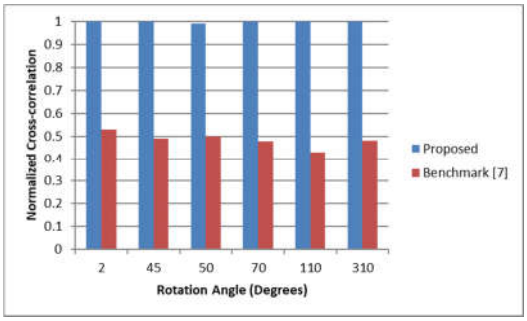

Figure 9 – Comparison of robustness against rotation for the Lena image.

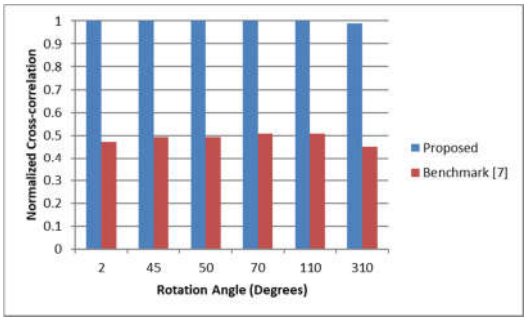

Figure 10 – Comparison of robustness against rotation for the Pepper image.

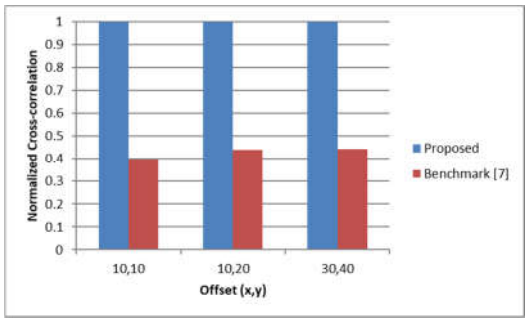

Figure 11 – Comparison of robustness against translation for the Lena image.

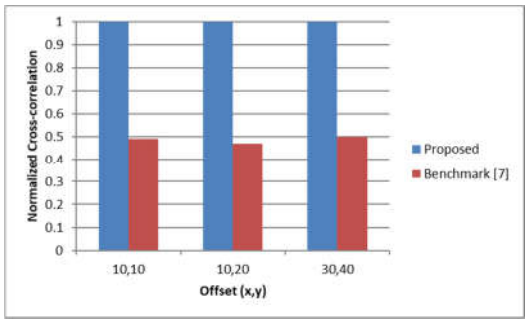

Figure 12 – Comparison of robustness against translation for the Pepper image.

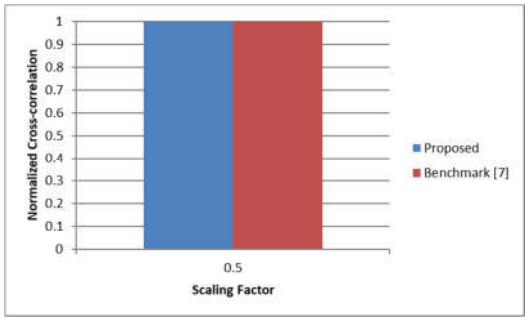

Figure 13 – Comparison of robustness against scaling for the Lena image.

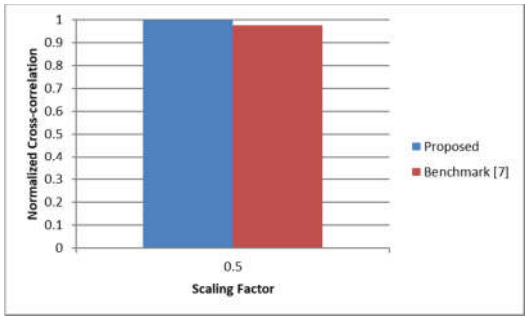

Figure 14 – Comparison of robustness against scaling for the Pepper image.

Fig. 11 and Fig. 12 show the results of our proposed algorithm compared to [7] when the image is shifted by three different offset values. The results are obtained using the Lena and the Pepper images respectively. From these results, we can see that, for both the images, our proposed algorithm again outperforms the one in [7].

Finally, Fig. 13 and Fig. 14 show the results of our proposed algorithm vs [7] when the resolution of the image is scaled down by a factor of 0.5. These results show that our algorithm achieves the same results for Lena but outperforms [7] for Pepper.

Further results for the Barbara and Airplane images are summarised in Table 1. As these results indicate, the proposed algorithm continues to perform very well for these images.

TABLE 1 PERFORMANCE OF THE PROPOSED ALGORITHM FOR AIRPLANE AND BARBARA IMAGES UNDER DIFFERENT ATTACK CONDITIONS

Type of attack	**Image**	
	Airplane	***Barbara***
Rotation (in degrees)	***(NCC)***	***(NCC)***
2	1	1
25	1	1
60	1	0.9944
70	1	1
90	1	1
Translation (offset (x, y) in pixel units)		
16, 16	1	1
24, 24	1	1
80, 80	1	1
Scaling factor		
0.5	1	0.9719
0.9	1	1
1.1	1	0.9944

V. CONCLUSIONS

In this paper, we presented a novel wavelet-based robust logo image watermarking algorithm based on the WTMM, robust to geometric attacks such as rotation, scaling, and translation. The WTMM has been little used for watermarking and in this paper we exploited its shift invariance property that made it popular in applications such as stereo vision and correspondence matching.

The robustness of the proposed scheme has been demonstrated for a variety of rotation angles, scaling factors, and translations offsets and shows very good promise.

The key feature of our proposed algorithm was the embedding of two different watermarks, both embedded in the wavelet domain: a 1-bit watermark used solely for attack

detection purposes, and the main multi-bit watermark for invisibly embedding the logo watermark in RGB images.

ACKNOWLEDGMENT

We would like to thank the Saudi Cultural Bureau and the Saudi government for their generous support for attending this conference.

REFERENCES

[1] A. Reddy and B. Chatterji, "A new wavelet based logo-watermarking scheme," in *Pattern Recognition Letters*, vol. 26, no. 7, pp. 1019 – 1027, 2005.

[2] I. J. Cox, M. L. Miller, and J. A. Bloom, "Watermarking applications and their properties," in *IEEE International Conference on Information Technology: Coding and Computing*, 2000.

[3] G. Bhatnagar, J. Q. Wu, and P. K. Atrey, "Robust logo watermarking using biometrics inspired key generation," in *Expert Systems with Applications*, vol. 41, no. 7, pp. 4563 – 4578, 2014.

[4] C. H. Chou and K. C. Liu, "A Perceptually Tuned Watermarking Scheme for Color Images," in *Image Processing, IEEE Transactions on*, vol.19, no.11, pp. 2966 - 2982, Nov. 2010.

[5] S. Kumar, N. Jain, and S. Fernandes, "Rough set based effective technique of image watermarking," *Journal of Computational Science*, vol. 19, pp. 121-137, 2017.

[6] J. Hu, Y. Shao, W. Ma, and T. Zhang, "A robust watermarking scheme based on the human visual system in the wavelet domain," in *2015 8th International Congress on Image and Signal Processing (CISP),* pp. 799 – 803, 2015.

[7] N. Makbol, B. Khoo, and T. Rassem, "Block-based discrete wavelet transform- singular value decomposition image watermarking scheme using human visual system characteristics," IET Image Processing, vol. 10, no. 1, pp. 34-52, 2016.

[8] S. Mallat. A wavelet tour of signal processing. Academic press, 1999.

[9] A. Bhatti, S. Nahavandi, Y. Frayman, "3D depth estimation for visual inspection using wavelet transform modulus maxima", Journal of Computers and Electrical Engineering, 33(1), pp.48-57, 2007.

[10] A. Bhatti, and S. Nahavandi, "Stereo correspondence estimation based on wavelets and multiwavelets analysis", in Stereo Vision, InTech Education and Publishing, Vienna, Austria, pp.27-48, 2008.