

DESIGN of HIGH PERFORMANCE DUAL PURPOSE WATERMARKING SYSTEM FOR COPYRIGHT PROTECTION AND IMAGE AUTHENTICATION

*Nidaa Hasan Abbas¹Sharifah **Mumtazah Syed Ahmad, ***SajidaParveen¹ Wan Azizun Wan,
*****Abed. Rahman Bin Ramli

Department of Computer and Communication System Engineering, Faculty of Engineering, Universiti Putra Malaysia,
Serdang,Selangor,Malaysia

*nidaahasan71@gmail.com, Tel-+60142637148), mumtazah@upm.edu.my, Tel-+603-89466436),
***sajidaupm@gmail.com.Tel- +923356300444), wawa@upm.edu.my, Tel- +603-8946 6442),
*****arr@upm.edu.my.Tel-+603-8946 6430.

ABSTRACT: In this paper, a new high- performance dual purpose watermarking algorithm is presented. It can provide integrated solution in copy right protection, content authentication and tamper detection. The main contribution of this paper is that the dual-purpose system has been tested against all stated attacks which impact the fragility as well as robustness and the performance stays at par or degrades to an acceptable level when the dual watermarks are inserted. This can be attributed to the insertion of the fragile watermark in a way which fully preserves the robust part. These properties are unlike the majority of current dual purpose schemes which deliver copyright protection at the cost of image authentication or vices versa.

Keywords Digital watermarking; robust watermarking; fragile watermarking; Lifting wavelet transform (LWT); Bi- dimensional Empirical Mode Decomposition (BEMD).

I. INTRODUCTION

Single watermarking methods, either robust or fragile, can only serve a limited number of purposes. They are bounded by their robustness or fragility. For example, fragile watermarks are not suitable for copyright protection because they can be destroyed by an attacker. However, for high-valued applications, such as military satellite images and e-commerce, it is necessary to verify that the image received is in fact authentic and confirm actual ownership. This trend has driven the launch of dual purpose, also known as dual function, watermarking [1].

A dual-purpose watermarking method combines a robust watermark and fragile watermark. Complementing the weaknesses of each single watermark, the dual-purpose watermarking method has a high potential in practical use. There are not many dual-purpose watermarking methods found in the literature compared to single watermark methods. This could be due to the complexity in designing a hybrid method.

A dual-purpose watermarking method combines a robust watermark and fragile watermark. Complementing the weaknesses of each single watermark, the dual-purpose watermarking method has a high potential in practical use. There are not many dual-purpose watermarking methods found in the literature compared to single watermark methods. This could be due to the complexity in designing a hybrid method.

II. Dual purpose watermarking algorithms

Dual purpose watermarking algorithms basically require the embedding of two different watermarks within the same media, which are collectively aimed at achieving different objectives, i.e. copyright protection and tampering detection. These two contradictory requirements present a great challenge in designing a multipurpose watermarking algorithm, where two watermarks of different natures should be embedded into the same digital contents for two different applications. The main restriction that should be taken into account when embedding them is that both watermarking techniques should neither interfere nor degrade the performance of the other [2].

The multipurpose watermark systems are classified into two schemes with respect to the priority principle of embedding order. In scheme (1), the two watermarks (the

robust and the fragile watermarks) are embedded in sequence one after the other, while in scheme (2), the two watermarks are embedded simultaneously.

Scheme (1)

In this method, the embedding process of two watermarks is performed consecutively one after the other. Figure 1 shows this scheme. As suggested by Mintzer and Braudaway [3], the ownership protection watermark should be cast first, then the less sensitive watermark for image authentication is embedded. Consequently, the order of extraction should follow the inverse order, from fragile watermark to robust watermark.

Most researchers adopt this scheme in performing the multipurpose watermark systems because the two watermarks can be embedded dynamically. Example is the work proposed by [4] in which the embedding and retrieving processes had been performed in wavelet transform.. The procedure of embedding is as follows: two different watermarks were used for authentication and recovery image simultaneously; the first watermark is image feature extracted from the DWT low frequency subband of the original image and was embedded into the corresponding subband. the second one is logo image was embedded in the middle frequency subband. Despite the algorithm performing the multipurpose watermark successfully, it is obvious that the computational complexity of the algorithm is high. The works proposed by [5, 6] were implemented by combining both spatial and transform domains to compensate the drawback of each other. In the algorithm proposed by [5], the original image is decomposed by DWT and the coefficients are quantized and hashed using secure cryptographic hash functions. The second watermark was added to the encrypted coefficients using dither modulation [7] to decrease the embedding visual distortion. In this way, the second watermark should not interfere with the watermark previously embedded in the spatial domain. The algorithm can withstand JPEG and JPEG2000 compression since the second watermark was embedded in the DWT domain of JPEG2000. On the other hand, in [6] the robust watermark was embedded in the spatial domain, whereas the fragile watermark was embedded in the DCT domain of the host video signal.

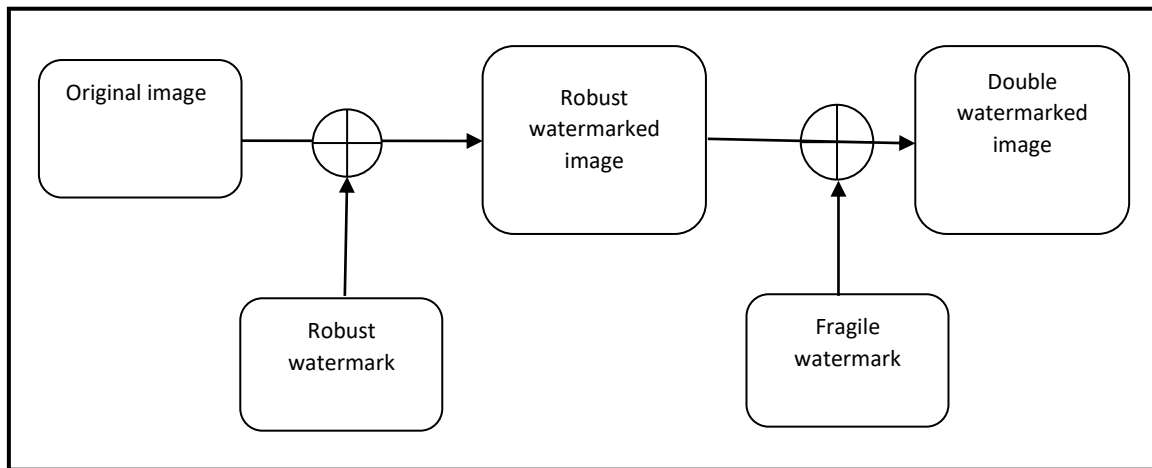


Figure 1: Multipurpose watermark embedding scheme (1)

Although the system can resist certain attacks and detect image manipulation, but still suffers from block artifacts introduced by DCT [8].

Scheme (2)

Embedding the two watermarks according to scheme (1) is impracticable in real applications [9] so few authors such as [10 -13] employed scheme (2) in embedding the two

watermarks simultaneously rather than consequently as in Figure 2.

The aim of this scheme is to solve the ordering problem of scheme (1) by decomposing the image into two components so the two watermarks can be embedded with no interference and the characteristics of each watermark can be preserved [9]

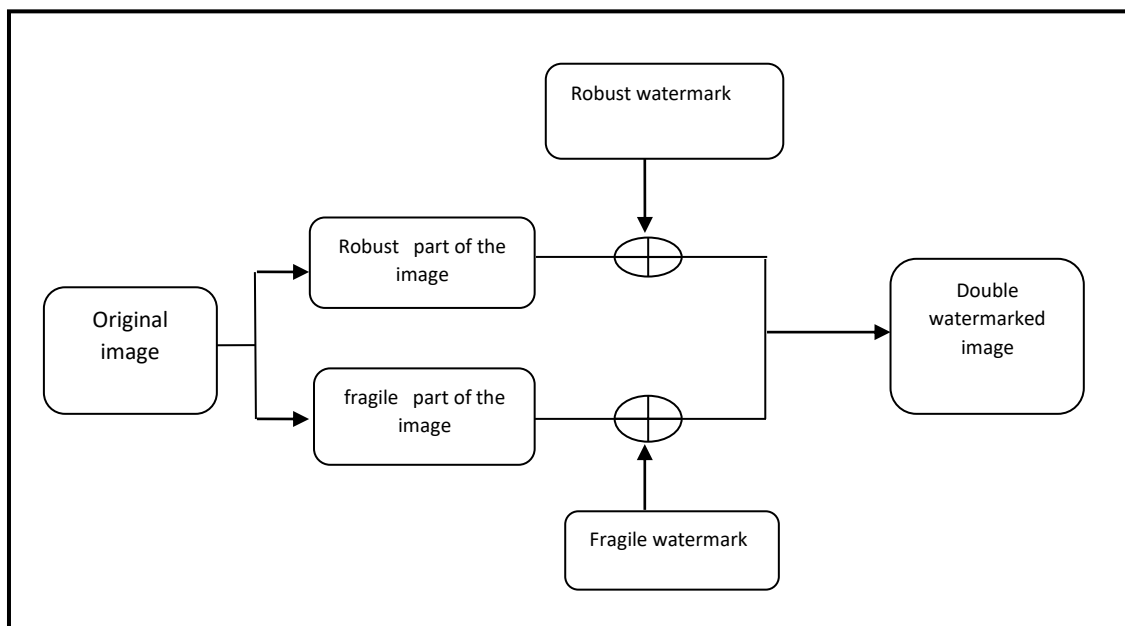


Fig. 2: Multipurpose watermark embedding scheme (2).

The two algorithms proposed by [10] and [11] were implemented in DCT. The fragile and robust watermarks in [10] were embedded into two different colour components of the colour image at the same time. Other approaches that embedded two watermarks simultaneously are [12] and [13] which were implemented in the wavelet domain. The work proposed by [12] used the cocktail watermarking [14]. However, the algorithm can resist many attacks excepting geometric attacks [15], the detection ability against tampering attacks was not reported. The authors in [13] extended the single robust algorithm proposed by [16] and [17] into a double function watermark algorithm for copyright protection and image authentication respectively. The robust watermark was embedded in the selected insensitive DWT coefficients and the fragile watermark in

the sensitive coefficients according to a switching matrix. Although the system has achieved a reasonable robustness against tested attacks, the watermarked image has some perceptual artefacts and the fragility was not tested against any tampering. In addition, the security issue wasn't taken into consideration [16].

The work presented by [18] embedded the two watermarks into two different components of the LWT of the original image using "zero-watermark" method - in this method the coefficients of the original image weren't modified directly. First the authentication watermark was embedded into the low frequency subband of the decomposed image using a secret

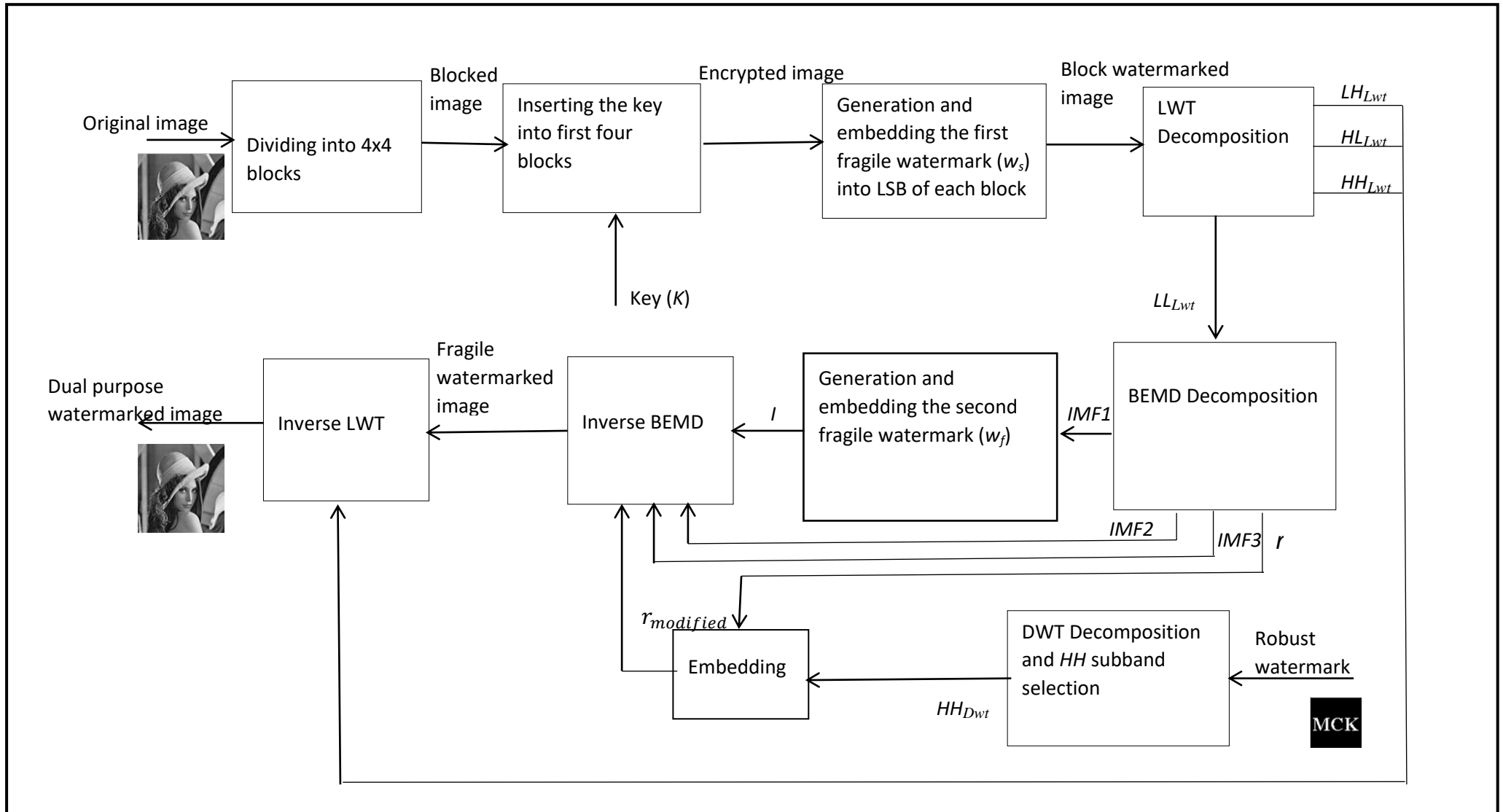


Figure 3: Proposed dual- purpose watermark algorithm

a11	a12	a13	a14	a15	a16	a17	a18
a21	a22	a23	a24	a25	a26	a27	a28
a31	a32	a33	a34	a35	a36	a37	a38
a41	a42	a43	a44	a45	a46	a47	a48
a51	a52	a53	a54	a55	a56	a57	a58
a61	a62	a63	a64	a65	a66	a67	a78
a71	a72	a73	a74	a75	a76	a77	a78
a81	a82	a83	a84	a85	a86	a87	a88

a ₃₇	a38	a31	a32	a33	a34	a35	a36
a47	a48	a41	a42	a43	a44	a45	a46
a57	a58	a51	a52	a53	a54	a55	a56
a67	a68	a61	a62	a63	a64	a65	a66
a77	a78	a71	a72	a73	a74	a75	a76
a87	a88	a81	a82	a83	a84	a85	a86
a17	a18	a11	a12	a13	a14	a15	a16
a27	a28	a21	a22	a23	a24	a25	a26

C11	C12	C13	C14	C15	C16	C17	C18
C21	C22	C23	C24	C25	C26	C27	C28
C31	C32	C33	C34	C35	C36	C37	C38
C41	C42	C43	C44	C45	C46	C47	C48
C51	C52	C53	C54	C55	C56	C57	C58
C61	C62	C63	C64	C65	C66	C67	C78
C71	C72	C73	C74	C75	C76	C77	C78
C81	C82	C83	C84	C85	C86	C87	C88

Figure 4: Secret key generation

key that contains the position of the coefficients that were randomly chosen to be used for embedding the watermark. Another key was constructed from the mean value of the wavelet components that selected by the first key and the corresponding values of the watermark. The same procedure was repeated in embedding the copyright watermark but in the middle frequency of LWT. This system required high storage capacity as four secret matrices should be stored and transmitted to be used by the decoder side as secret keys [19].

In spite embedding two watermarks, fragile and robust according to scheme (2) has solved the problem of avoiding the interference between the two watermarks, the embedding has some considerations that should be taken into account during the embedding and retrieving stages since the two watermarks are embedded at the same time into two different components of the original image and this may explain why the scheme has been used quite sparingly.

III. Dual purpose watermarking system architecture

It can be observed from reviewed literature that dual-purpose watermarking is not a well-explored area. The main drawbacks of them are that only one function has been achieved: either the robustness function has been done at the expense of the fragility or vice versa due to shortcomings in the technique employed for copyright protection or tamper detection. In this paper, a new high-performance dual purpose watermarking system is proposed as shown in Figure 3. It has been devised to

meet the criteria of fragility as well as robustness, while combining the processes of copyright protection and proofing tampering at the same time without significant degradation of each other.

The logical operation of the fragile and the robust watermarks could provide good robustness against critical attacks and reactivity to any manipulation at the pixel level. Besides, a good invisibility of the watermarked image has been obtained.

In the proposed dual purpose watermarking system (Figure 3), the fragile watermarking stage consists of two stages; the first stage is in the spatial domain while the other stage is in the frequency domain. Adding the fragile watermark first in the spatial domain using the block wise and the LSB method ensures small change on the imperceptibility and minimal effect on the robustness [19]. At the same time, it gives the highest possible tamper detection.

The second stage of the watermarking process is performed in the frequency domain by embedding the second fragile watermark and the robust watermark simultaneously. Through this way, the fragile watermark in the frequency domain which has a high capacity does not overlap with the robust watermark as depicted in Figure 3. The overall process of embedding the dual-purpose watermarks is as follows:

1. **Step one:** To provide data security, the secret key is produced and encrypted using the block encryption method as described below and Figure 4. The secret key is

embedded into the first four selected blocks of the cover image prior the embedding process.

Key generation procedure

A secret key is generated prior to watermark generation to increase the security of the system. The password is first selected by the user to avoid attackers from breaking the

authentication process which is then encrypted. A block encryption method is used which is simple but makes confusion for the attacker. Four blocks of the original image are chosen to embed the encrypted key. The process for encrypting the secret key is depicted in Figure 4 and as follows:

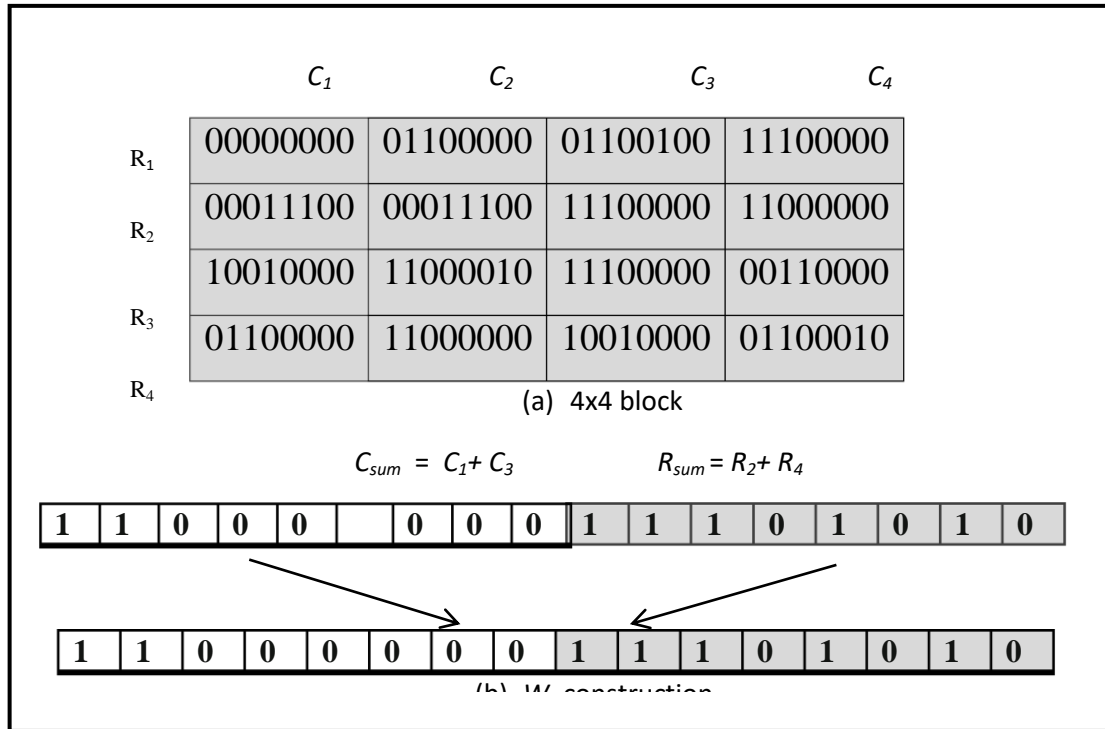


Figure 5: Example of spatial domain fragile watermark construction

1. The password (P) of length 64-bit binary is chosen by the user.
2. The rows are shifted by two positions.
3. The columns are shifted by two positions.
4. The original password matrix (P) is XOR-ed with the newly converted one ($P_{encrypted}$) to produce the resulted encrypted key matrix (K).
5. The first four blocks of 4x4 size are selected from the original image for embedding the secret key.
6. The resulted encrypted matrix (K) is changed into a 4x4 array to be embedded in the LSB of the selected blocks

The main goal of shifting rows and columns by two positions is to distort the order of the original numbers and to give them a new structure that makes it difficult for the attacker to decrypt the information. It also gives the algorithm the ability to resist different types of collage attacks. Moreover, choosing the XOR function between the original and the permuted key results in new values that completely differ from the original values as the XOR function is more ambiguous than other logical functions such as OR and AND [20].

2. **Step two:** The image is then divided into blocks of 4x4 pixels and the fragile watermark in the spatial domain (W_s) is generated from each block using the procedure described below. The generated fragile watermark (W_s) is then embedded in the LSB of each block producing blocked watermarked image.

Spatial domain fragile watermark generation procedure

After inserting the secret key, the fragile watermark is generated in the time domain by dividing the image into blocks of 4x4 pixels. In order to create standard template in both the embedding and tamper detection procedure, the LSB of each pixel in the two processes is initially set to zero [20]. Once the LSB of each pixel is set to zero, the process of constructions the fragile watermark (W_s) from each block begun. W_s consists of 16 bits length, the first 8 bits of them (C_{sum}) are constructed by adding the values of the pixel in the first and third columns for each block. The next 8 bits (R_{sum}) are then constructed by repeating the same procedure but on the second and fourth rows for each block. Figure 5 shows example of constructing 16 bits watermark for certain block. At this stage, the combination of C_{sum} and R_{sum} represents the 16 bit watermarks; W_s which are then changed to binary form to be embedded into the LSB of the block itself. After all the image blocks are watermarked, the image is rebuilt to its original dimensions from all the watermarked blocks.

3. **Step three:** The blocked watermarked image is then decomposed using LWT into four subbands; LL_{LWT} , LH_{LWT} , HL_{LWT} and HH_{LWT} .

4. **Step four:** LL_{LWT} subband is selected to be decomposed by BEMD into three $IMFs$ and one residue (r) according to the following equation :

$$I = \sum_{i=1}^3 (IMFi) + r \quad (1)$$

where $i \in \{1, 2, 3\}$.

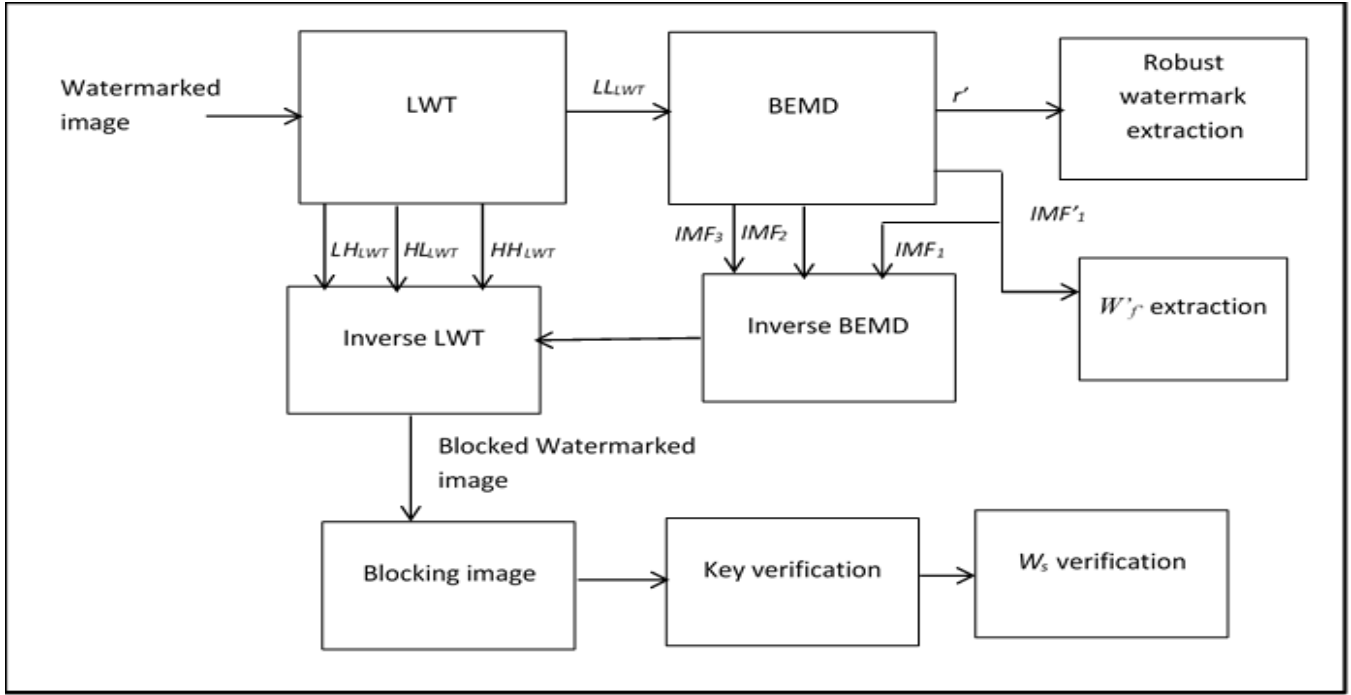


Figure 6: Procedure of dual purpose watermarking detection

The $IMFs$ is used to generate and embed the fragile watermark in frequency domain (W_f) while the residue component is employed for embedding the robust watermark.

5. **Step five:** The robust watermark which is a binary image is decomposed by DWT into four subbands; LL_{Dwt} , LH_{Dwt} , HL_{Dwt} and HH_{Dwt} and only high subband; HH_{Dwt} subband is selected for the embedding process.

6. **Step six:** The high sub-band (HH_{Dwt}) of the decomposed watermark is embedded in the residue (r) component of the LWT- BEMD decomposed original image. The process of inserting the watermark is managed by watermark strength k ($0 < k < 1$) in order to improve the invisibility of the watermarked image as shown in equation 2.

$$r_{modified} = \begin{cases} r + k \times HH_{Dwt}, & r < T \\ r, & \text{otherwise} \end{cases} \quad (2)$$

where $r_{modified}$ is the residue value of the original image after inserting the watermark, T denotes a threshold.

The threshold (T) is utilised during the embedding process and detection decisions as follows: in the case of r value is less than the threshold T , HH_{Dwt} is multiplied by the watermark strength k and added to the residue component. Otherwise, no changes are achieved in the value of r . The values of both k and T are determined empirically.

7. **Step seven:** At the same time, the fragile watermark in the frequency domain (W_f) is created from IMF_1 subband by selecting the first right- top corner block of size 8×8 from IMF_1 .

8. **Step eight:** The binary watermark W_f is constructed by mapping the pixel values of the selected block into binary values based on an empirically chosen threshold (T_h) according to equation 3.

$$w_f = \begin{cases} 1, & b_{ij} \geq T_h \\ 0, & \text{otherwise} \end{cases} \quad (3)$$

where b_{ij} is the first right - top corner block, $i \in \{1, \dots, 8\}$ and $j \in \{1, \dots, 8\}$

9. **Step nine:** The binary watermark (W_f) is then iterated to be same dimension as the original IMF_1 and embedded into IMF_1 according to equation 4.

$$IMF_{1new} = IMF_1 + W_f \quad (4)$$

where IMF_{1new} is the watermarked version of IMF_1 .

10. **Step ten:** The dual purpose watermarked image is initially derived using the inverse BEMD by summing the watermarked residue with three $IMFs$ as explained in equation 5 to obtain $I_{watermarked1}$.

$$I_{watermarked1} = IMF_{1new} + IMF_2 + IMF_3 + r_{modified} \quad (5)$$

where $I_{watermarked1}$ is the output of the inverse BEMD

11. **Step eleven:** Next, inverse LWT is applied to $I_{watermarked1}$ and the remaining subbands of the LWT; LH_{LWT} , HL_{LWT} and HH_{LWT} as depicted in equation 6 to produce the dual purpose watermarked image $I_{watermarked}$.

$$I_{watermarked} = ILWT(I_{watermarked1}, LH_{LWT}, HL_{LWT}, HH_{LWT}) \quad (6)$$

IV. The dual-purpose watermarking detection procedure

The watermarks detection is the reverse process of their embedding stages as shown in Figure 6 and listed below:

1. The first step of extracting the watermarks begins by transforming the watermarked image to the frequency domain via LWT. The lower subband of the transformed image; LL_{LWT} is further decomposed using BEMD. The fragile watermark (W'_f) in the frequency domain is recreated using the LSB of the IMF_1 to be compared with the primary watermark (W_f). To achieve image authentication, a binary error matrix (E_f) is generated by computing the bit error between the original and the extracted watermarks according to Equation 7.

$$E_f = (W_f \oplus W'_f) \quad (7)$$

where \oplus is the XOR logical operation. The mismatch and match between the two watermarks yields 1's and 0's in E_f , respectively. The tampering area can be allocated in terms of the bit error matrix as the most error pixels would cluster in distorted regions if tampering attacks were made on the watermarked image. On the other hand, the isolated error pixel is not considered as tampered because it is caused by unintentional attack [21].

2. Simultaneously, the robust watermark is deducted from the residue constituent of the LWT-BEMD transformed watermarked image. The residue constituent of the LWT-BEMD decomposed original image; r is deducted from the residue constituent of the LWT-BEMD decomposed watermarked image; r' . The outcome of the deduction denotes the HH'_{Dwt} sub-band of the watermark once it is split by the watermark strength k . Lastly, inverse DWT is employed on the watermark subbands; LL_{Dwt} , LH_{Dwt} , HL_{Dwt} and HH'_{Dwt} to obtain the robust watermark.
3. To implement the authentication procedure in the spatial domain, the image is restructured to the spatial domain by combining all $IMFs$ and the residue component according to Equation 1. The image is then divided into blocks of size 4×4 pixel.
4. The secret key is verified by the receiver. The receiver is provided with the key (K) which is then encrypted using the encryption procedure described previously. The encrypted key is then compared with embedded key (K'). If the two key bits do not match, the corresponding watermarked image is considered as tampered, and the detection process is stopped. Otherwise, the image is considered as authentic.
5. The third procedure of the authentication is implemented by extracting the embedded watermark Ws' from the LSB of each pixel. Another 16 bits watermark Ws is produced for each block by applying the same procedure used in generating the watermark bits explained previously. The comparison between the newly produced watermark Ws and the embedded watermark Ws' is done for each single block to achieve the third level of authentication. If the value of one bit in a certain block is not equal to the extracted one, the given block is considered as tampered; otherwise it is marked as authentic.

V. The experimental results

In this section, the implementation of the robust and the fragile algorithms of the proposed hybrid watermarking scheme for the dual-purpose image watermarking is presented and analysed. The watermark image embedding and detecting procedures detailed in Sections III and IV respectively, were applied to greyscale images of dimensions (512×512) pixels. Furthermore, the robust watermark is a binary image with the dimensions of 256×256 pixels while the fragile watermark was self-generated from the original image in the spatial and frequency domain.

To prove the efficiency of the proposed dual purpose watermarking algorithm in achieving copyright protection and tamper detection, both the robust and fragile watermarks are extracted with and without attacks as in the following subsections:

V.1 Verifying the algorithm robustness

In the case of all the experiments carried in this study, the watermark strength (k) was set at 0.027, whereas the threshold (T) was set at 150. For objectively assessing the watermarked image's perceptual quality, the Peak Signal-to-Noise Ratio ($PSNR$) value, has been used. The $PSNR$ between the original image (I) and the watermarked image (I') is given by:

$$PSNR = 10 \log_{10} \left[\frac{M \times N \times \max(I)^2}{\sum_{i=1}^M \sum_{j=1}^N (I - I')^2} \right] \quad (8)$$





where M and N are the dimensions of the image. Also, for objectively analysing the watermarking scheme robustness, the Normalised Cross Correlation (NCC) value, between the original watermark (w) and the extracted watermark (w^*) is calculated using the following equation:

$$NCC = \frac{\sum_{i=1}^M \sum_{j=1}^N w(i,j) w^*(i,j)}{\sum_{i=1}^M \sum_{j=1}^N w(i,j)^2} \quad (9)$$

To prove the algorithm robustness, the detection procedure described in section IV was applied to extract the robust watermark from the dual watermarked images for three cases: without any attack, with nongeometric attacks and with geometric attacks as in the following;

Verifying the algorithm robustness without attacks

First the robust watermark is extracted from Lena watermarked image without attack as shown in Table 1

Table 1: Robust watermark extraction			
Original image	Original watermark	Dual watermarked image	Extracted watermark
		 $PSNR=48.68$	 $NCC=0.998$

The obtained value of NCC is 0.998 while the $PSNR$ is 48.68. The results indicate that the dual-purpose watermarking algorithm exhibited a reasonable robustness. In general, for ensuring that the inserted watermark is imperceptible, the image $PSNR$ value must be higher than 35 dB while the NCC value must be ideally '1' in case of no attack [22] and the NCC value above or equal to 0.75 is acceptable [23].

For further investigating the robustness of the algorithm, its performance was tested against the critical attacks as described below.

Verifying the algorithm robustness against non-geometric attack

For determining the algorithm performance, several non-geometric attacks were applied to the algorithm. Non-

geometric attack includes filtering, noise and JPEG compression attacks.

Table 2: Robust watermark extraction under filter attack

Filter	Reconstructed watermark/NCC	Filter	Reconstructed watermark/NCC	Filter	Reconstructed watermark/NCC
Median (2, 2)	0.978	Wiener (2, 2)	0.978	Gaussian (2, 2)	0.978
Median (5,5)	0.976	Wiener (5,5)	0.975	Gaussian (5,5)	0.975
Median (9,9)	0.974	Wiener (9,9)	0.975	Gaussian (9,9)	0.974
Median (11,11)	0.974	Wiener (11,11)	0.974	Gaussian (11,11)	0.974

Table 3: Robust watermark extraction under noise attack

Noise	Reconstructed watermark NCC	Noise	Reconstructed watermark NCC	Noise	Reconstructed watermark NCC
Gaussian (M=0,var=0.5)	0.978	Speckle (M=0,var=0.5)	0.978	Salt & pepper (0.5)	0.978
Gaussian (M=0,var=0.1)	0.976	Speckle (M=0,var=0.1)	0.975	Salt & pepper (0.1)	0.975
Gaussian (M=0,var=0.01)	0.974	Speckle (M=0,var=0.01)	0.975	Salt & pepper (0.01)	0.974
Gaussian (M=0,var=0.001)	0.974	Speckle (M=0,var=0.001)	0.974	Salt & pepper (0.001)	0.974

Table 4: Robust watermark extraction under JPEG compression

Attack	Reconstructed robust Watermark/NCC
JPEG compression Q = 5	0.934
JPEG compression Q = 10	0.947
JPEG compression Q = 30	0.955
JPEG compression Q = 40	0.959
JPEG compression Q = 50	0.957
JPEG compression Q = 70	0.964

The filtering operation can be implemented using various window sizes, as in the proposed scheme, which has been tested with six various window sizes (e.g., 2×2, 3×3, 5×5, 7×7, 9×9 and 11×11) for three different filtering attacks, i.e., median, Wiener and Gaussian filter attacks. Table 2 shows the robustness performance of the dual-purpose algorithm under filters attacks.

The performance investigation also involves noise addition. Noise addition is another type of attack that falls under non-geometric attacks category which could be added to the image when transmitted on communication channels. Gaussian noise, speckle noise and the salt and pepper were added to the watermarked Lena image with six different

values of variance i.e. 0.5, 0.3, 0.1, 0.01, 0.001, 0.005 as depicted in Tables 3.

JPEG compression is the last non-geometric attack employed to test the proposed algorithm. Different quality factors of JPEG varying in the range 5- 70 are employed as depicted in Table 4.

Verifying the robustness algorithm against geometric attack

The proposed algorithm was further tested for the various geometric attacks. Translation attack is implemented for the ranges: (10 rows,10 columns), (10 rows,20 columns), (20 rows,35 columns), (35 rows,40 columns), (40 rows,40 columns) and (50 rows,50 columns). In addition, watermarked Lena image is shearing attacked by rows and columns for two cases; (0.2, 0.2) and (1, 0.2). Cutting attack is implemented by cutting Lena image with 10 rows, 10 columns, 20 rows, 30 rows, 30 columns and centred cropped by 20%. The results depicted in Tables 5-7.

Table 5: Robust watermark extraction under translation attack

Attack	Reconstructed watermark/NCC
Translation (50,50)	0.943
Translation (40, 40)	0.950
Translation (10, 10)	0.971

Table 6: Robust watermark extraction under shearing attack

Attack	Reconstructed watermark/NCC
Shearing (1, 0.2)	0.902
Shearing (0.2, 0.2)	0.924

Table 7: Robust watermark extraction under cut attack

Attack	Reconstructed watermark/NCC
Cut 10 rows	0.943
Cut 10 columns	0.954
Cut 20 rows	0.975
Cut 30 rows	0.975
Cut 30 columns	0.975
centred cut 20%	0.959

V.2 Verifying the algorithm fragility

The detection rate (R) is used to evaluate the tampering detection capability of the authentication algorithm according to the following equation:

$$R = 1 - \frac{fN + fP}{1 + N} \times 100 \% \quad (10)$$

where N stands for the number of tampered regions, F_P is the false positive and F_N is the false negative which calculated according to the following expressions:

$$fP = \frac{\text{number of pixels in untampered region, detected as tampered}}{\text{total number of pixels in untampered region}} \quad (11)$$



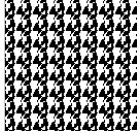
$$fN = \frac{\text{number of pixels in tampered region, detected as untampered}}{\text{total number of pixels in tampered region}} \quad (12)$$

The false positive value refers to the number of pixels detected as tampered pixels although they are untampered. By contrast, the false negative value refers to the number of tampered pixels that are detected as untampered. To prove the algorithm fragility, the detection procedure described in section IV was applied to extract the fragile watermark from the dual watermarked images for three cases: without applying any attack, by applying deletion attack and by applying copy paste attack as in the following:

Verifying the algorithm fragility without attacks

The fragile watermark was first extracted from the dual watermarked Lena image without applying attack as shown in Table 8:

Table 8: Fragile watermark extraction

Original image	Dual watermarked image (PSNR=48.68)	Extracted watermark (NCC=1)
		

The obtained value of NCC is '1' i.e. the watermark bits were all extracted successfully and the probe image was seen to be authentic. In addition, the $PSNR$ value for dual watermarked Lena image was still high and tolerable i.e.48.68 dB.

For further investigating the fragility of the algorithm, its performance was tested against the critical attacks as described below.

Verifying the algorithm fragility under deletion attacks

To verify the fragility performance of the algorithm, deletion attack was first applied, which focuses on deleting part of the watermarked image. Different scales of this attack with different target locations are performed to evaluate the detection efficiency of the proposed scheme, as shown in Table 9.

Table 9: Fragile watermark extraction under deletion attack


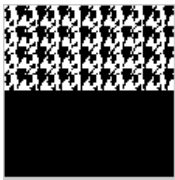



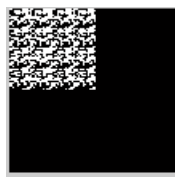


Tampered watermarked image	Bit error rate matrix
	
	
	
	




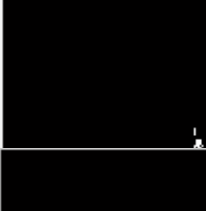

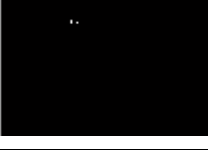
Table 9 explains the tampered watermarked images and the corresponding bit error matrix after carrying out many attacks by deleting 50%, 25% and 12.5% of Lena and Tank watermarked images. The distorted region in the error matrix corresponds to erroneous pixel in which the tampered has been made to the watermarked image, wherein any mismatch between the embedded and extracted watermarks yields 1's [21].

Based on the above tables, the proposed scheme could identify the deletion attacks that took place on the image with respect to the bit error rate matrix as a majority of the error pixels were seen to cluster in the distorted regions of the image if any size of tampering attacks were carried out on the watermarked image.

Verifying the algorithm fragility under copy paste attacks

A copy-paste type of attack was also carried out on the dual watermarked Lena image. A portion of the feather present in her hat was copied and pasted on the opposite side of the face. Also, a black rectangular region was copied and then pasted in the shadow of the woman's hat. Furthermore, another small region in the image was tampered wherein the clasp was pasted above her hat (a small region). These tampering areas have been illustrated in Table 10 with the bit error matrix.

Table 10: Fragile watermark extraction under copy paste attack

Tampered watermarked image	Bit error rate matrix
	
	
	

As depicted in the above table, the clustered region in the error matrix corresponds to erroneous pixel in which the tampered has been made to the watermarked image, wherein any mismatch between the embedded and extracted watermarks yields 1's [21]. Based on the above table, the proposed algorithm was able to detect the different tampering even when small tampering areas were carried out which involved pasting a small clasp on the Lena hat.

For a better estimation, the tampering detection rate (R) was used to evaluate the proposed algorithm for different image tampering sizes i.e., 10%, 20%, 30%, 40%, and 50%. as presented in Table 11 below.

According to all the observations noted in in this table, it can be seen that the achieved detection rate (R) for the dual purpose algorithm is greater than 94.98 % for the case of 10% tampering. Thus, the proposed algorithm could efficiently detect the tampering attacks with high detection rate even when the image was tampered slightly (10%).

Table 11: Robust watermark extraction

Image	10%	20%	30%	40%	50%
Lena	94.98	96.49	97.98	98.04	98.76
Cameraman	95.98	95.95	96.92	97.95	98.12
Peppers	96.10	95.69	95.86	99.00	99.15
Pirate	95.37	96.87	96.08	96.43	97.95
Woman blonder	96.94	97.43	97.46	98.87	99.94
Jet Plane	97.23	97.13	96.05	96.45	98.58
Lake	94.89	95.79	96.94	95.84	98.76
Elaine	96.57	97.38	98.06	98.06	99.78
woman_darkh air	95.85	96.98	98.49	98.28	99.94
mandrill	96.94	97.17	98.75	98.26	99.67

VI. CONCLUSION

This paper presented new and high performance dual purpose watermarking scheme for copyright protection and image verification. For this purpose, two different watermarks are embedded within the same image; the first watermark is robust watermark while the second watermark is fragile watermark. the fragile watermarking stage consists of two stages; the first stage is in the spatial domain while the other stage is in the frequency domain. Adding the fragile watermark first in the spatial domain using the block wise and the LSB method ensures small change on the imperceptibility and minimal effect on the robustness. At the same time, it gives the highest possible tamper detection. The second stage of the watermarking process is performed in the frequency domain by embedding the robust watermark and the second fragile watermark simultaneously into two different components of the BEMD decomposed image. Through this way, the fragile watermark in the frequency domain which has a high capacity does not overlap with the robust watermark. The robustness was tested against various geometric and non-geometric attacks, at the same time the system exhibited good sensitivity against tampering attacks.

REFERENCES

- [1] H. Yang and T. Zhang, "A New Algorithm of Compound Image Watermarking Based on DDWT," in *2008 International Conference on MultiMedia and Information Technology, IEEE.*, 2008, pp. 268–271.
- [2] C. S. Avila and M. N. Miyatake, "Multipurpose Image Watermarking Scheme based on Self-embedding and Data Hiding into Halftone image," in *Electronics, Robotics and Automotive Mechanics Conference (CERMA), 2010*, 2010, pp. 394–398.
- [3] F. Mintzer and G. W. Braudaway, "If one watermark is good, are more better?," in *Acoustics, Speech, and Signal Processing, 1999. Proceedings., 1999 IEEE International Conference on*, 1999, vol. 4, pp. 2067–2069.
- [4] L. Wang and M. Syue, "A Wavelet-based Multipurpose Watermarking for Image Authentication and Recovery," vol. 2, no. 4, pp. 100–108, 2013.
- [5] M. Schlaueg, D. Pröfrock, B. Zeibich, and E. Müller, "Dual watermarking for protection of rightful ownership and secure image authentication," in *Proceedings of the 4th ACM international workshop on Contents protection and security - MCPS '06*, 2006, p. 59.
- [6] S.-W. Moon, H.-D. Kim, J. Lee, and H.-K. Lee, "Dual video watermarking for CCL protection and manipulation detection," *2012 IEEE Int. Symp. Circuits Syst.*, pp. 1420–1423, May 2012.
- [7] M. Schlaueg, D. Pröfrock, T. Palfner, and E. Müller, "Quantization-based semi-fragile public-key watermarking for secure image authentication," in *Optics & Photonics 2005*, 2005, p. 591506.
- [8] R. Kaur and G. S. Brar, "REDUCTION OF BLOCKING COMPRESSION ARTIFACTS."
- [9] C. Zhang, L. L. Cheng, Z. Qiu, and L.-M. Cheng, "Multipurpose watermarking based on multiscale curvelet transform," *Inf. Forensics Secur. IEEE Trans.*, vol. 3, no. 4, pp. 611–619, 2008.

- [10] Y. Jun, C. Guo-Hua, and Z. Yi-jia, "A practical multipurpose color image watermarking algorithm for copyright protection and image authentication," in *Digital Telecommunications*, 2006. *ICDT'06. International Conference on*, 2006, p. 72.
- [11] M. Habib, S. Sarhan, and L. Rajab, "A Robust-Fragile Dual Watermarking System in the DCT Domain," in *Knowledge-Based Intelligent Information and Engineering Systems*. Springer, 2005, pp. 548–553.
- [12] C.-S. Lu and H.-Y. M. Liao, "Multipurpose watermarking for image authentication and protection," *Image Process. IEEE Trans.*, vol. 10, no. 10, pp. 1579–1592, 2001.
- [13] H. Shen and B. Chen, "From single watermark to dual watermark: A new approach for image watermarking," *Comput. Electr. Eng.*, vol. 38, no. 5, pp. 1310–1324, Sep. 2012.
- [14] C.-S. Lu, S.-K. Huang, C.-J. Sze, and H.-Y. M. Liao, "Cocktail watermarking for digital image protection," *Multimedia, IEEE Trans.*, vol. 2, no. 4, pp. 209–224, 2000.
- [15] M. Kutter, "Watermarking resistance to translation, rotation, and scaling," in *Photonics East (ISAM, VVDC, IEMB)*, 1999, pp. 423–431.
- [16] S. Craver, N. Memon, B.-L. Yeo, and M. M. Yeung, "Resolving rightful ownerships with invisible watermarking techniques: Limitations, attacks, and implications," *Sel. Areas Commun. IEEE J.*, vol. 16, no. 4, pp. 573–586, 1998.
- [17] G. Xie and H. Shen, "Toward improved wavelet-based watermarking using the pixel-wise masking model," in *Image Processing, 2005. ICIP 2005. IEEE International Conference on*, 2005, vol. 1, pp. I–689.
- [18] X. I. E. Gui and S. Hong, "A new fusion based blind logo-watermarking algorithm," *IEICE Trans. Inf. Syst.*, vol. 89, no. 3, pp. 1173–1180, 2006.
- [19] F. Deguillaume, S. Voloshynovskiy, and T. Pun, "Secure hybrid robust watermarking resistant against tampering and copy attack," *Signal Processing*, vol. 83, no. 10, pp. 2133–2170, 2003.
- [20] S. Dadkhah, A. A. Manaf, and S. Sadeghi, "Efficient image authentication and tamper localization algorithm using active watermarking," in *Bio-inspiring Cyber Security and Cloud Services: Trends and Innovations*, Springer, 2014, pp. 115–148.
- [21] X. Xin, "A Singular-Value-Based Semi-Fragile Watermarking Scheme for Image Content Authentication with Tampering Localization," *J. Vis. Commun. Image Represent.*, 2010.
- [22] Y.-P. Lee, J.-C. Lee, W.-K. Chen, K.-C. Chang, J. Su, and C.-P. Chang, "High-payload image hiding with quality recovery using tri-way pixel-value differencing," *Inf. Sci. (Ny)*, vol. 191, pp. 214–225, 2012.
- [23] A. Al-Haj, "Combined DWT-DCT digital image watermarking," *J. Comput. Sci.*, vol. 3, no. 9, pp. 740–746, 2007.