Wavelet Transform Modulus Maxima based Robust Logo Watermarking

Mohammad Barr[1] and Dr. Cristian Serdean[2]

[1]Department of Electrical Engineering, Northern Border University, Arar, Saudi Arabia
[2]School of Engineering and Sustainable Development, De Montfort University, Leicester, UK.
E-mails: m.abarr@nbu.edu.sa, cvs@dmu.ac.uk

Abstract: Digital image watermarking is used to protect the copyright of digital images. In this paper, a novel blind logo image watermarking technique for RGB images is proposed. The proposed technique exploits the error correction capabilities of the Human Visual System (HVS). It embeds two different watermarks in the wavelet/multiwavelet domains. The two watermarks are embedded in different sub-bands, are orthogonal, and serve different purposes. One is a high capacity multi-bit watermark used to embed the logo, and the other is a 1-bit watermark which is used for the detection and reversal of geometrical attacks. The two watermarks are both embedded using a spread spectrum approach, based on a pseudo-random noise (PN) sequence and a unique secret key. Robustness against geometric attacks such as Rotation, Scaling, and Translation (RST) is achieved by embedding the 1-bit watermark in the Wavelet Transform Modulus Maxima (WTMM) coefficients of the wavelet transform. The experimental results show that the proposed watermarking technique has better distortion parameter detection capabilities and compares favourably against existing techniques in terms of robustness against geometrical attacks such as rotation, scaling, and translation.

1. Introduction

Digital watermarking is a valuable technique which enables the hiding or embedding of a signal (usually containing ownership information) into another signal (usually image or video content) [1]. Spread spectrum techniques [2] [3] and wavelet transforms have proved to be very popular in watermarking in spite of their susceptibility to 'desynchronization' attacks and respectively the lack of shift invariance of the conventional wavelet transforms. Various techniques have been used over time to address these issues and provide robustness to geometrical and other desynchronization-type attacks [4] [5]. One technique that addresses the afore mentioned limitation of the wavelet (and multiwavelet) transforms [6], is to make use of the Dual-Tree Complex Wavelet Transform (DTCWT) [7]. In the context of watermarking, DTWCT has several useful features such as approximate shift invariance, low computational complexity, perfect reconstruction, and directional sensitivity [8]. However, watermarking schemes based on DTCWT usually have low embedding capacity [9]. Another possible technique to address this limitation and which avoids the need to rely on a Complex transform, is to make use of the Wavelet Transform Modulus Maxima (WTMM) coefficients of the wavelet transform. The maxima values of the wavelet transform, aka the WTMM [10], [11], provide interesting insights about an image. For example, they represent edge related information in an image but unlike the standard DWT (Discrete Wavelet Transform) coefficients which are not translation invariant, the WTMM coefficients are translation invariant. This valuable property is exploited in this paper to fight against geometrical attacks on watermarks. WTMM has been little used so far in digital watermarking. For example, Zhu and Zhu [12], Alghouniemy and Tewfik [13] and Luo, Xing, and Shi [14] are amongst the few authors that employed WTMM in watermarking. It is worth noting that although WTMM has been very little used in digital watermarking, it has been used quite extensively especially for image fusion, in the field of medical imaging [15], [16] and for stereo correspondence matching in stereo vision applications, where it has shown very good promise. The use of DTCWT for watermarking has been first investigated by Loo and Kingsbury [17], [18]. Various techniques have been proposed since then to increase invisibility and robustness and to address the lower capacity of the DTCWT [8], [9], [19], although beyond cropping and translation, most of these techniques tend to offer limited robustness to other specific geometrical transformations. Other watermarking techniques designed to provide robustness to geometrical attacks based on shift invariance transform properties, include O'Ruanaidh & Pun's [20] Fourier-Mellin transform (FMT) based watermarking technique. However, the FMT is computationally complex and due to the need to preserve FFT symmetry, offers a low watermark capacity.

Amongst other techniques, DWT and Singular Value Decomposition were used together with Scale Invariant Features Transform (SIFT) by Ye et al. [21]. Similarly, Fazli & Moeini's Discrete Cosine Transform (DCT), SVD, and DWT based watermarking scheme [22] is another efficient technique. However, they do not take into consideration HVS during watermark embedding, and hence, their method has low capacity. Li et al. [23] also used DWT and SVD with Zernike moments in their watermarking scheme. However, like the scheme in [21], their scheme also has disadvantages such as inaccuracy, high computational complexity, and numerical instability at higher order of moments.

The main aim of this work is to propose a novel blind logo watermarking technique for RGB images, which is robust to geometrical transforms. The proposed technique exploits the error correction capabilities of the Human Visual System (HVS). It embeds two different watermarks in the wavelet and respectively multiwavelet domains.

The two watermarks are embedded in different sub-bands, are orthogonal, and serve very different purposes. One is a high capacity multi-bit watermark used to embed the logo, and the other is a 1-bit watermark which is used for the detection and reversal of geometrical attacks. The two

[1]Mohammad Barr was with De Montfort University, Leicester, UK and is now with Northern Border University, Arar, Saudi Arabia.

watermarks are both embedded using a spread spectrum approach, based on a pseudo-random noise (PN) sequence and a unique secret key. Robustness against geometric attacks such as Rotation, Scaling, and Translation (RST) is achieved by embedding the 1-bit watermark in the WTMM coefficients of the wavelet transform. The proposed scheme also looks at how the HVS can be taken into account and adaptively used for RGB images. For example, the human eye has different levels of sensitivity for different colour components and different frequencies [24]. This fact is exploited by embedding watermarks of different strengths in each color component according to the sensitivity level of the eye to a particular colour component.

The experimental results show that the proposed watermarking technique has better distortion parameter detection capabilities and compares favourably against existing techniques in terms of robustness against geometrical attacks such as rotation, scaling, and translation.

2. Wavelet Transform Modulus Maxima

In this work, WTMM has been used mainly because of its shift-invariance property. It is the WTMM's shift invariance property, which standard wavelets and multiwavelets do not have, that enables the proposed watermarking scheme to identify and undo geometrical attacks.

Consider an image $\boldsymbol{F}(\boldsymbol{x},\boldsymbol{y})$ and let $\boldsymbol{\theta}(\boldsymbol{x},\boldsymbol{y})$ represent a 2D low pass filter. Let $\boldsymbol{\psi^1}(\boldsymbol{x},\boldsymbol{y})$ and $\boldsymbol{\psi^2}(\boldsymbol{x},\boldsymbol{y})$ represent two partial derivative functions of $\boldsymbol{\theta}(\boldsymbol{x},\boldsymbol{y})$ along the horizontal and vertical directions respectively. The functions $\boldsymbol{\psi^1}(\boldsymbol{x},\boldsymbol{y})$ and $\boldsymbol{\psi^2}(\boldsymbol{x},\boldsymbol{y})$ are defined in Eq. (1) and Eq. (2) respectively [14] [25] as:

$$\boldsymbol{\psi^1}(\boldsymbol{x},\boldsymbol{y}) = \frac{\partial \boldsymbol{\theta}}{\partial \boldsymbol{x}}(\boldsymbol{x},\boldsymbol{y}) \tag{1}$$

$$\boldsymbol{\psi^2}(\boldsymbol{x},\boldsymbol{y}) = \frac{\partial \boldsymbol{\theta}}{\partial \boldsymbol{y}}(\boldsymbol{x},\boldsymbol{y}) \tag{2}$$

Let $\boldsymbol{s}$ denote the scale of wavelet transform. Then, the partial derivatives of $\boldsymbol{\theta}(\boldsymbol{x},\boldsymbol{y})$ at each scale can be defined as $\boldsymbol{\psi^1}_{\boldsymbol{s}}(\boldsymbol{x},\boldsymbol{y}) = \left(\frac{\boldsymbol{1}}{\boldsymbol{s}}\right)^{\boldsymbol{2}}, \boldsymbol{\psi^i}\left(\frac{\boldsymbol{x}}{\boldsymbol{s}},\frac{\boldsymbol{y}}{\boldsymbol{s}}\right), for\ \boldsymbol{i} = \boldsymbol{1},\boldsymbol{2}$. The wavelet transform $\boldsymbol{WF}(\boldsymbol{s},\boldsymbol{x},\boldsymbol{y})$ at each scale $\boldsymbol{s}$ has two components $\boldsymbol{W^1F}(\boldsymbol{s},\boldsymbol{x},\boldsymbol{y})$ and $\boldsymbol{W^2F}(\boldsymbol{s},\boldsymbol{x},\boldsymbol{y})$. These components represent the horizontal and vertical directions of wavelet transform as denoted in Eq. (3).

$$\begin{pmatrix} \boldsymbol{W^1F}(\boldsymbol{s},\boldsymbol{x},\boldsymbol{y}) \\ \boldsymbol{W^2F}(\boldsymbol{s},\boldsymbol{x},\boldsymbol{y}) \end{pmatrix} = \boldsymbol{s}\begin{pmatrix} \boldsymbol{F}*\boldsymbol{\psi^1}_{\boldsymbol{s}}(\boldsymbol{x},\boldsymbol{y}) \\ \boldsymbol{F}*\boldsymbol{\psi^2}_{\boldsymbol{s}}(\boldsymbol{x},\boldsymbol{y}) \end{pmatrix} \tag{3}$$

The magnitude ($\boldsymbol{Mf}(\boldsymbol{s},\boldsymbol{x},\boldsymbol{y})$) and the angle ($\boldsymbol{Af}(\boldsymbol{s},\boldsymbol{x},\boldsymbol{y})$) of the WTMM can be computed as in Eq. (4) and Eq. (5) respectively:

$$\boldsymbol{Mf}(\boldsymbol{s},\boldsymbol{x},\boldsymbol{y}) = \sqrt{|\boldsymbol{W^1f}(\boldsymbol{s},\boldsymbol{x},\boldsymbol{y})|^2 + |\boldsymbol{W^2f}(\boldsymbol{s},\boldsymbol{x},\boldsymbol{y})|^2} \tag{4}$$

$$\boldsymbol{Af}(\boldsymbol{s},\boldsymbol{x},\boldsymbol{y}) = \begin{cases} \boldsymbol{\alpha}(\boldsymbol{s},\boldsymbol{x},\boldsymbol{y}), & \boldsymbol{if}\ \boldsymbol{W^1f}(\boldsymbol{s},\boldsymbol{x},\boldsymbol{y}) \geq \boldsymbol{0} \\ \boldsymbol{\pi} + \boldsymbol{\alpha}(\boldsymbol{s},\boldsymbol{x},\boldsymbol{y}), & \boldsymbol{if}\ \boldsymbol{W^1f}(\boldsymbol{s},\boldsymbol{x},\boldsymbol{y}) < \boldsymbol{0} \end{cases} \tag{5}$$

where, $\boldsymbol{\alpha}(\boldsymbol{s},\boldsymbol{x},\boldsymbol{y}) = \boldsymbol{tan^{-1}}\left(\frac{\boldsymbol{W^2f}(\boldsymbol{s},\boldsymbol{x},\boldsymbol{y})}{\boldsymbol{W^1f}(\boldsymbol{s},\boldsymbol{x},\boldsymbol{y})}\right)$.

The WTMM coefficients can be identified by applying a suitable threshold to the magnitude Mf of the WTMM and can be represented with the help of a binary image where white and black pixels correspond to zero and respectively large-amplitude (modulus maxima) coefficients. The angle Af of the WTMM represents the angles at the points where

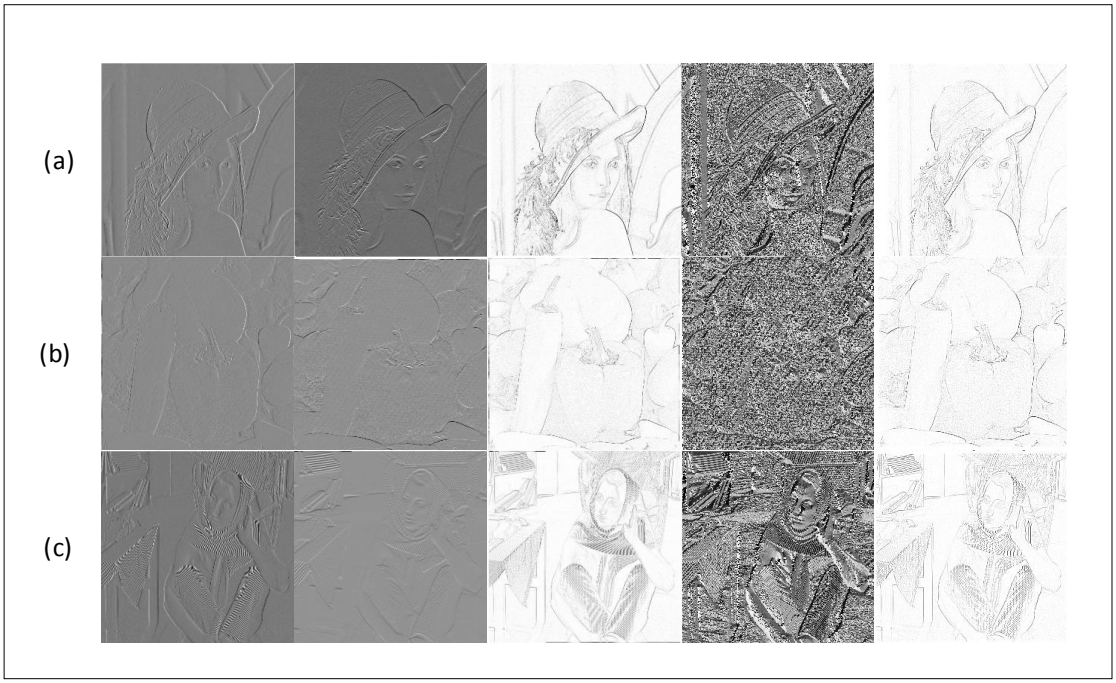
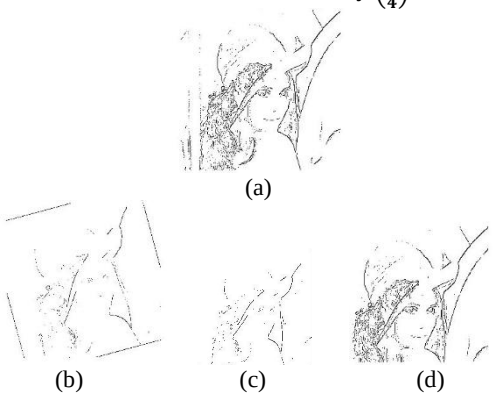


Figure 1. *WTMM examples for (a) Lena, (b) Pepper, and (c) Barbara images. From left to right: LH sub-band, HL sub-band, WTMM magnitude (Mf), WTMM angle (**Af**), and WTMM coefficients*

the modulus is nonzero. Figure 1 shows the vertical detail (LH) sub-bands, horizontal detail (HL) sub-bands, magnitude (Mf), phase (Af), and respectively the WTMM images corresponding to one level of decomposition and Haar wavelet.

The WTMM can be calculated using the following steps:

1. Separate the Low-High (LH) and High-Low (HL) parts of the wavelet transform coefficients so that they can be used to calculate the absolute value (magnitude) and the angle of the WTMM.
2. Compute the magnitude (absolute value) of wavelet transform coefficients using Eq. (5).
3. Use a threshold value to retain the wavelet transform coefficients with a magnitude larger than the threshold and discard the wavelet transform coefficients with a magnitude smaller than the threshold.
4. Compute the angle of wavelet transform coefficients using Eq. (5).
5. Quantize the angle to the multiple of $\left(\frac{\pi}{4}\right)$ to force the angle to start from 45 degrees.
6. Obtain the quantized angle as it follows:
   a. Round the angle values to the nearest integer value.
   b. Divide the rounded values by $\left(\frac{\pi}{4}\right)$.



(a) (b) (c) (d)

Figure 2. *(a) WTMM of the original Lena image; (b) Lena watermarked image rotated by (15°); (c) Lena watermarked image scaled by (0.7); (d) Lena watermarked image translated by (+80, -80).*

The quantized angles obtained are used as the direction of the angle. There are eight possible directions: 0 degrees, 45 degrees, 90 degrees, 135 degrees, 180 degrees, 225 degrees, 270 degrees, and 315 degrees. These angles correspond to the horizontal (right), diagonal (right, up), vertical (up), diagonal (left, up), horizontal (left), diagonal (left, bottom), vertical (down), and diagonal (right, bottom) directions respectively. The central pixel and its eight neighbouring pixels are used to determine the direction. The relevant direction is decided by the value of the angle. Figure 2 shows some visual examples of the WTMM outputs for rotation, scaling and translation.

3. Proposed Technique

This section presents a detailed description of the proposed robust logo image watermarking technique for colour images. The proposed technique consists of two parts: watermark embedding and watermark detection. Watermark detection itself is a two-stage process. The proposed watermark embedding technique is presented in Section 3.1 while the proposed watermark detection technique is presented in Section 3.2.

3.1. Watermark Embedding

The key features of the proposed watermark embedding technique are the embedding of two orthogonal 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 DMWT of the watermarked image already containing the 1-bit watermark. The 1-bit watermark is embedded in the wavelet domain, using the Haar wavelet, while the multibit watermark is embedded in the multiwavelet domain using the Cardbal2 multiwavelet. The proposed watermark embedding technique is shown in Figure 3. As it is shown in Figure 3, DWT is first applied to the original image and the LH and HL sub-bands are used to calculate the WTMM and embed a 1-bit watermark.

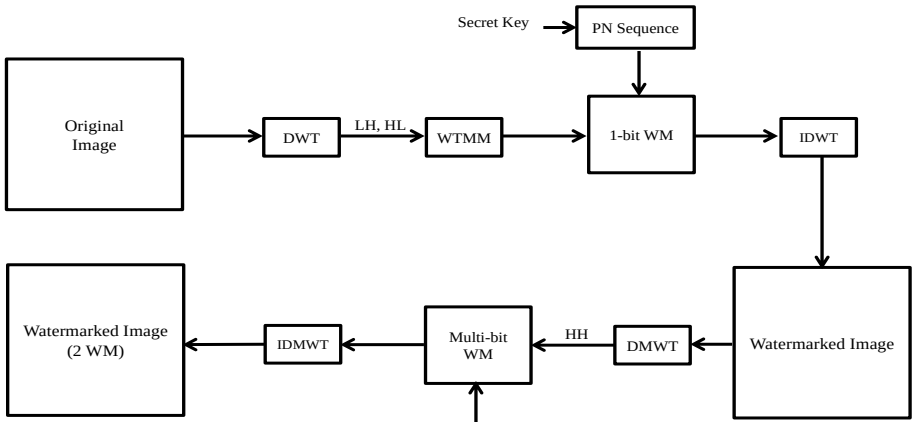


Figure 3. *The overall watermark embedding process.*

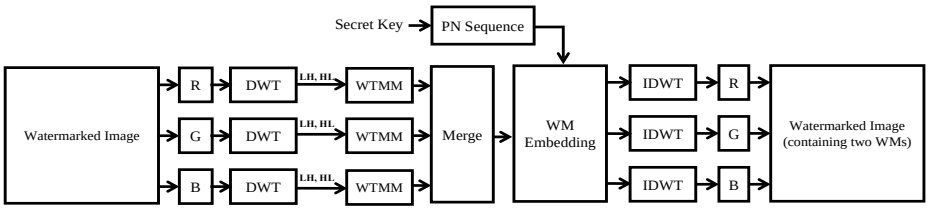


Figure 4. *The proposed 1-bit watermark embedding process.*

The principle behind the WTMM and 1-bit watermark is that WTMM provides the (shift invariant) modulus maxima values, so that the 1-bit watermark can be embedded in the relevant shift invariant coefficients. The PN sequence corresponding to the 1-bit WM is generated based on a secret key. The purpose of embedding this 1-bit watermark is to improve the robustness of the proposed scheme against geometric attacks. Once the 1-bit watermark is embedded, the next step is to apply the Inverse DWT to obtain the 1-bit watermarked image. Then, the DMWT is applied to the 1-bit watermarked image to access the High-High (HH) sub-band. The actual logo image which is the multi-bit watermark is then embedded in the HH sub-band with the help of a PN sequence and a secret key. Lastly, IDMWT is again applied to obtain the final watermarked image.

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 a geometric attack, establish what the attack parameters were and undo this attack prior to the extraction of the logo. While spread-spectrum techniques possess many appealing properties [26], their main disadvantage is their sensitivity to any geometric attack that leads to 'desynchronization' between the resulting image and the generated PN sequence. Therefore, the proposed watermark embedding technique relies on the shift invariance property of the WTMM to embed a robust 1-bit watermark. The embedding of a 1-bit watermark is solely done as an attack detection mechanism, allowing the proposed watermarking scheme to undo the geometric transformation and 'resynchronize' the image prior to the recovery of the multibit logo (watermark). 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. Then, the proposed algorithm recovers the multi-bit logo.

The 1-bit watermark and multi-bit watermark embedding processes are illustrated in more detail in Figure 4 and Figure 5 respectively. Figure 4 shows the embedding process of the low capacity 1-bit watermark.

After embedding the high capacity watermark, the watermarked image is then split into its three colour components R, G, and B. DWT is applied on each colour component. This is followed by a step in which the LH, and HL sub-bands are extracted from each colour component. At the end of this step, six matrices corresponding to the LH and HL coefficients of each of the three colour components are obtained. Next, WTMM is computed for these components. The WTMM provides the (shift invariant) modulus maxima values, so that the 1-bit watermark can be embedded in the relevant shift invariant coefficients. For simplicity, these outputs can be merged together and treated as one large contiguous block (with a higher chip rate) for watermark insertion (and later detection) purposes.

The 1-bit watermark is then embedded with respect to the PN sequence and a secret key. Lastly IDWT is applied to each of the colour component to obtain the final watermarked image.

From Figure 5, it can be seen that for the embedding of the multi-bit watermark, the original image is first read. It is then split into its three colour components: Red, Green, and Blue represented by the 'R', 'G', and 'B' blocks respectively. Next, the HH sub-band is extracted from each of these components. This is followed by a step in which the HH sub-band coefficients of the R, G, and B components are merged into a large contiguous block. This effectively triples the chip rate reported to the size of the image. The logo is then spread over the merged coefficients. This is done with the help of a PN sequence and a secret key. Lastly, IDWT is applied to obtain the watermarked image.

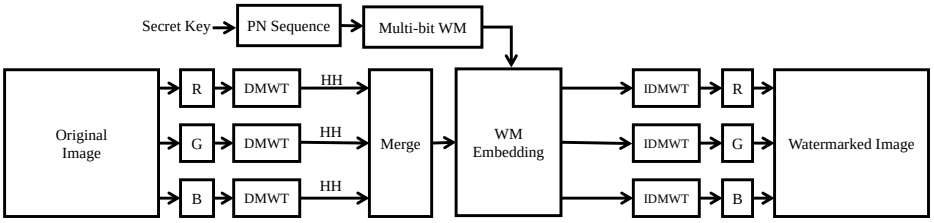


Figure 5. *The proposed multi-bit watermark embedding process.*

As it can be observed from Figure 4 and Figure 5, the DWT/DMWT 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.

3.2. Watermark Detection

The overall watermark recovery process is shown in Figure 6. Two scenarios have been considered for recovering the watermark. First, the 1-bit watermark is recovered. The recovered 1-bit watermark shows weather any attack on the watermarked image has taken place or not. The process starts by reading the watermarked image and splitting it into its three colour components R, G, and B. The LH, HL sub-bands are then extracted and the WTMM is computed. This is followed by merging all coefficients in a large contiguous block just like for embedding. The 1-bit watermark is then recovered by cross-correlating the merged coefficients with the same PN sequence that was used for generating the 1-bit watermark. At this stage, if a single large cross-correlation peak is found, this signals that the watermarked image has not suffered any desynchronization attacks as a result of some geometrical attack and therefore the multi-bit watermark can be safely recovered.

In the second scenario, the single large peak is not found. Rather, many smaller peaks are observed. This indicates that there is something wrong with the watermarked image which has likely been subjected to a geometric attack. In this scenario, the attack needs to be identified and the watermarked image must be first corrected and brought back in sync with the PN sequence, by undoing the geometrical transformation before being able to successfully recover the multi-bit watermark.

The multi-bit watermark recovery process is presented in Figure 7. First, the watermarked image is read. Then, it is split into its R, G, and B components. DWT is applied to each component. Then, the HH sub-band is extracted from each of the components. The coefficients are then merged into one larger block. Finally, cross-correlation is computed between the merged coefficients and the same PN sequence that was generated during the embedding of the multi-bit watermark. Finally, the multi-bit watermark is recovered. 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 R, G, and B components of the watermarked image. The only data required for watermark recovery is the watermarked image itself and the secret key used to generate the original PN sequence during embedding. This is one of the key advantages of spread spectrum based watermarking techniques.

As noted earlier, if during Stage 1 a single large cross-correlation peak cannot be found, then this outcome points to the scenario in which a geometric attack has taken place and the watermark recovery process enters an intermediate stage (Stage 1.5) designed to detect, undo the attack and resynchronize the watermark, before Stage 2 can be applied. In the case of this second scenario, in which the watermarked image has been geometrically attacked, the steps taken to

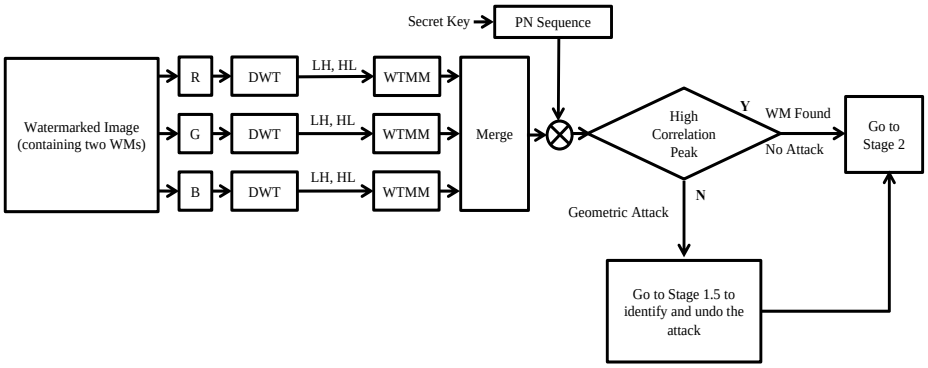


Figure 6. *The proposed watermark recovery process.*

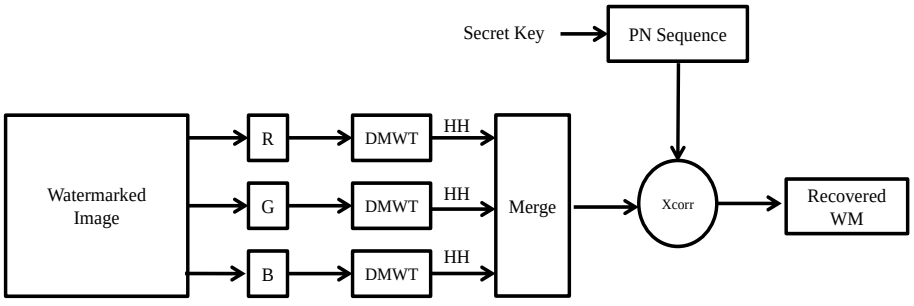


Figure 7. *Stage 2 of the proposed watermark recovery scheme.*

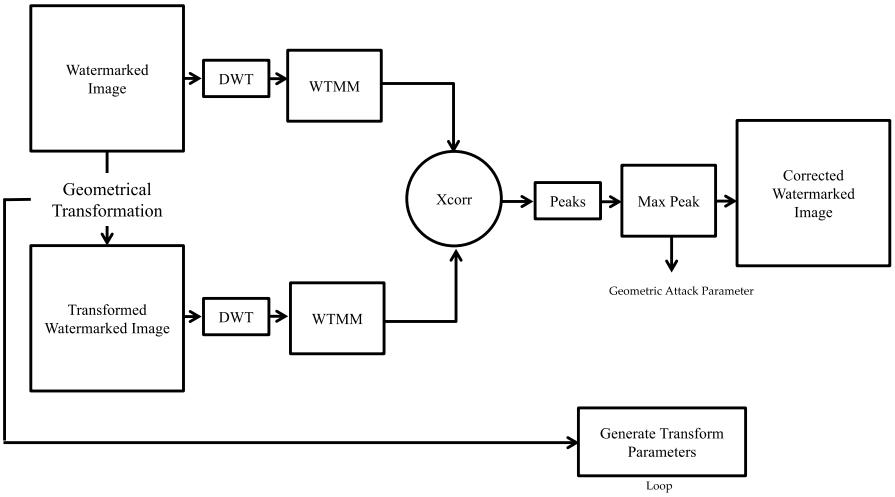


Figure 8. *Stage 1.5 of the proposed watermark recovery process.*

counter the manipulation and to recover the multi-bit watermark logo from the resynchronized watermarked image are shown in Figure 8. Attack parameters are determined via an extensive search carried out in a given attack parameter range. The attacked watermarked image is subjected to a number of successive geometrical transformations in this range. As shown in Figure 8, DWT is applied to both images and WTMM is computed. Cross-correlation is performed between the two outputs for each transform parameter in this range.

The transform parameters for which the cross-correlation peak is maximum represent the detected attack parameters. This mechanism can be used to recover common geometrical transforms such as rotation, scaling and translation. Finally, once identified, the transform parameters are used to correct the attacked watermarked image, by undoing the attack and resynchronizing the watermark to allow the successful recovery of the logo at Stage 2. The search algorithm works as it follows. Once DWT and WTMM are computed, then cross-correlation of the WTMM of the attacked watermarked image and the WTMM of the rotated version of this image is repeatedly computed step by step and the value of each cross-correlation peak is recorded for each rotation step, as part of a loop.

Once the loop completes, the rotation value that corresponds to the maximum recorded cross-correlation peak value amongst all other recorded cross-correlation values, represents the identified attack parameter itself. Once the attack parameter has been identified in this way, this value is used to undo the attack and correct the geometrically attacked watermarked image.

4. Results and Discussion

All the experiments were performed using MATLAB R2016. The experiments were performed on a MacBook Pro with a 2.2 GHz Intel Core i7 microprocessor, 16 GB DDR3 RAM, Intel Iris Pro 1536 MB graphics card and OS X El Capitan operating system. Two metrics were used to objectively evaluate the performance of the proposed algorithm. These are the Normalized Cross-Correlation (NCC) and the Bit Error Rate (BER).

4.1 Human Visual System Considerations

The Human Visual System (HVS) has been taken into consideration while assigning the embedding weights for the red, green, and blue components of the image. As the human eye is less sensitive to blue, the blue colour can be weighted higher than the red and green components. Many different weight combinations were empirically tested.

After experimenting with different weight factor combinations, the following weights were found to provide a good trade-off between robustness and quality of watermarked images: red (0.55), green (0.42), and blue (0.87). This weight assignment is also consistent with the fact that the human eye is more sensitive to changes in the green colour and least sensitive to changes in the blue colour. Hence, the smallest weight has been assigned to the green colour (i.e. lowest embedding strength) while the largest weight has been assigned to the blue colour (i.e. highest embedding strength.)

4.2 Test Dataset

The test dataset for the experiments included six cover images which are well-known and publicly available. The resolutions of these images are either 256x256 or 512x512. For each resolution, different images were used covering a broad range of characteristics.

Two different black and white (1 bit per pixel) logo images of different sizes were used. These are the ‘TEST’ logo image which has 50×20 pixels and the ‘ME’ logo image which has 21×10 pixels. These logos translate to a watermark length of 1000 bits and respectively 210 bits. Black and white logo images were chosen to keep the watermark length manageable. The logo images are shown in Figure 9.

(a)  (b) 

Figure 9. *The 'TEST' and 'ME' logo images.*

4.3 Attack Types

The main focus of the experiments is on demonstrating the robustness of the proposed algorithm against geometric attacks. These attacks include rotation, scaling and translation. For testing robustness against rotation, the images are rotated by different angles from 1 degree to 359 degrees and for each rotated angle the watermark is detected and recovered. Similarly, for testing robustness against translation, the image is shifted using different pixel offset values and in each case the watermark is detected and recovered. Lastly, to test the robustness of the proposed algorithm against scaling, the image is scaled both up and down by different scaling factors and in each case the watermark is detected and recovered.

4.4 Discussion

The proposed watermarking scheme can efficiently detect watermarks even after the cover image has undergone geometric attacks of varying intensities. This section demonstrates the watermark detection and recovery capabilities of the proposed watermarking scheme. For this purpose, both the 1-bit and multi-bit (logo) watermarks are first embedded in a cover image. The watermarked image is then subjected to rotation, translation, and scaling and in each case the proposed scheme is used to find the right transform parameters and undo them.

Figure 10 shows the detection result for the 1-bit watermark. It can be seen from Figure 10 that since a peak value of 1 has been achieved, with no side peaks, no geometrical attack has been detected, and the 1-bit watermark is successfully extracted, indicating that no attack took place and that it is safe to proceed to Stage 2 and recover the embedded logo. It is worth noting that the profile of NCC values can also indicate that a desynchronization type attack took place and therefore the logo watermark image cannot be recovered without first resynchronizing the image by undoing the attack. A typical example of this is illustrated in Figure 11 where many peaks of similar amplitudes can be seen. The presence of many peak values indicates that the watermarked image has been subjected to some geometrical manipulation/attack which would need to be identified and corrected before the actual logo watermark image can be recovered.

The results for the recovery of the multi-bit watermark are shown in Table 1 for the 'TEST' logo image and respectively in Table 2 for the 'ME' logo image. The multiwavelet used is Cardbal2.

Figure 12 shows examples of rotation attacks, detection of attack parameters and the restored images. Stage 1.5 of the proposed algorithm is applied in order to detect the amounts of rotation and to undo the rotation attacks. The position of the maximum value of the cross-correlation peaks indicates the amounts of rotation detected. Figure 13 shows examples of scaling attacks. Here, again the scaling attack

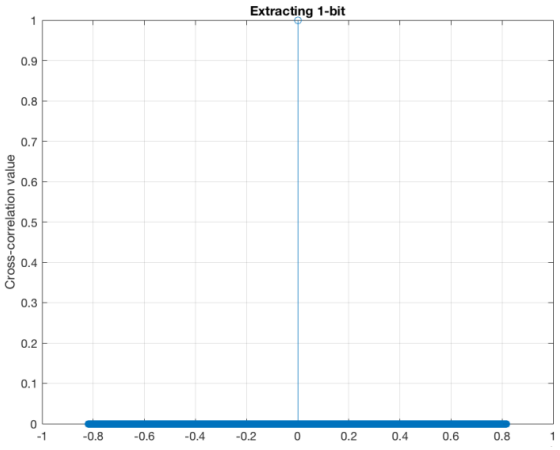


Figure 10. *The detection of 1-bit watermark.*

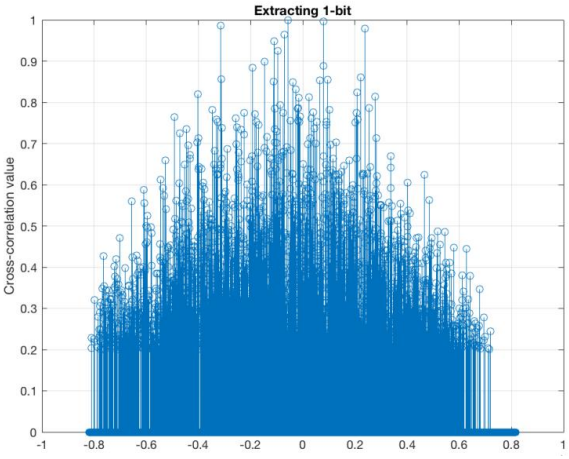


Figure 11. *In case of an attack, the NCC profile shows many peaks.*

Table 1. Recovering the logo watermark in case of no attack. The results are shown for the 'TEST' logo and cover images of size 512x512.

Image	PSNR (dB)	Normalized Cross-Correlation (NCC)	Bit Error Rate (BER)
Lena	37.24	1	0
Pepper	37.29	1	0
Barbara	36.44	1	0

Table 2. Recovering the logo watermark in case of no attack. The results are shown for the 'ME' logo and cover images of size 512x512.

Image	PSNR (dB)	Normalized Cross-Correlation (NCC)	Bit Error Rate (BER)
Lena	42.447	1	0
Pepper	40.423	1	0
Barbara	42.216	1	0

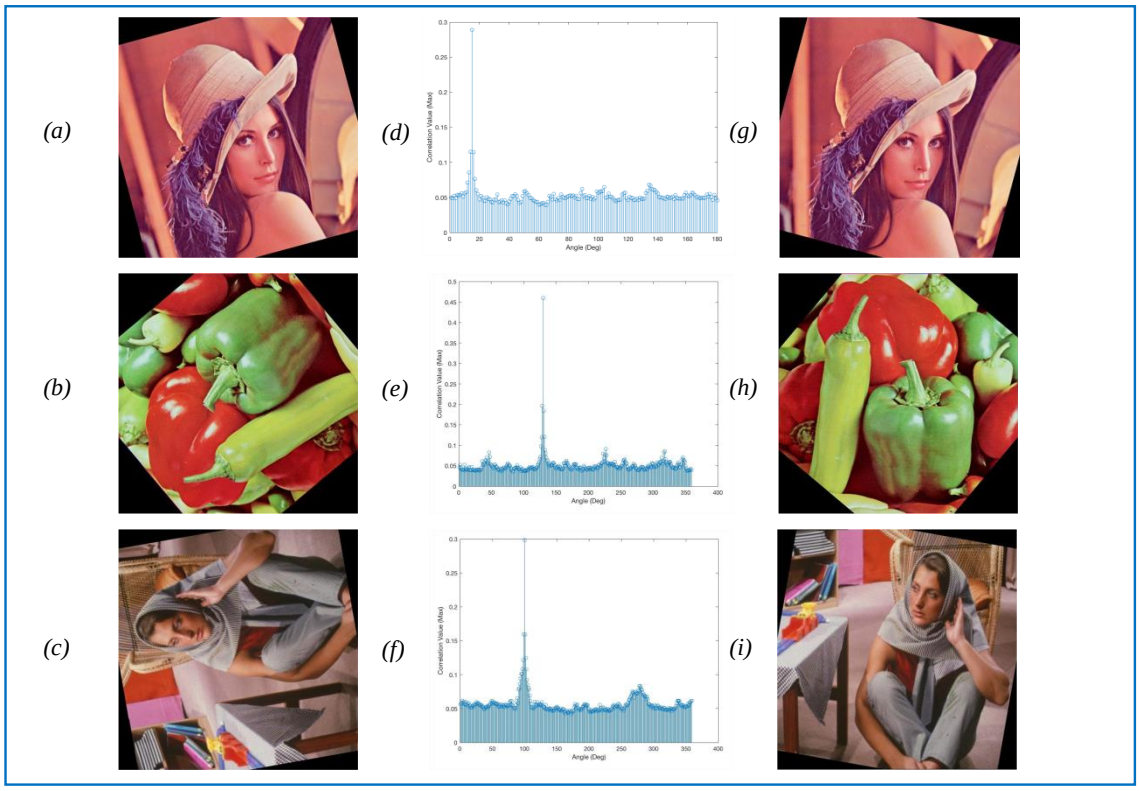


Figure 12. *(a-c): Rotated images (Lena, 15°; Pepper, 130°; Barbara, 100°). (d-f): corresponding detected parameters. (g-i): corresponding recovered images.*

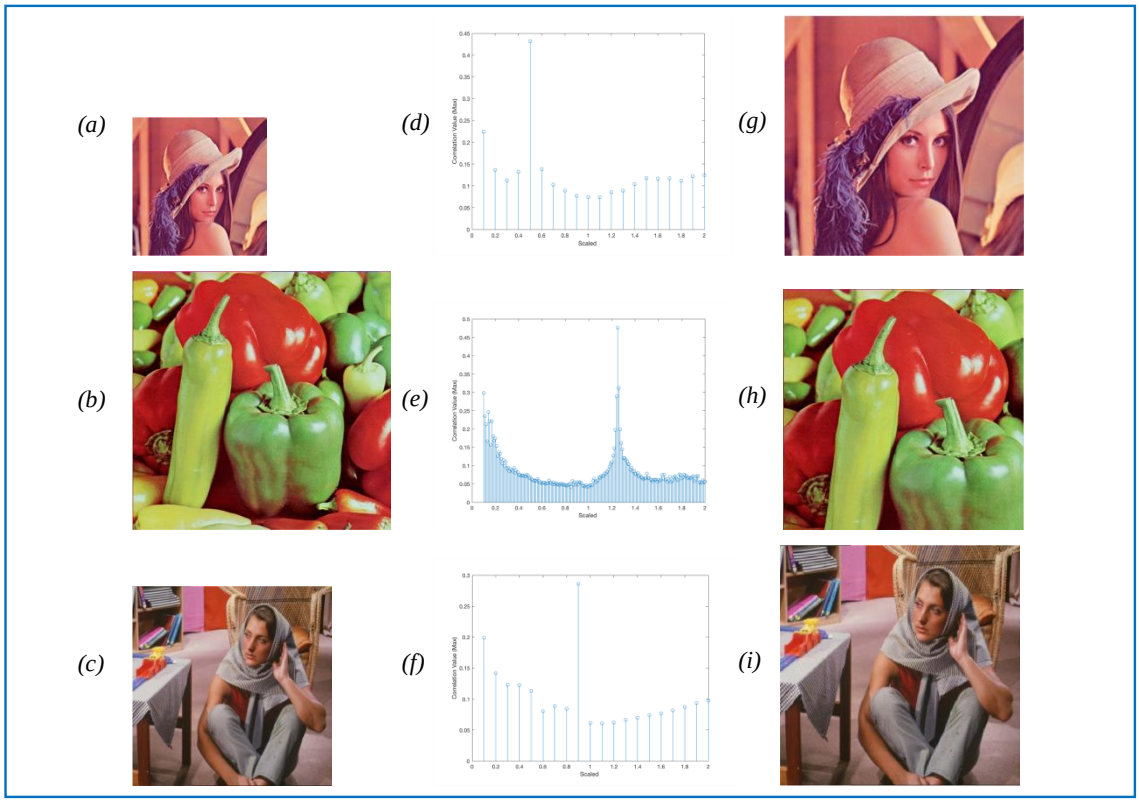


Figure 13. *(a-c): Scaled images (Lena, 0.5; Pepper, 1.25; Barbara, 0.9). (d-f): corresponding detected parameters. (g-i): corresponding recovered images.*

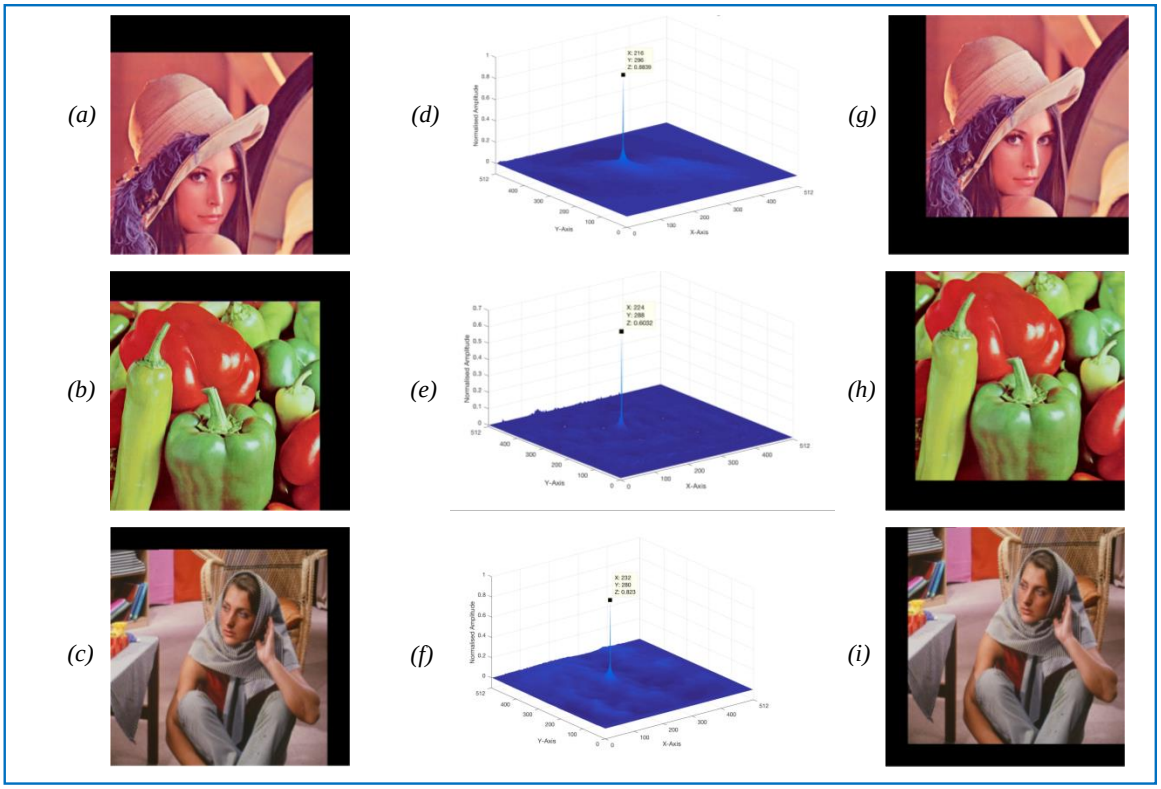


Figure 14. *(a-c): Translated images (Lena, (+80, -80); Pepper, (+64, -64); Barbara, (+48, -48)). (d-f): corresponding detected parameters. (g-i): corresponding recovered images.*

parameters are detected and undone using Stage 1.5 of the proposed algorithm. Finally, Figure 14 shows examples of translation attacks, detection of translation attack parameters, and the recovered images.

The results presented in Table 3 – Table 6 demonstrate the capability of the proposed method to detect the amount of rotation, scaling, or translation that the watermarked image is subjected to. The results in Table 3 and Table 4 are for the 'TEST' logo watermark and for cover images of resolution 512x512 and 256x256 respectively. Similarly, the results in Table 5 and Table 6 are for the 'ME' logo watermark and for cover images of resolution 512x512 and 256x256 respectively. For rotation attacks, the watermarked image is rotated by various degrees (such as 40, 90, 120, and 150 degrees) and after undergoing Step 1.5 of the proposed scheme, the distortion parameters are successfully detected with the help of WTMM and cross-correlation. For scaling attacks, the watermarked image is scaled by different scaling factors (such as 0.4, 0.8, 1.25, and 1.4) and the values of these scaling factors are also successfully detected as part of Step 1.5 of the proposed scheme. Similarly, for translation, the watermarked image is subjected to various translation offset values (such as [12,24], [66,88], [86,124] and [176,176]) which are also successfully detected.

Table 4 and Table 6 show the results for the case when smaller watermarked images of size 256x256 are subjected to geometrical attacks. This is to see the effect of using smaller cover size images and by implication smaller chip rates. The algorithm has still managed to detect the

Table 3. Distortion parameter detection using the proposed method. 'D' represents the 'Detected Parameter' and 'N' represents the 'Normalized Cross-Correlation Coefficient'. Results are shown for the 'TEST' logo and cover images of size 512x512.

Attack / Image		Lena		Pepper		Barbara	
Distortion Parameter		D	N	D	N	D	N
Rotation (Degrees)	40°	40°	0.98	40°	1	40°	0.98
	90°	90°	1	90°	1	90°	1
	120°	120°	0.98	120°	1	120°	1
	150°	150°	1	150°	1	150°	0.99
Scaling Factor	0.4	0.4	0.66	0.4	0.75	0.4	0.66
	0.8	0.8	1	0.8	1	0.8	0.99
	1.25	1.25	1	1.25	1	1.25	1
	1.4	1.4	0.99	1.4	0.98	1.4	0.94
Translation (x, y)	12, 24	12, 24	1	12, 24	1	12, 24	1
	66, 88	66, 88	1	66, 88	1	66, 88	1
	86, 124	86, 124	1	86, 124	1	86, 124	1
	176,176	176,176	0.99	176,176	0.99	176,176	0.94

Table 4. Distortion parameter detection using the proposed method. 'D' represents the 'Detected Parameter' and 'N' represents the 'Normalized Cross-Correlation Coefficient'. Results are shown for the 'TEST' logo and cover images of size 256x256.

Attack / Image		Lena		Pepper2		Foods	
	Distortion Parameter	D	N	D	N	D	N
Rotation (Degrees)	45º	45º	0.93	45º	0.98	45º	0.92
	90º	90º	1	90º	1	90º	1
	140º	140º	0.93	140º	0.97	140º	0.92
	220º	220º	0.91	220º	0.98	220º	0.95
Scaling Factor	0.7	0.7	0.56	0.7	0.66	0.7	0.43
	1.1	1.1	1	1.1	1	1.1	1
	1.3	1.3	1	1.3	1	1.3	0.99
	1.6	1.6	0.99	1.6	1	1.6	1
Translation (x, y)	10, 30	10, 30	1	10, 30	1	10, 30	1
	40, 80	40, 80	1	40, 80	1	40, 80	1
	120,120	120,120	1	120,120	1	120,120	0.99

Table 5. Distortion parameter detection using the proposed method. 'D' represents the 'Detected Parameter' and 'N' represents the 'Normalized Cross-Correlation Coefficient'. Results are shown for the 'ME' logo and cover images of size 512x512.

Attack / Image		Lena		Pepper		Barbara	
	Distortion Parameter	D	N	D	N	D	N
Rotation (Degrees)	40º	40º	1	40º	1	40º	1
	90º	90º	1	90º	1	90º	1
	120º	120º	1	120º	1	120º	1
	180º	180º	1	180º	1	180º	1
Scaling Factor	0.4	0.4	0.90	0.4	0.93	0.4	0.90
	0.8	0.8	1	0.8	1	0.8	1
	1.25	1.25	1	1.25	1	1.25	1
	1.4	1.4	1	1.4	1	1.4	1
Translation (x, y)	32, 32	32, 32	1	32, 32	1	32, 32	1
	80, 80	80, 80	1	80, 80	1	80, 80	1
	128, 128	128, 128	1	128, 128	1	128,128	1

Table 6. Distortion parameter detection using the proposed method. 'D' represents the 'Detected Parameter' and 'N' represents the 'Normalized Cross-Correlation Coefficient'. Results are shown for the 'ME' logo and cover images of size 256x256.

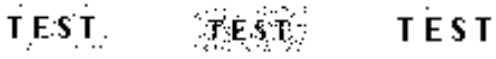
Attack / Image		Lena		Pepper2		Foods	
	Distortion Parameter	D	N	D	N	D	N
Rotation (Degrees)	45º	45º	1	45º	1	45º	1
	90º	90º	1	90º	1	90º	1
	140º	140º	1	140º	1	140º	1
	220º	220º	1	220º	1	220º	1
Scaling Factor	0.6	0.6	0.63	0.6	0.79	0.6	0.63
	0.7	0.7	0.96	0.7	0.97	0.7	0.92
	1.1	1.1	1	1.1	1	1.1	1
	1.2	1.2	1	1.2	1	1.2	1
Translation (x, y)	10, 30	10, 30	1	10, 30	1	10, 30	1
	40, 80	40,80	1	40, 80	1	40, 80	1
	120, 120	120, 120	1	120,120	1	120,120	1

distortion transform parameters successfully for all rotation, scaling, and translation attacks that watermarked images were subjected to.

Figure 15 shows examples of the recovered 'TEST' logo watermarks for different cases when 512x512 size cover images are used. Results for 256x256 size cover images are shown in Figure 16. Similarly, Figure 17 and Figure 18 show respectively examples of the recovered 'ME' logo images when cover images of 512x512 and 256x256 are used. It can be seen from Figure 16 and Figure 18 that in the case of 256x256 size cover images, as the watermarked image is already small in size, the chip rate decreases and as the image

(a) (b) (c)

Figure 15. *The recovered 'TEST' logo watermarks in case of 512x512 size cover images: (a) Lena (Rotation: 40º; NCC: 0.98), (b) Barbara (Translation: [86, 124]; NCC: 1), (c) Pepper (Scaling: 0.4; NCC: 0.75).*



(a) (b) (c)

Figure 16. *The recovered 'TEST' logo watermarks in case of 256x256 size cover images: (a) Lena (Rotation: 45º; NCC: 0.93), (b) Pepper2 (Scaling: 0.7; NCC: 0.66), (c) Foods (Translation: [120, 120]; NCC: 0.99).*

(a) (b)

Figure 17. *The recovered 'ME' logo watermarks in case of 512x512 size cover images: (a) Lena (Scaling: 0.4; NCC: 0.90), (b) Pepper (Scaling: 0.4; NCC: 0.93).*

(a) (b)

Figure 18. *The recovered 'ME' logo watermarks in case of 256x256 size cover images: (a) Lena (Rotation: 45°; NCC: 1), (b) Pepper2 (Scaling: 0.6; NCC: 0.79).*

is scaled down further, this starts affecting the logo which for more aggressive scaling factors gets destroyed in the process.

The results of the proposed method are also compared against the existing logo watermarking schemes in [21], [22], and [23]. These methods used 512x512 images with 32x32 size binary watermark image. Table 7 compares the NCC values and distortion parameter detection performance of the proposed method and the method in [21]. The results are shown for the 'Lena' image. The results show that, overall, the proposed method outperforms the method in [21], especially in terms of distortion parameter detection performance. Table 8 presents the comparison of NCC values of the proposed method and the method presented in [22]. From the results in Table 8, it can be concluded that both methods perform almost equally well in case of rotation, scaling and translation. Finally, Table 9 presents a comparison of the distortion parameter detection performance of the proposed method compared to the method presented in [23]. Again, both methods perform very well in case of rotation, scaling and translation attacks.

Table 7. Comparison of Normalized Cross-Correlation (NCC) values and distortion parameter detection performance of the proposed method and the method in [21]. The results are shown for the Lena image.

Distortion		Detected Parameter		NCC	
		Proposed	[21]	Proposed	[21]
Rotation (Degrees)	30°	30°	29.94°	0.98	1
	45°	45°	45.01°	1	0.99
	60°	60°	59.94°	1	1
	90°	90°	90.06°	1	1
Scaling Factor	0.25	0.25	0.24	0.153	0.69
	0.5	0.5	0.49	1	0.99
	0.8	0.8	0.8	1	1
	2	2	2.03	0.972	1

Table 8. Comparison of Normalized Cross-Correlation (NCC) values for the proposed method and the method in [22]. The results are shown for the Lena image.

Distortion		Proposed	[22]
Rotation (Degrees)	15°	1	0.99
	35°	0.98	0.98
	55°	0.99	0.98
	75°	1	0.99
Scaling Factor	0.5	1	0.980
	0.75	1	0.982
	1.5	0.983	0.986
	3	0.978	0.986
Translation (x, y)	(35, 25)	0.983	0.987

Table 9. Comparison of distortion parameter detection for the proposed method and the method in [23].

Distortion		Detected Parameter	
		Proposed	[23]
Rotation (Degrees)	15°	15°	15.024°
	60°	60°	59.988°
Scaling Factor	0.4	0.4	0.399
	1.5	1.5	1.501
Translation (x, y)	(40, 30)	(40, 30)	(40, 30)
	(7, 7)	(7, 7)	(7, 7)

In terms of time-complexity, the test results reveal that, on average, embedding of both watermarks in a host image takes around 90 seconds. In case of no attack, the embedded logo can be recovered on average in around 55 seconds. The total average time for both embedding and recovery (assuming no attack) is therefore 145 seconds. In order to analyse the time-complexity of the proposed watermarking scheme, the average embedding and recovery times are investigated. These time values correspond to the average of several tests performed using a number of different host images and include both watermarks.

Similar results were observed when the dataset was extended to include Airplane, Sailboat, and Parrot images. These results are summarized in Table 10.

Table 10. Distortion parameter detection using the proposed method. 'D' represents the 'Detected Parameter' and 'N' represents the 'Normalized Cross-Correlation Coefficient'. Results are shown for the 'TEST' logo and for the extended dataset contain additional cover images (Airplane, Sailboat, and Parrots) of size 512x512.

Attack / Image		Airplane		Sailboat		Parrots	
Distortion Parameter		D	N	D	N	D	N
Rotation (Degrees)	40º	40º	0.95	40º	0.97	40º	0.98
	90º	90º	1	90º	1	90º	1
	120º	120º	0.99	120º	0.98	120º	0.99
	150º	150º	1	150º	0.99	150º	0.99
Scaling Factor	0.4	0.4	0.66	0.4	0.67	0.4	0.55
	0.8	0.8	1	0.8	0.98	0.8	1
	1.25	1.25	1	1.25	0.98	1.25	1
	1.4	1.4	0.99	1.4	0.94	1.4	0.97
Translation (x, y)	12, 24	12, 24	0.99	12, 24	1	12, 24	1
	66, 88	66, 88	1	66, 88	0.98	66, 88	1
	86, 124	86, 124	1	86, 124	0.99	86, 124	1
	176,176	176,176	1	176,176	0.94	176,176	0.98

5. Conclusions

This paper proposes a robust logo watermarking scheme for colour images. By embedding a watermark in RGB colour images, the chip rate associated with a spread spectrum system can be increased three-fold compared to embedding the watermark in a grayscale image. This can improve the cross-correlation performance and the robustness of the watermark. The proposed scheme embeds two separate and orthogonal watermarks. A single-bit watermark is used to detect whether an attack has taken place or not, while a second multi-bit watermark carries the actual logo watermark. By embedding a logo, it is no longer required that the recovered watermark be an exact copy of the embedded watermark, since the recovered watermark can be inspected and recognised visually by exploiting the pattern recognition and error correction capabilities of the HVS. Therefore, a certain amount of error can be tolerated, as long as this doesn't become so visually significant, that the logo can no longer be recognised by the HVS.

The proposed scheme can successfully recover all rotation attacks, any scaling attacks as long as the size of the scaled image is at least 30% of the original image and any translation attacks provided that this doesn't lead to cropping more than 65% of the original image size.

In terms of future work, the chip rate and as such the robustness of the multi-bit watermark can be increased by using more sub-bands than just the HH sub-band to embed the logo. Using more sub-bands for embedding the logo is also in line with the spread spectrum philosophy, which relies on a large spread across a wide spectrum of frequencies in order to better withstand any attacks. By embedding the watermark in more sub-bands and/or levels, it will essentially get embedded/spread into a larger number of frequencies and scales, which can increase its robustness.

References

[1] Cox, I., Miller, M., Fridrich, J., and Kalker. T.: 'Digital watermarking and Steganography' (Elsevier, Burlington, 2007, 2nd edn.)
[2] Cox, I., Kilian, J., Leighton, F., and Shamoon, T.: 'Secure spread spectrum watermarking for multimedia', IEEE Transactions on Image Processing, 1997, 6, (12), pp. 1673 – 1687.
[3] Hartung, F., Su, J., and Girod, B.: 'Spread spectrum watermarking: Malicious attacks and counterattacks', Electronic Imaging, 1999, 3657, pp. 147-158.
[4] Senthil, V., Bhaskaran, R.: 'Wavelet Based Digital Image Watermarking with Robustness against Geometric Attacks', Proc. International Conference on Computational Intelligence and Multimedia Applications, December 2007, pp. 89 – 93.
[5] Nyeem, H., Boles, W., and Boyd, C.: 'Digital image watermarking, its formal model, fundamental properties and possible attacks', EURASIP Journal on Advances in Signal Processing, 2014, 1, pp. 1 – 22.
[6] Serdean, C., Ibrahim, M., Moemeni, A., and Al-Akaidi, M.: 'Wavelet and multiwavelet watermarking', IET Image Processing, 2007, 1, (2), pp. 223-230.
[7] Kingsbury, N.: 'Shift invariant properties of the Dual-Tree Complex Wavelet Transform', Proc. International Conference on Acoustics, Speech, and Signal Processing, Phoenix, Arizona, March 1999, pp. 16 – 19.
[8] Esfahani, R., Akhaee, M., and Norouzi, Z., 'A fast video watermarking algorithm using dual tree complex wavelet transform', Multimedia Tools and Applications, 2019, 78, (12), pp. 16159-16175.
[9] Agarwal, H., Atrey, P., and Raman, B., 'Image watermarking in real oriented wavelet transform domain', Multimedia Tools and Applications, 2015, 74, (23), pp. 10883-10921.
[10] Bhatti, A., Nahavandi, S., Frayman, Y.: '3D depth estimation for visual inspection using wavelet transform modulus maxima,' Journal of Computers and Electrical Engineering, 2007, 33, (1), pp. 48-57.
[11] Bhatti, A., Nahavandi, S.: 'Stereo correspondence estimation based on wavelets and multiwavelets analysis', Stereo Vision, (I-Tech, Vienna, Austria, 2008), pp. 27 – 48.
[12] Zhu, L., Zhu, L.: 'Electronic signature based on digital signature and digital watermarking', Proc. International Congress on Image and Signal Processing, 2012, pp. 1644 – 1647.
[13] Alghoniemy M., Tewfik, A.: 'Geometric distortion correction in image watermarking', Electronic Imaging, 2000, 3971, pp. 82 – 89.
[14] Luo, T., Xing, G., and Shi, I.: 'Mutual information based watermarking detection in wavelet domain for copyright protection', Proc. Asia-Pacific Trusted Infrastructure Technologies Conference, 2008, pp. 113-119.

[15] Prakash, O., Khare, A.: 'CT and MR Images Fusion Based on Stationary Wavelet Transform by Modulus Maxima', Computational Vision and Robotics, 2015, pp. 199-204.
[16] Gerasimova, E., Audit, B., Roux, S.G., Khalil, A., Gileva, O., Argoul, F., Naimark, O. and Arneodo, A.: 'A Wavelet-Based Method for Multifractal Analysis of Medical Signals: Application to Dynamic Infrared Thermograms of Breast Cancer', Proc. Nonlinear Dynamics of Electronic Systems, 2014, pp. 288-300.
[17] Loo, P., Kingsbury, N.: 'Digital watermarking with complex wavelets', Proc. International Conference on Image Processing, 2000, pp. 29–32.
[18] Loo, P., Kingsbury, N.: 'Watermarking using complex wavelets with resistance to geometric distortion', Proc. European Signal Processing Conference, Tampere, 2000, pp. 1-4.
[19] Zebbiche, K., Khelifi, F., & Loukhaoukha, K.: 'Robust additive watermarking in the DTCWT domain based on perceptual masking', Multimedia Tools and Applications, 2018, 77, (16), pp. 21281-21304.
[20] Ruanaidh J., Pun, T.: 'Rotation, scale and translation invariant spread spectrum digital image watermarking', Signal processing, 1998, 66, (3), pp. 303-317.
[21] Ye, X., Chen, X., Deng, M., and Wang, Y.: 'A SIFT-based DWT-SVD blind watermark method against geometrical attacks', Proc. International Congress on Image and Signal Processing, 2014, pp. 323-329.
[22] Fazli S., Moeini, M.: 'A robust image watermarking method based on DWT, DCT, and SVD using a new technique for correction of main geometric attacks', Optik - International Journal for Light and Electron Optics, 2016, 127, (2), pp. 964 – 972.
[23] Li, J., Zhu, Y.: 'A geometric robust image watermarking scheme based on DWT-SVD and Zernike moments', Proc. International Conference on Computer Science and Information Technology, 2010.
[24] Hu, J., Shao, Y., Ma, W., and Zhang, T.: 'A robust watermarking scheme based on the human visual system in the wavelet domain', Proc. International Congress on Image and Signal Processing, 2015, pp. 799 – 803.
[25] Lu, Z., Zhang, X.: 'Robust image watermarking based on the wavelet contour detection', Proc. International Conference on Acoustics, Speech, and Signal Processing, 2005, pp. ii-1165.
[26] Cox, I., Miller, M., and Bloom, J.: 'Watermarking applications and their properties', Proc. International Conference on Information Technology: Coding and Computing, 2000.