International Journal of Innovative Computing, Information and Control
Volume **8**, Number **7(B)**, July **2012**

ICIC International ©2012 ISSN 1349-4198
pp. 5067–5081

A NEW FUZZY PERFORMANCE MODELING FOR EVALUATING THE TRADE-OFF AMONG ROBUSTNESS, QUALITY AND CAPACITY IN WATERMARKING ALGORITHMS

Mir Shahriar Emami[1], Ghazali Bin Sulong[1] and Salbiah Binti Seliman[2]

[1]Department of Computer Graphics and Multimedia
Faculty of Computer Science and Information Systems
[2]Department of Management
Faculty of Management and Human Resource Development
Universiti Teknologi Malaysia
81310, Skudai, Johor, Malaysia
shemami85@yahoo.com

Received May 2011; revised September 2011

Abstract. *There are several digital watermarking metrics proposed by researchers. These metrics can determine the robustness and the imperceptibility of watermarking schemes discretely. Here, there is a lack of an effective strategy to evaluate the balanced trade-off between these requirements. Meanwhile, it is hardly possible to determine crisp thresholds to limit the acceptable and unacceptable boundaries for robustness and imperceptibility. Hence, it is difficult to obtain an accurate mathematical model in order to evaluate the degree of trade-off between watermarking requirements. Thus, it is most advantageous to adopt the fuzzy-based model to fulfill this need. This paper develops a fuzzy inference system (FIS) effectively for exploring the performance trade-off among watermarking performance requirements. We implemented this technique to evaluate EISB (Enhanced Intermediate Significant Bit) watermarking scheme. We also focused on different intensities of Reset Removal Attack which were less considered before, by other researchers. Two main contributions of this paper are the performance fuzzy model itself, and the performance analysis of this model which was carried out and confirmed by results via simulation.*

Keywords: Watermarking, Performance measurement, Fuzzy, ISB, EISB, Trade-off, Robustness, Imperceptibility

1. **Introduction.** Free access multimedia communication through the Internet provides opportunities for piracy of digital multimedia intellectual properties. Therefore, the commercial demand for digital watermarking has been increasing. In order to meet this demand, since the last decade, researchers have been challenged with the introduction of many digital watermarking techniques, and in the coming decades, the challenge for more advanced techniques will be more intense.

A digital watermark is an ownership identification message in the form of a pattern of bits which is embedded into digital media during the embedding process. This watermark can be extracted through the extracting procedure in order to identify the ownership of the multimedia object. Unfortunately, the embedding process normally degrades the image quality. Thus, the visible imperceptibility (quality) of a watermarking algorithm should be seriously given attention. Moreover, the watermarking algorithm must be robust and able to resist against intentional and unintentional attacks [1,7,32]. Otherwise, embedded owner information hidden in the watermarked multimedia content can easily be detected and destroyed or replaced by malicious users or some software tools intentionally or unintentionally. Furthermore, a high-embedding capacity is always considered

in watermarking schemes. Consequently, these three basic requirements namely, the imperceptibility, the robustness and the capacity have to be fulfilled in order to satisfy the performance of any digital watermarking scheme. For this reason, researchers have applied several performance metrics, for example in [1,4,9,10,14,25,26,28-30,35,37,42], in order to evaluate to what extent the watermarking scheme satisfies above requirements. However, there is a trade-off among these requirements [22,45,47].

According to the authors' recent research in [38], this trade-off can be measured and represented based on degrees. However, not all of the watermarking metrics gave substantial discretion to determine degree of the trade-off among these requirements because it is hardly possible to determine crisp margins for mentioned requirements to define the levels of acceptability and unacceptability. On the other hand, both the density distribution in a host image and the watermarking attack mechanisms are often nonlinear or unknown. Hence, it is difficult to construct an accurate mathematical model with the purpose of evaluating the degree of the balanced trade-off among the mentioned requirements.

Meanwhile, a convenient configuration of a watermarking scheme can result in a balanced trade-off among these requirements. However, prior to achieving this goal, there must be a technique used to assess the trade-off among these requirements in any watermarking scheme. Unfortunately, no effective strategy has been reported so far.

To fulfill above needs, this paper proposes a fuzzy inference system (FIS) to estimate both the qualitative and the quantitative measures of this trade-off. This FIS can provide a method to choose the optimal configuration of a known watermarking algorithm which balances a trade-off among robustness, quality and capacity requirements.

Fuzzy inference can be defined as the procedure of formulating the mapping from a set of input data to a set of output data based on fuzzy logic. In general, an FIS modeling is described by establishing IF THEN rules using experimental data. An FIS comprises of fuzzy sets and fuzzy operations. A fuzzy set A in a universe discourse S is described by a membership function $\mu(s)$ which associates each element (s) in S with a real number in the interval I such that $I \in [0, 1]$. Fuzzy inference process comprises of five main parts:

- Fuzzification of the input variables
- Application of the fuzzy operator in the antecedent
- Implication from the antecedent to the consequent
- Aggregation of the consequents across the rules
- Defuzzification

In order to evaluate the proposed FIS, we used Matlab R2010 fuzzy logic toolbox environment. We obtained the test results on bit-plane algorithms using Ms Excel 2010 and Matlab R2010. By providing a balanced trade-off among robustness, imperceptibility and capacity, the experiments revealed that the 3rd and 4th bit-plane ISB algorithms were the most superior of all ISB watermarking algorithms.

2. **Problem Statement.** Researchers have employed several metrics [1,2,4,5,9,10,25,26, 33,34,36,44] to evaluate the performance of watermarking requirements including quality (imperceptibility), robustness and capacity. However, these requirements always conflict one another [2-4,30]. Most researchers implicitly or explicitly emphasize that there is a trade-off among these requirements, for example in [4,8,22,23,30,35,43,49]. Although they emphasized about the existence of this trade-off and attempted to propose a new algorithm to fulfill the optimal situation, they failed to measure this trade-off by means of an exact method. The authors in [38] introduced a threshold-based method to evaluate this trade-off. They, for the first time, stated the performance trade-off regarding watermarking schemes with a degree ranging from 0 to 1. Although the threshold-based method is the first technique to measure this performance trade-off, it is not accurate

enough because many of the watermarking performance factors have uncertain and imprecise values. Therefore, determining an optimal threshold value is extremely difficult. For example, coupling a strict threshold value with an imperceptibility metric, such as PSNR (Peak Signal to Noise), with the purpose of evaluating the visible imperceptibility of a watermarked image, cannot be accurate because there are no precise boundaries for this requirement. In other words, evaluating the watermarking performance requirements and measuring the trade-off among them are not a matter of denial or affirmation, but rather a matter of degree. Consequently, new approaches should emerge to evaluate the trade-off among quality, robustness and capacity in order to evaluate the performance of any watermarking scheme. Now the question is: Is it possible to propose a method to measure the balanced trade-off reasonably among imperceptibility, robustness and embedding capacity in watermarking techniques?

3. **Proposed Scheme.**

As mentioned earlier, in any digital watermarking scheme, several metrics are used in order to measure the performance of a watermarking scheme. Imperceptibility, robustness and embedding capacity are the most important watermarking performance requirements. Unfortunately, the mentioned requirements are often in a trade-off. Meanwhile, a convenient configuration can bring about a balanced situation among them but before achieving this goal, there must be a method to measure the trade-off among these requirements in any watermarking scheme.

In this section we proposed a three-input two-rule fuzzy model to measure this trade-off. In this study to simplify the analysis procedures, we proposed a straightforward image strip as a host image and a semi text-based watermark pattern as the owner identification information. In addition, in order to select a bit-plane algorithm which provides a balanced trade-off among robustness, imperceptibility and capacity, five bit-plane algorithms were evaluated based on the proposed method.

The novelty of the proposed approach is in twofold. Firstly, this approach introduced a fuzzy model to assess the trade-off among robustness and imperceptibility requirements in a watermarking scheme. In the proposed approach, imperceptibility *before attack*, robustness and perceptibility *after attack* were considered as fuzzy sets as it is hardly possible to define crisp margins when the density distribution regarding the watermarking attack as well as the target host image is often nonlinear, complex or unknown. Secondly, an experimental technique utilizing the proposed fuzzy model was proposed to estimate degree of the performance balanced trade-off in spatial domain watermarking algorithms.

3.1. **Methodology.**

Watermarking performance metrics are greatly affected by several uncertain factors such as host image data distribution, watermark information, method of watermarking and attack mechanisms. Furthermore, the definition of acceptable boundaries for these metrics cannot be precise because they are fuzzy quantities. In this section, we propose a fuzzy measurement model with the aim of measuring the trade-off among the performance requirements. Figure 1 graphically shows the proposed fuzzy performance model. This figure shows the input and output variables, and also the two rules of the proposed model.

3.2. **Proposed fuzzy performance model.**

In this section we proposed an FIS to evaluate degree of the performance balanced trade-off among watermarking performance requirements. All the input and output variables in the proposed FIS are fuzzy sets so we used the Mamdani Fuzzy Rule Based (MFRB) method as shown in Table 1.

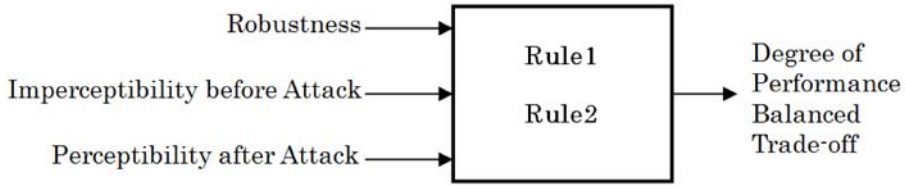

FIGURE 1. Proposed fuzzy-based measurement model to measure degree of the balanced trade-off among watermarking performance requirements

TABLE 1. The characteristics of the proposed FIS

Name of Characteristics	Type of Characteristics
Input/Output Variables	B, R, A, T, PBT
Type of the Rule-base	Mamdani
Number of the rules	2
Type of MFs in antecedent	Zimmermann Straight Line
Type of MFs in consequent	Zimmermann Straight Line
"And" method ($\wedge$)	Min
"OR" method ($\vee$)	Max
Implication method	AND
Aggregation method	OR
Defuzzification method	MOM (Mean Of Maximum)

3.2.1. *Fuzzification of the input variables.* In the proposed model, visible imperceptibility of the host image *before attack after watermarking* (B), visible perceptibility of the host image *after attack* (A) and robustness *after attack* (R) have been considered as three fuzzy input variables. The fuzzy set T which is the output variable, is the degree of the trade-off among watermarking performance requirements.

We adapted Zimmermann's straight-line shaped membership function [40] to represent these variables, because firstly, the straight line shaped membership function is the primary strategy to construct the fuzzy membership functions and secondly, the fuzzy numbers B, R, A, T can be adapted to this shape. The following propositions represent the degree of the membership of any element of both input vectors (B, A, R) and output vector (T).

Proposition 3.1. *Let B denote fuzzy set of visible imperceptibility of the host image before attack after watermarking such that $B = \{(b, \mu_B(b)) \,|b \in [\alpha, \beta], \mu_B(b) \in I\}$ where $\mu_B(b)$ is considered as a straight line. The values of α and β will be obtained in Section 3.2.5.*

Proposition 3.2. *Let A denote fuzzy set of visible perceptibility of the host image after attack such that $A = \{(a, \mu_A(a)) \,|a \in [\alpha, \beta], \mu_A(a) \in I\}$ where $\mu_A(a)$ is considered as a straight line. The values of α and β will be obtained in Section 3.2.5.*

Proposition 3.3. *Let $I \in [0, 1]$ denote the universe of a discourse and R denote fuzzy sets of robustness after attack such that $R = \{(r, \mu_R(r)) \,|r, \mu_R(r) \in I\}$ where $\mu_R(r)$ is considered as a straight line.*

Proposition 3.4. *Let $I \in [0, 1]$ denote the universe of a discourse and T denote fuzzy set regarding degree of watermarking performance trade-off such that $T = \{(z, \mu_T(z))|z, \mu_T(z) \in I\}$ where $\mu_T(z)$ is considered as a straight line.*

3.2.2. *Application of the fuzzy operators.* Let us consider the preliminary definitions of fuzzy 'AND' and 'OR' operators in Definitions 3.1 and 3.2.

Definition 3.1. *Let P and Q represent two fuzzy sets, and, $\mu_P(x)$ and $\mu_Q(x)$ indicate their membership functions respectively. Now let fuzzy logical connective 'AND' be defined as:* $\mu_P(x) \wedge \mu_Q(x) = \mu_{P\cap Q}(x) = \min\{\mu_P(x), \mu_Q(x)\}$.

Definition 3.2. *Let P and Q represent two fuzzy sets, and, $\mu_P(x)$ and $\mu_Q(x)$ indicate their membership functions respectively. Now let fuzzy logical connective 'OR' be defined as:* $\mu_P(x) \vee \mu_Q(x) = \mu_{P\cup Q}(x) = \max\{\mu_P(x), \mu_Q(x)\}$.

3.2.3. *Implication and aggregation.* Here, we proposed Rule 1, R1, and Rule 2, R2, based on the MFRB method, and OR function for aggregation.

$$\text{R1}: \text{ If } [b_1 \text{ is Imperceptible}] \wedge [r_1 \text{ is Strong}] \text{ Then } [z_1 \text{ is Balance}] \tag{1}$$

$$\text{R2}: \text{ If } [b_1 \text{ is Imperceptible}] \wedge [a_1 \text{ is Perceptible}] \text{ Then } [z_1 \text{ is Balance}] \tag{2}$$

3.2.4. *Defuzzification.* This stage transformed the final integrated fuzzy set to a crisp value as the degree of performance balanced trade-off or PBT in short. For the defuzzification strategy, in order to calculate the PBT, we used the MOM (Mean Of Maximum) method (Equation (3)). This method has been widely used in defuzzification strategy. This method calculates the average of the maximizing z i.e. z', in which the membership function approaches a maximum μ i.e. μ^*, so $z' = \{z|\mu(z) = \mu^*\}$.

$$PBT = \frac{\int_{z'} z dz}{\int_{z'} dz} \tag{3}$$

3.2.5. *Membership functions.* As mentioned earlier, in fuzzy modeling, researchers mainly utilize linear membership functions which are conceptually straightforward, low in complexity and obvious in interpretation [39]. Therefore, these membership functions are used in many applications. Zimmermann [40] and later on, Sakawa [41] proposed a simple and practical linear membership function. In this paper, the Zimmermann's linear membership function plays a key role to represent the characteristics of input and output fuzzy variables. Zimmermann's membership function is shown in Equation (4).

$$\mu(x_i) = \begin{cases} 1 & \text{for} \quad x_i \leq \alpha \\ 1 - \frac{x_i - \alpha}{\beta} & \text{for} \quad \alpha \prec x_i \leq \alpha + \beta \\ 0 & \text{for} \quad x_i \succ \alpha + \beta \end{cases} \tag{4}$$

where $\mu(x_i)$ denotes the membership function, $x_i \in [\alpha, \beta]$ represents the ith element of the universe of discourse X. Then the fuzzy set A can be represented as bellow (Equation (5)).

$$A = \{(x_i, \mu(x_i)|x_i \in X\}) \tag{5}$$

With the purpose of evaluating the robustness (R), in spite of the fact that the NCC (Normalized Cross Correlation) metric is generally used by many researchers [10-14] to measure the degree of similarity between the extracted watermark and the original one, we chose this metric because it is computed in spatial domain [24] (the domain which we used in our testing platform). This metric provides a quantitative estimation for the watermark quality after extraction (W) with reference to the original watermark (W'). The NCC is given in Equation (6).

$$NCC = \frac{\sum_x \sum_y \left(W_{x,y} \times W'_{x,y}\right)}{\sum_x \sum_y \left(W_{x,y}\right)^2} \tag{6}$$

According to M. Xuan and J. Jiang [14], if the NCC value is greater than 0.6, a watermarking algorithm can be considered robust. If the NCC is about 0.75 it is considered robust by other researchers [19-21]. According to the authors work in [38], if the NCC is

greater than or equal to 0.7 it is considered as robust. In actual fact, the value about 1.0 is the desirable value for the NCC. Hence, we considered $NCC \in [0,1]$. Here, we adapted Equation (4) as the membership function regarding fuzzy set R, $\mu_R(r)$, with a growing slope. This can be represented as Equation (7),

$$\mu_R(r) = \begin{cases} 0 & \text{for} \quad r \leq \alpha' \\ \frac{r-\alpha'}{\beta'} & \text{for} \quad \alpha' \prec r \leq \alpha' + \beta' \\ 1 & \text{for} \quad r \succ \alpha' + \beta' \end{cases} \tag{7}$$

where $r \in [\alpha', \beta']$.

As the $NCC \in [0,1]$ then

$$\mu_R(r) = r \quad \text{for} \quad r \in [0,1] \tag{8}$$

To mathematically represent the quality of the watermarked image after the embedding process, i.e., the difference between the original image (I) and the watermarked image (K), researchers [9,10,17,20,27-30] have widely used the $PSNR$ measure which is the simplest and still the most practical metric. This measure is given in Equation (9),

$$PSNR = 10 \times \log_{10}\left(\frac{MAX_I^2}{MSE}\right) \tag{9}$$

where MAX_I is the maximum pixel value of I and MSE is the mean square error as is given in Equation (10),

$$MSE = \frac{1}{m \times n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} (I_{ij} - K_{ij})^2 \tag{10}$$

where I_{ij} is the value of the pixel (i,j) of the host image, and K_{ij} is the pixel (i,j) value of the watermarked image. As the host image was an 8-bit grayscale image, so $MAX_I = 2^8 - 1 = 255$.

Here, the imperceptibility metric is considered for both *before attack* and *after attack* situations. Despite the fact that the $PSNR$ is an imperceptibility metric, there is no standard value for the measurement. However, some researchers suggested 34 dB (decibel) [15,16], while others proposed 30 dB [10,17,18,38]. In this study we considered the range the $PSNR$ between 0 and 50 (i.e., $\alpha = 0$ and $\beta = 50$) so $a, b \in [0,50]$.

Adapting Equation (4), the membership function regarding fuzzy set B, $\mu_B(b)$, with a growing slope can be represented as Equation (11),

$$\mu_B(b) = \begin{cases} 0 & \text{for} \quad b \leq \alpha \\ \frac{b-\alpha}{\beta} & \text{for} \quad \alpha \prec b \leq \alpha + \beta \\ 1 & \text{for} \quad b \succ \alpha + \beta \end{cases} \tag{11}$$

where $b \in [\alpha, \beta]$.

Then

$$\mu_B(b) = \frac{b}{\beta} \quad \text{for} \quad b \in [0,50] \tag{12}$$

Again, adapting Equation (4), the membership function regarding fuzzy set A, $\mu_A(a)$, maintaining a negative slope can be represented as Equation (13),

$$\mu_A(a) = \begin{cases} 1 & \text{for} \quad a \leq \alpha \\ 1 - \frac{a-\alpha}{\beta} & \text{for} \quad \alpha \prec a \leq \alpha + \beta \\ 0 & \text{for} \quad a \succ \alpha + \beta \end{cases} \tag{13}$$

where $a \in [\alpha, \beta]$.

Then

$$\mu_A(a) = 1 - \frac{a}{\beta} \quad \text{for} \quad a \in [0, 50] \tag{14}$$

Once again, adapting Equation (4), the membership function regarding fuzzy set T, $\mu_T(z)$, with a growing slope can be represented as Equation (15),

$$\mu_T(z) = \begin{cases} 0 & \text{for} \quad z \leq \alpha'' \\ \frac{z-\alpha''}{\beta''} & \text{for} \quad \alpha'' \prec z \leq \alpha'' + \beta'' \\ 1 & \text{for} \quad z \succ \alpha'' + \beta'' \end{cases} \tag{15}$$

where $z \in [\alpha'', \beta'']$.

The authors in [38] found that the watermarking performance balanced trade-off can be stated based on degrees between 0 and 1. Hence,

$$\mu_T(z) = z \quad \text{for} \quad z \in [0, 1] \tag{16}$$

Furthermore, usage capacity (C) is always considered in watermarking schemes and of course more capacity is always more desirable. Equation (17) shows the maximum embedding capacity, C_{Max}, while m bit per byte is used to embed the watermark data within m bit-planes of an n-bit gray-scale host image in a spatial domain watermarking scheme.

$$C_{Max} = \frac{m}{n} \times \frac{SizeOfHostImage}{SizeOfWatermark} \tag{17}$$

For an 8-bit gray-scale image when one bit-plane is used for watermark embedding, the embedding capacity must be considered less than or equal to the value of $\frac{SizeOfHostImage}{8 \times SizeOfWatermark}$. In addition, we considered the range between 0 and 1 for the embedding capacity. We mapped this range to the range of 0 to 10. Therefore, the universe of discourse is $C \in [0, 10]$.

3.3. **Proposed prerequisites and experimental settings.** Pseudorandom bits embedding watermarks have been used by many researchers [48-51]. However, as text watermarks normally are comprised of name of owner, address, etc., so only capital letters and ten digits plus space character are adequate to make an ownership proof statement. Thus, we proposed a semi-text based statement which was approximated by the ASCII binary codes of 26 capital letters, 10 digits and space character. Table 2 shows the number of ones and zeros in ASCII binary codes of capital letters, ten digits and space character. From this table, it can be understood that almost 60% of these ASCII binary codes are 0 and obviously the remaining 40% are 1.

Hence, we proposed a watermark bit stream pattern as $W_n = (11010011)^{n/16}$ $(011011\ 10)^{n/16}$ in which approximately 62% of watermark bits are 0 and 38% of them are 1. For example, if the length of watermark is 16 (i.e., $n = 16$) then the watermark bit stream would be W_{16} = "1101001101101110". Therefore, the two adjacent watermark pixel values for W_{16} are 211 and 110.

Based on the above watermark bit stream pattern, ten different watermarks were considered in the experiments, viz: W_{512}, W_{448}, W_{400}, W_{352}, W_{304}, W_{256}, W_{192}, W_{144}, W_{96} and W_{48} for ten different usage capacities of the host image, viz: 12.50%, 11.25%, 10.00%, 8.75%, 7.50%, 6.25%, 5.00%, 3.75%, 2.50% and 1.25% respectively.

For the host image, as the uniform areas of an image are much more sensitive for watermark embedding than edge areas, here, for more accuracy and also more simplicity of the performance analysis, an 8-bit grayscale image strip of 1×512 size was proposed as the host image. Figure 2 depicts its histogram.

TABLE 2. The number of 1s and 0s in the capital letters and the ten digits ASCII binary codes

Charachter	ASCII	Binary	Number of 0s	Number of 1s
Space	32	00010000	7	1
0	48	00110000	6	2
1	49	00110001	5	3
2	50	00110010	5	3
3	51	00110011	4	4
4	52	00110100	5	3
5	53	00110110	4	4
6	54	00110110	4	4
7	55	00110111	3	5
8	56	00111000	5	3
9	57	00111001	4	4
A	65	01000001	6	2
B	66	01000010	6	2
C	67	01000011	5	3
D	68	01000100	6	2
E	69	01000101	5	3
F	70	01000110	5	3
G	71	01000111	4	4
H	72	01001000	6	2
I	73	01001001	5	3
J	74	01001010	5	3
K	75	01001011	4	4
L	76	01001100	5	3
M	77	01001101	4	4
N	78	01001110	4	4
O	79	01001111	3	5
P	80	01010000	6	2
Q	81	01010001	5	3
R	82	01010010	5	3
S	83	01010011	4	4
T	84	01010100	5	3
U	85	01010101	4	4
V	86	01010110	4	4
W	87	01010111	3	5
X	88	01011000	5	3
Y	89	01011001	4	4
Z	90	01011010	4	4

This study employed the Enhanced ISB Watermarking Algorithm (EISB) [10,38] as the testing platform. In order to embed a bit of embedding watermark in EISB approach, the closest value to the original pixel value, which delivers the watermark bit, is chosen. For this reason, predefined sub-ranges as is shown in Table 3 should be available in advance.

As mentioned earlier, this study attempted to measure degree of the balanced trade-off among robustness, quality and capacity in bit-plane watermarking scheme. In this sense, ten different usage capacities of the host image, viz: 12.50%, 11.25%, 10.00%, 8.75%, 7.50%, 6.25%, 5.00%, 3.75%, 2.50% and 1.25% were used to embed the watermark.

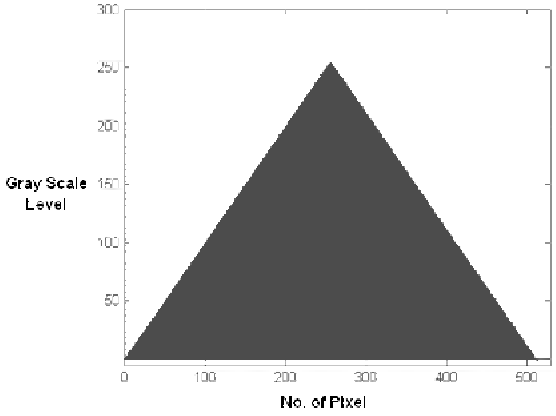

FIGURE 2. Subject host image histogram

TABLE 3. Sub-ranges in EISB watermarking scheme

Bit-plane	Sub-Ranges in which Embedding Position has Value of 0	Sub-Ranges in which Embedding Position has Value of 1
$1^{st}(MSB)$	[0..127]	[128..255]
2^{nd}	[0..63][128..191]	[64..127][192..255]
3^{rd}	[0..31][64..95] ... [192..223]	[32..63][96..127] ... [224..255]
4^{th}	[0..15][32..47] ... [224..239]	[16..31][48..63] ... [240..255]
5^{th}	[0..7][16..23] ... [240..247]	[8..15][24..31] ... [248..255]
$8^{th}(LSB)$	[0][2][4][6][8] ... [254]	[1][3][5][7][9][11] ... [255]

Referring to Equation (17), in a bit-plane algorithm 12.5% is the maximum embedding capacity, i.e., 100% (1.0) when one bit per byte is used for watermark embedding in a gray-scale host image. Here, let us consider the bit-plane usage capacity instead of the host image usage capacity. Thus, the usage capacities in this study are 1.0, 0.9, 0.8, 0.7, 0.6, 0.5, 0.4, 0.3, 0.2 and 0.1 respectively.

Correspondingly, ten intensities of Reset Removal attack [38], viz: 10%, 20%, 30%, 100% were used to simulate the attacks on the watermarked image. For example, in a 10% Reset Removal attack, a maximum of 10% of the embedded watermark bits can be replaced by zero values (Reset). In addition, for the worst case scenario, it was presumed that the attacker had a prior knowledge of the starting point of the embedded watermark.

4. **Experimental Results and Discussions.** In this section, we discuss the results of our experiments on the five mentioned bit-plane algorithms under Reset Removal attack in which the intensity of the attack varied between 10% and 100% (0.1 to 1.0). Moreover, the usage capacity was changed between 10% and 100% (0.1 to 1.0) under each intensity of attack. In addition, Table 4 illustrates interpretation of the PBT degree regarding the watermarking algorithms.

TABLE 4. The interpretations of the performance balanced trade-off

PBT Range	Interpretation
$PBT \leq 0.4$	LOW
$0.4 \prec PBT \prec 0.6$	MEDIUM (MED)
$PBT \geq 0.6$	HIGH

4.1. **Analysis of the results.** Figure 3 shows degree of the performance balanced trade-off regarding the five bit-plane algorithms using the proposed scheme. Figure 3(a) demonstrates that when the capacity of 0.1 was used, the degree of the balanced trade-off for the LSB algorithm under any intensity of attack were LOW (PBT = 0.20). In contrast, the 2nd and 3rd bit-plane algorithms behaved highly balanced but the 4th bit-plane algorithm had a MEDIUM balanced degree in average. Figure 3(b) illustrates that the LSB algorithm still had a LOW balanced degree when usage capacity was 0.2. In contrast, the 2nd, 3rd and 4th bit-plane algorithms had HIGH balanced degrees. Figure 3(c) demonstrates that when the usage capacity was 0.3, the 5th bit-plane algorithm had a MEDIUM balanced degree but LSB algorithm still had a LOW balanced degree in average. Figures 3(d) and 3(e) show that when the usage capacity was between 0.4 and 0.5 the balanced degree in 2nd bit-plane algorithm suddenly dropped but the 3rd and 4th bit-plane algorithms still had MEDIUM balanced degree in average. Figures 3(f), 3(g) and 3(h) illustrate that the 3rd, 4th and 5th bit-plane algorithms had MEDIUM balanced degree in average when the usage capacity was between 0.6 and 0.8. Finally, Figures 3(i) and 3(k) demonstrate that when the usage capacity was more than 0.8 the 4th and 5th bit-plane algorithms had MEDIUM balanced degree in average. Figure 3 also revealed that both the 3rd and 2nd bit-plane algorithms had LOW balanced degree. Thus, this figure illustrates that the 4th bit-plane algorithm was more stable in comparison with other bit-plane algorithms. Table 5 summarizes the above discussion.

TABLE 5. The PBT interpretations of five bit-plane watermarking algorithms

	Capacity									
Algorithm	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0
LSB	LOW	LOW	LOW	LOW	LOW	LOW	LOW	LOW	LOW	LOW
5th	LOW	LOW	LOW	LOW	LOW	LOW	LOW	MED	MED	MED
4th	HIGH	MED	MED	MED	MED	MED	MED	MED	MED	MED
3rd	HIGH	HIGH	MED	MED	MED	MED	MED	MED	MED	LOW
2nd	HIGH	HIGH	HIGH	LOW	LOW	LOW	LOW	LOW	LOW	LOW

4.2. **Discussions.** Table 6 shows different watermarking performance evaluation metrics and their application. This table shows that NCC, Correlation Factor (ρ), BCR and NMSE measure only the robustness of watermarking schemes. Similarly, Table 6 shows that PSNR, wPSNR, SIMM, and Watson JD evaluate only the quality of the watermarked image in comparison with the corresponding host image. Evidently, none of the mentioned methods measure the trade-off among all three watermarking main requirements including: robustness, imperceptibility and usage capacity. Meanwhile, as said earlier, these three requirements are strictly in conflict. For example, in spatial domain watermarking, the use of higher bit-planes increases the robustness but decreases the imperceptibility. Another example is when a watermarking scheme uses the blocking strategy. For example, some watermarking schemes use the blocking strategy in order to increase the robustness but this brings about a drastic decrease in the embedding capacity. Hence, there is a need to measure the trade-off among all these three requirements and find the best situation in which a balanced trade-off among these requirements can be obtained. The authors in [38] proposed a technique to measure this trade-off. However, this technique was based on predefined crisp margins for these requirements. These crisp margins could not be accurate as it was hardly possible to determine crisp thresholds to limit the acceptable and unacceptable boundaries for these requirements. In contrast, by defining imperceptibility

and robustness as fuzzy sets, the proposed method could obtain better results than the methods based on crisp margins.

TABLE 6. Watermarking performance evaluation metrics

Watermarking Performance Evaluation Metric	Robustness	Imperceptibility	Trade-off
NCC [11-15]	×		
PSNR [10,11,18,21,28,29]		×	
Correlation Factor (ρ) [1,22,55]	×		
Watson JND [61]		×	
NMSE [56-58]	×		
SSIM [45,64]		×	
BCR [43,59,60]	×		
wPSNR [32,47,61-63]		×	
Emami et al. [39]			×
Proposed Scheme			×

5. **Conclusions.** We have constructed a fuzzy model to evaluate the trade-off among watermarking requirements. We also have proposed an experimental technique utilizing the proposed model to estimate the balanced performance trade-off in EISB watermarking scheme. The proposed technique revealed that three factors including imperceptibility *after watermarking before attack*, perceptibility *after attack* and robustness *after attack* should all be considered together in order to make a balanced trade-off among quality, robustness and capacity. We successfully tested the proposed method on the EISB watermarking scheme under a severe attack. The results of the experimental investigations on the proposed method illustrated that if after attack the NCC seriously drops, the extracted watermark can no longer be applied for ownership identification of the watermarked image. However, a low PSNR after attack can compensate this drawback, but if the PSNR after attack remains high and the NCC remains low, the watermarked image has a strong potential for misuse or piracy. The results also revealed that the 3rd and the 4th bit-plane algorithms, in average, have managed a medium degree of balanced performance trade-off among robustness, imperceptibility and capacity. However, the 4th bit-plane algorithm was more stable in comparison with the 3rd bit-plane algorithm.

Acknowledgment. This work was supported by Ministry of Higher Education (MOHE) to UTMVicubelab at Department of Computer Graphics and Multimedia, Faculty of Computer Science and Information System, Universiti Teknologi Malaysia (UTM), under the Research University Grant Scheme (RUGS) with Reference No. Q.J130000.7128.01J12 for providing financial support of this research. The authors thank UTM for the award

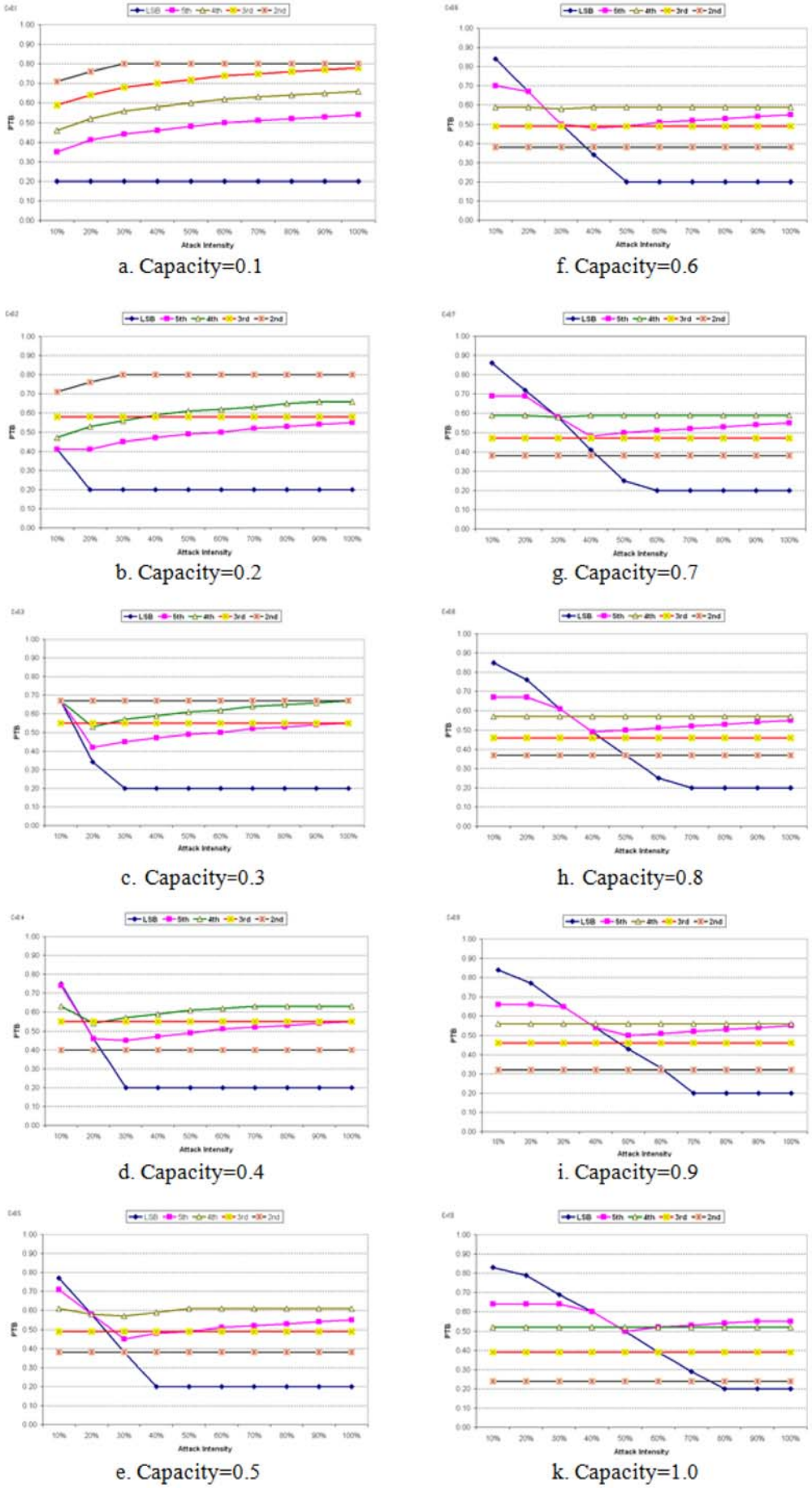

FIGURE 3. Watermarking performance trade-off balanced degree

of International Doctoral Fellowship (IDF) to Mir Shahriar Emami. The authors also gratefully acknowledge the suggestions made by anonymous reviewers that have enhanced greatly the quality of the manuscript.

REFERENCES

[1] H. M. Al-Otum and N. A. Samara, A robust blind color image watermarking based on wavelet-tree bit host difference selection, *Signal Processing*, vol.90, no.3, pp.2498-2512, 2010.

[2] R. B. Wolfgang, C. I. Podilchuk and E. J. Delp, Perceptual watermarks for digital images and video, *Proc. of the IEEE*, vol.87, no.7, pp.1108-1126, 1999.

[3] J. Cox, M. L. Miller and J. A. Bloom, *Digital Watermarking*, Morgan Kaufmann Publishers, 2001.

[4] S. Fazli and G. Khodaverdi, Trade-off between imperceptibility and robustness of LSB watermarking using SSIM quality metrics, *Proc. of IEEE the 2nd International Conference on Machine Vision*, 2009.

[5] N. Wu and M. Hwang, Data hiding: Current status and key issues, *International Journal of Network Security*, vol.4, no.1, pp.1-9, 2007.

[6] M. Ozturk, A. Akan and Y. Cekic, A robust image watermarking in the joint time-frequency domain, *EURASIP Journal on Advances in Signal Processing*, vol.2010, pp.1-9, 2010.

[7] J. J. K. O'Ruanaidh and T. Pun, Rotation scale and translation invariant digital watermarking, *Proc. of IEEE International Conference on Image Processing*, pp.536-538, 1997.

[8] V. Licks and R. Jordan, Geometric attacks on image watermarking systems, *IEEE MultiMedia*, vol.12, no.3, pp.68-78, 2005.

[9] A. M. Zeki and A. A. Manaf, Robust digital watermarking method based on bit-plane ranges, *Studies in Informatics and Control Journal*, Romania, 2007.

[10] A. M. Zeki and A. A. Manaf, A novel digital watermarking technique based on ISB (intermediate significant bit), *International Journal of Information Technology*, vol.5, no.3, pp.141-148, 2009.

[11] M. M. El-Ghoneimy, Coparison between two watermarking algorithms using DCT coefficient, and LSB replacement, *Journal of Theoretical and Applied Information Technology, JATIT*, pp.132-139, 2008.

[12] Q. Liu and Z. Ding, Spread spectrum watermark for color image, based on wavelet tree structure, *Proc. of International Conference on Computer Science and Software Engineering*, pp.692-695, 2008.

[13] M. B. Aliwa, T. El-Ahmady El-Tebely, M. M. Fahmy and M. El Said Naser, Robust digital watermarking based on falling-off-boundary in corners board-MSB-6 gray scale images, *International Journal of Computer Science and Network Security*, vol.9, no.8, pp.227-240, 2009.

[14] M. Xuan and J. Jiang, A novel watermarking algorithm in entropy coding based on image complexity analysis, *Proc. of International Conference on Multimedia Information Networking and Security*, pp.128-129, 2009.

[15] N. W. Cheung, Digital image watermarking in spacial and transform domain, *Proc. of TENCON*, pp.374-378, 2000.

[16] J. J. Eggers, J. K. Su and B. Girod, Robustness of a blind image watermarking scheme, *Proc. of IEEE International Conference on Image Processing*, Canada, pp.17-20, 2000.

[17] J. Bennour, J. L. Dugelay and F. Matta, Watermarking attack: BOWS contest, *Proc. of SPIE*, 2007.

[18] N. Wu, *A Study on Data Hiding for Gray-Level and Binary Images*, Master Thesis, Chaoyang University of Technology, Taiwan, 2004.

[19] S. S. Muhammad and Y. Dot, A watermarking scheme for digital images using multilevel wavelet composition, *Malaysian Journal of Computer Science*, vol.16, pp.24-36, 2003.

[20] K. Hameed, A. Mumtaz and S. A. M. Gilani, Digital image watermarking in the wavelet transform domain, *Proc. of WASET*, vol.13, pp.86-89, 2006.

[21] A. Al-Haj, Combined DWT-DCT digital image watermarking, *Journal of Computer Science*, vol.3, pp.740-746, 2007.

[22] V. Aslantas, An optimal robust digital image watermarking based on SVD using differential evolution algorithm, *Optics Communications*, vol.282, pp.769-777, 2009.

[23] N. R. Dasre, On watermarking in frequency domain, *Proc. of SPIE the 2nd International Conference on Digital Image Processing*, vol.7546, pp.1-6, 2010.

[24] J. Yoo, B. Choi and H. Choi, 1-D fast normalized cross-correlation using additions, *Digital Signal Processing*, vol.20, pp.1482-1493, 2010.

[25] J. Shieh, D. Lou and M. Chang, A semi-blind digital watermarking scheme based on singular value decomposition, *Computer Standards and Interfaces*, vol.28, pp.428-440, 2006.

[26] S. P. Maity and M. K. Kundu, Robust and blind spatial watermarking in digital image, *Proc. of the 3rd Indian Conference on Computer Vision, Graphics and Image Processing*, pp.388-393, 2002.
[27] W. Zhu, Z. Xiong and Y. Zhang, Multiresolution watermarking for images and video, *IEEE Transactions on Circuits and Systems for Video Technology*, vol.9, no.4, pp.545-550, 1999.
[28] M. Devapriya and K. Ramar, Statistical image watermarking in DWT with capacity improvement, *Global Journal of Computer Science and Technology*, vol.10, no.2, pp.20-24, 2010.
[29] E. E. Abdallah, A. B. Hamza and P. Bhattacharya, Video watermarking using wavelet transform and tensor algebra, *Signal, Image and Video Processing*, vol.4, no.2, pp.233-245, 2010.
[30] A. Cheddad, J. Condell, K. Curran and P. M. Kevitt, Digital image steganography: Survey and analysis of current methods, *Signal Processing*, vol.90, pp.727-752, 2010.
[31] S. Voloshynovskiy, S. Pereira, A. Herrigel, N. Baumgartner and T. Pun, Generalized watermarking attack based on watermark estimation and perceptual remodulation, *Proc. of SPIE the 12th Annual Symposium, Electronic Imaging 2000: Security and Watermarking of Multimedia Content II*, San Jose, CA, USA, vol.3971, pp.358-370, 2000.
[32] S. Voloshynovskiy, S. Pereira, V. Iquise and T. Pun, Attack modelling-towards a second generation watermarking benchmark, *Signal Processing*, vol.81, pp.1177-1214, 2001.
[33] D. Yan, R. Yand, Y. Yu and H. Xin, Blind digital image watermarking technique based on intermediate significant bit and discrete wavelet transform, *Proc. of IEEE International Conference on Computational Intelligence and Software Engineering*, pp.1-4, 2009.
[34] B. A. Mehemed, T. E. A. El-Tobely, M. M. Fahmy, M. E. L. Said Naser and M. H. A. El-Aziz, Robust digital watermarking based falling-off boundary in corners board-MSB-6 gray scale images, *International Journal of Computer Science and Network Security*, vol.9, no.8, pp.227-240, 2009.
[35] I. J. Cox, J. Kilian and T. Shamoon, Secure spread spectrum watermaking for multimedia, *IEEE Transactions on Image Processing*, vol.6, no.12, pp.1673-1687, 1997.
[36] C. Song, S. Sudirman, M. Merabti and D. Llewellyn-Jones, Analysis of digital image watermark attacks, *Proc. of IEEE the 7th Consumer Communications and Networking Conference*, pp.1-5, 2010.
[37] S. M. Perumal and V. Vijayakumar, A wavelet based digital watermarking method using thresholds on intermediate bit values, *International Journal of Computer Applications*, vol.15, no.3, 2011.
[38] M. S. Emami, G. B. Sulong and J. M. Zain, A new performance trade-off measurement technique for evaluating image watermarking schemes, *Communications in Computer and Information Science*, vol.179, pp.567-580, 2011.
[39] J. Kluska, Analytical methods in fuzzy modeling and control, *Studies in Fuzziness and Soft Computing*, 2009.
[40] H.-J. Zimmermann, Fuzzy programming and linear programming with several objective functions, *Fuzzy Sets and Systems*, vol.1, no.1, pp.45-55, 1978.
[41] M. Sakawa, Interactive computer programs for fuzzy linear programming with multiple objectives, *International Journal of Man-Machine Studies*, vol.18, no.5, pp.489-503, 1983.
[42] C.-C. Chang, C.-C. Lin and Y.-S. Hu, An SVD oriented watermark embedding scheme with high qualities for the restored images, *International Journal of Innovative Computing, Information and Control*, vol.3, no.3, pp.609-620, 2007.
[43] L.-D. Li, B.-L. Guo and J.-S. Pan, Robust image watermarking using feature based local invariant regions, *International Journal of Innovative Computing, Information and Control*, vol.4, no.8, pp.1977-1986, 2008.
[44] K. Seshadrinathan and A. C. Bovik, Unifying analysis of full reference image quality assessment, *Proc. of the 15th IEEE International Conference on Image Processing*, pp.1200-1203, 2008.
[45] K. Kim, J. Choi, S. Kim and J. Choi, A robust digital watermarking in geometric attacks, information optics and photonics technology, *Proc. of SPIE*, Bellingham, vol.5642, 2005.
[46] F. Autrusseau, P. L. Callet and A. Ninassi, A study of content based watermarking using an advanced HVS model, *Proc. of IEEE Intelligent Information Hiding and Multimedia Signal Processing*, pp.485-488, 2010.
[47] X. Zhao and A. T. S. Ho, An introduction to robust transform based image, *Intelligent Multimedia Analysis for Security Application, Studies in Computational Intelligence*, vol.282, pp.337-364, 2010.
[48] S. K. Amirgholipour and A. R. Naghsh-Nilchi, Robust digital image watermarking based on joint DWT-DCT, *International Journal of Digital Content Technology and Its Applications*, vol.3, no.2, pp.42-54, 2009.

[49] A. M. Kothari, A. C. Suthar and R. S. Gajre, Performance analysis of digital image watermarking technique-combined DWT-DCT over individual DWT, *International Journal of Advanced Engineering and Applications*, 2010.

[50] S. E. I. Baba, L. Z. Krikor, T. Arif and Z. Shaaban, Watermarking of digital images in frequency domain, *International Journal of Automation and Computing*, vol.7, no.1, pp.17-22, 2010.

[51] S. P. Kumar, K. Anusha and R. V. Ramana, A novel approach to enhance robustness in steganography using multiple watermark embedding algorithm, *International Journal of Soft Computing and Engineering*, vol.1, no.1, pp.50-56, 2011.

[52] H. Kamran, A. Mumtaz and S. A. M. Gilani, Digital image watermarking in the wavelet transform domain, *Proc. of WASET*, vol.13, pp.86-89, 2006.

[53] S. Ghannam and F. E. Z. Abou-Chadi, WPT versus WT for a robust watermarking technique, *International Journal of Computer Science and Network Security*, vol.9, no.1, pp.236-241, 2009.

[54] C. Jin, Z. Zhang, Y. Jiang, Z. Qu and C. Ma, A blind watermarking algorithm based on modular arithmetic in the frequency domain, *Advances and Innovations in Systems, Computing Sciences and Software Engineering*, pp.543-547, 2007.

[55] S. Ghannam and F. Abou-Chadi, Enhancing performance of image watermarks using wavelet packet, *Proc. of IEEE International Conference on Computer Engineering and Systems*, pp.83-87, 2008.

[56] S. Chu, L. C. Jain, H. Huang and J. Pan, Error-resilient triple-watermarking with multiple description coding, *Journal of Networks*, vol.5, no.3, pp.267-274, 2010.

[57] H. Huang, C. Chu and J. Pan, Genetic watermarking for copyright protection, *Information Hiding and Applications*, vol.227, pp.1-19, 2009.

[58] S. Wang, D. Zheng, J. Zhao, W. J. Tam and F. Speranza, An accurate method for image quality evaluation using digital watermarking, *IEICE Electronics Express*, vol.2, no.20, pp.523-529, 2005.

[59] W. Fourati and M. S. Bouhlel, Amelioration of the JPEG2000 by a variable window pretreatment, *Proc. of IEEE Information and Communication Technologies*, pp.1824-1829, 2006.

[60] H. Qi, D. Zheng and J. Zhao, Human visual system based adaptive digital image watermarking, *Signal Processing*, vol.88, no.1, pp.174-188, 2008.

[61] A. Hore and D. Ziou, Image quality metrics: PSNR vs SSIM, *Proc. of IEEE International Conference on Pattern Recognition*, pp.2366-2369, 2010.