IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received September 23, 2019, accepted October 15, 2019, date of publication October 17, 2019, date of current version October 30, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2948086

An Improved Watermarking Technique for Copyright Protection Based on Tchebichef Moments

FERDA ERNAWAN AND MUHAMMAD NOMANI KABIR
Faculty of Computer Systems & Software Engineering, Universiti Malaysia Pahang, Kuantan 26300, Malaysia

Corresponding author: Ferda Ernawan (ferda@ump.edu.my)

This work was supported by the Fundamental Research Grant Scheme (FRGS) from the Ministry of Higher Education, Malaysia, under Grant RDU190117.

ABSTRACT Watermarking technique is a method to protect ownership of digital multimedia. Most existing watermarking techniques achieve a good level of imperceptibility and robustness. The challenges to achieve higher invisibility and resistance with lower computational time motivate researchers to work on new watermarking schemes. Robustness against noise attacks and JPEG2000 compression needs to be improved to acquire a better resistance capability of the watermark. In this paper, we present a block-based Tchebichef watermarking technique for protecting copyrights. In this technique, the host image is first divided into non-overlapping blocks and Tchebichef moments are calculated for each block. The watermarks are embedded into the blocks with lower visual entropies. The watermark image is scrambled by Arnold transform before embedding into the Tchebichef moments of the selected image blocks. The proposed watermarking scheme was tested under noise additions, filtering, cropping and compressing attacks. Our scheme was verified and compared to the existing watermarking techniques under image geometric and processing attacks. Furthermore, the proposed scheme demonstrated a superior performance in robustness under noise attacks and JPEG2000.

INDEX TERMS Watermarking, copyright protection, embedding algorithm, tchebichef moments, visual entropies.

I. INTRODUCTION

Recently, watermarking techniques have been the focus of researchers for their role in copyright protection. In watermarking process, watermarks are embedded into the host image in a clever way. A watermark is ideally a logo, which becomes invisible after embedding into the host image. The watermark size is usually small in size, such that the watermark can fit for embedding in the image. A watermark logo should not be large in size, since it incurs significant effect to the quality of watermarked images. Watermarking is used for authentication, copyright protection and owner's identification. Due to its importance, the researchers continue to develop improved methods, which can resist different types of attacks and secure the image contents.

Watermarking is carried out in spatial domain or frequency-transform domain. In general, watermarking in spatial domain has a high accuracy for tampered pixels in the image and it is suitable for watermark authentication. However, this technique possesses a lack of robustness to defend against signal processing attacks and transformations. Therefore, watermarking based on spatial domain is not suitable for watermark protection. The transform techniques such as Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Integer Wavelet Transform (IWT) and Redundant Discrete Wavelet Transform (RDWT) and image moments are well-known in digital watermarking. Each method has its own limitations, and advantages and disadvantages. Image moments have attracted the attention for last few decades due to the minimum information redundancy. Some orthogonal moments introduced by Legendre, Pseudo-Zernike [1], [2], Tchebichef moments [3] and [4] have been widely used in image watermarking. The embedded watermark using moments produces the minimum reconstruction error of the watermarked image.

This paper presents a watermark embedding technique based on Tchebichef moments. First, the host image is divided by 8×8 block pixels of non-overlapping blocks.

The associate editor coordinating the review of this manuscript and approving it for publication was Amit Singh.

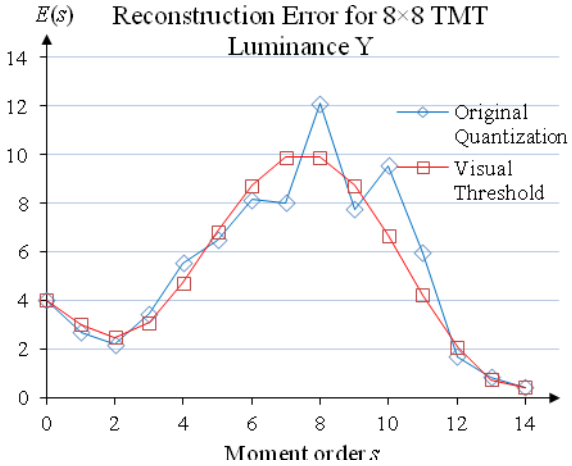


FIGURE 1. Variation of average reconstruction error for incrementing Tchebichef-moment order *s*.

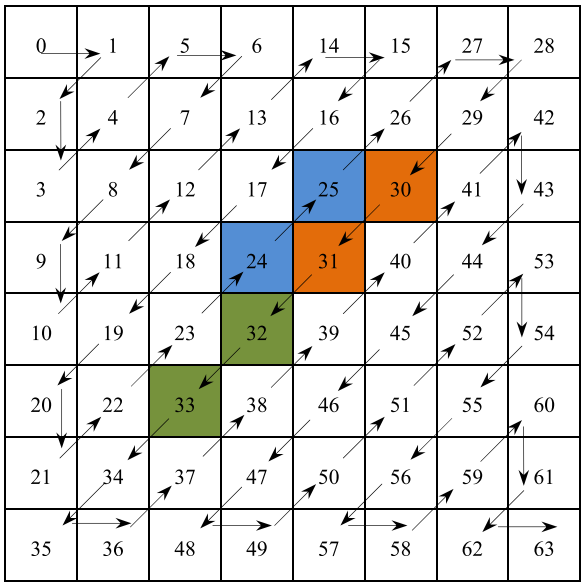


FIGURE 2. Selected TMT coefficient pairs based on psychovisual threshold.

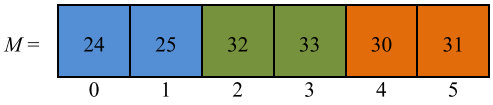


FIGURE 3. Selected coefficient pairs for embedding watermark.

Each block of the image is computed by a visual entropy. The blocks with the lowest values of entropy are selected considering the size of watermark bits. The number of selected blocks is equal to the watermark bits' size. Each selected block is transformed by Tchebichef moments, then it is traversed in a zig-zag order. The watermark is scrambled by Arnold transform and the scrambled watermark is not embedded directly to the Tchebichef moment; rather the scrambled watermark is taken into consideration by examining specific coefficient pairs with certain rules described in this paper. The results are presented and compared to the existing watermarking techniques for verifying the robustness and imperceptibility.

This paper is organized as follows. In section 2, related work and motivation are discussed. In section 3, the fundamental concept of human visual characteristics, Arnold transform, Tchebichef moments and the psychovisual threshold are briefly presented. The proposed embedding and extracting procedures are given in section 4. The experimental setup and performance evaluation in terms of robustness and imperceptibility are provided in section 5. Section 6 presents the simulation results and a comparison of the proposed technique to several recent watermarking techniques. Finally, section 6 concludes the paper.

II. RELATED WORK AND MOTIVATION

Most existing watermarking techniques involves frequency-transformation e.g., Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Redundant Discrete Wavelet Transform (RDWT) and Moment transforms for embedding the watermark into the transformed domains. Some watermarking techniques, known as hybrid schemes combines different transforms with Singular Value Decomposition (SVD). The combination achieves high robustness for watermark images. However, the computational complexity increases with the use of hybrid schemes.

Lai's scheme [5] presented a digital watermarking technique based on DCT-SVD. Watermark embedding is performed by examining orthogonal U matrix. The watermark is not embedded directly to the orthogonal U matrix, but the coefficients in U matrix are modified based on certain rules. This approach can avoid false positive problem that occurs when the watermark is embedded in singular values (S) of SVD. This scheme achieves a good level of imperceptibility and robustness of the watermarked image. However, they do not reveal the optimal threshold which is used to balance between imperceptibility and robustness.

Makbol's scheme [6] demonstrated block-based DWT-SVD in image watermarking. This approach was adopted by [5] for embedding and extracting the watermark. In this scheme, they presented a watermark embedding method by examining orthogonal U matrix obtained from DWT-SVD. In addition, they used AES-192 to encrypt the embedding coordinates. The authors presented a comparison between the proposed scheme and the Lai scheme where their scheme produces higher robustness than the Lai scheme in terms of bit correction rate (BCR). The authors used some threshold values for the experiment, while the thresholds may not suitable for other transforms e.g., DCT in the Lai scheme. Furthermore, the proposed thresholds do not provide the optimal balance between imperceptibility and robustness.

Li's scheme [7] and Ernawan's scheme [8] proposed watermarking methods using the mid-band of Tchebichef moment with scaling factors. Although, this approach produces high

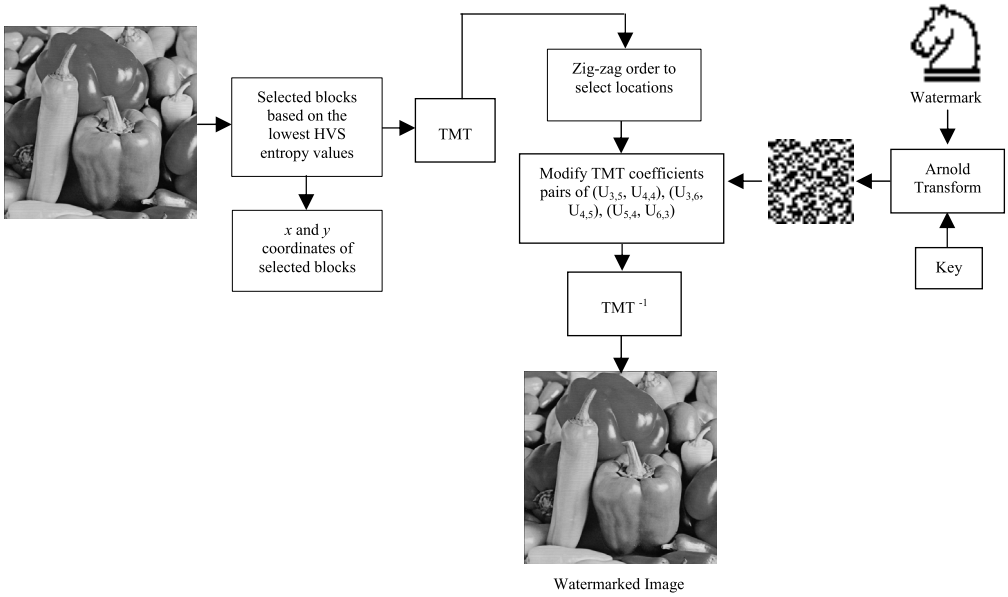


FIGURE 4. Schematic block diagram of the proposed watermark embedding.

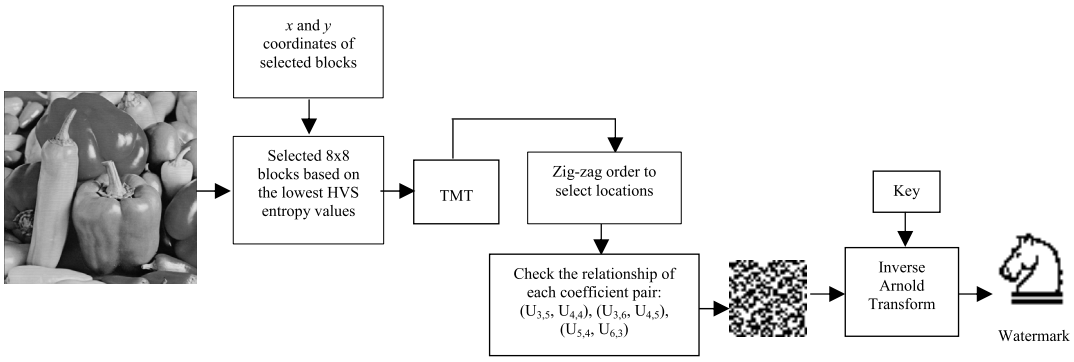


FIGURE 5. Schematic block diagram of the proposed watermark extraction.

robustness, the scaling factor depends on the types of images. To acquire a trade-off between imperceptibility and robustness for different images, the scaling factor in this scheme needs to be optimized. The scheme of [7] neither describes the specific locations of the mid-band of Tchebichef moments, nor does it consider the specific embedding locations. Moreover, each moment has a different effect on the distortion of the reconstructed watermarked image.

Lagzian's method [9] and Makbol & Khoo's method [10] presented watermarking schemes using RDWT and SVD. In both schemes, the watermark is embedded into each sub-band by modifying singular value S. However, these approaches were pointed out to be fundamentally flawed by researchers [11] and [12], since it produces a false-positive problem in the watermark-extraction stage because of embedding into S as reported by [13]. Mishra's scheme [14] presented an optimized watermarking scheme using hybrid DWT-SVD and Firefly algorithm. Firefly algorithm is used to optimize the scaling factor of the embedding watermark. The watermark is then embedded into the third level DWT in singular values. This approach also involves a fundamental flaw in its design as reported by [15].

Zhang's scheme [16] developed a watermarking scheme considering SVD in spatial domain. The watermark is inserted to the largest singular value of each block of the image. This scheme avoids false-positive errors that occur in traditional SVD-based watermarking schemes. It maintains good imperceptibility and robustness, while it must be tested under various attacks. Roy & Pal's scheme [17] presented a color-watermarking scheme with DCT-blocks. In the scheme, watermark bits are embedded into green/blue components of the transformed blocks by modifying middle significant AC coefficients using a repetition code. This scheme performs well on robustness to JPEG compression, while the specific locations for selected middle coefficients are not considered and the maximum number of embedding bits is not taken

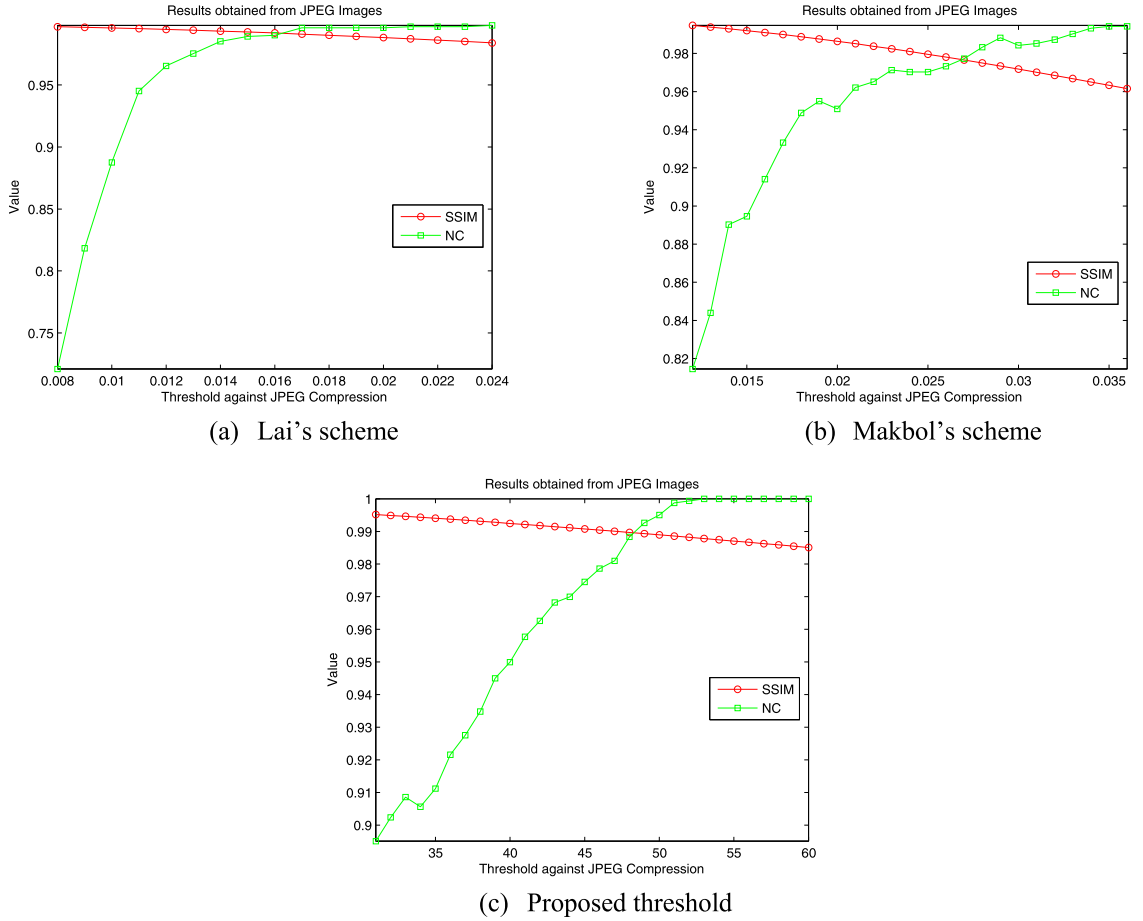


FIGURE 6. Tradeoff between SSIM and NC values: (a) Lai's scheme, (b) Makbol's scheme, (c) Proposed.

into account. Notice that each transformed block of size 8×8 has a limited number of bits. Embedding randomly on the middle frequency also may affect the image quality.

Das's scheme [18] proposed a watermarking technique using inter-block coefficient correlation. To embed the watermark bits, DCT coefficients of adjacent (neighbor) DCT blocks in the same position are modified according to the certain condition. This scheme does not sufficiently consider the important image information of the low-, middle- and high-frequency effect to the error reconstruction. This scheme has a good imperceptibility, while the robustness needs to be improved to satisfy a good resistance of watermark. A Summary of the reviewed literature is listed in Table 1.

This paper is mainly inspired by the following motivations:

1) A fast (low computational time) watermarking technique with an easy-implementation feature is always desirable. With reference to the perceptual distortion (high imperceptibility), the proposed digital watermarking technique must achieve the sufficient quality after embedding the watermark. With respect to robustness, the embedded watermark must provide high robustness under different types of attacks. For example, DWT produce high imperceptibility and robustness for watermarked images, while it also has high computational complexity due to wavelet transform. The challenges to achieve high imperceptibility, high robustness

TABLE 1. Comparison of existing watermarking techniques.

Author	Method	False Positive Problem	Disadvantage
Lai [5]	DCT-SVD	No	Security issues
Makbol et al. [6]	DWT-SVD	No	Requires higher computational cost.
Lagzian et al. [9]	RDWT-SVD	Yes	Requires higher computational cost.
Zhang et al. [16]	SVD	No	Less robustness under extreme JPEG compression.
Roy & Pal [17]	DCT	No	Embedding locations at middle coefficients not considered affecting the image quality.
Das et al. [18]	DCT	No	The embedding scheme does not sufficiently consider the low, middle and high frequency effect to the error reconstruction.
Ernawan & Kabir [19]	DCT-Psychovisual Threshold	No	Robustness performance needs to be improved.

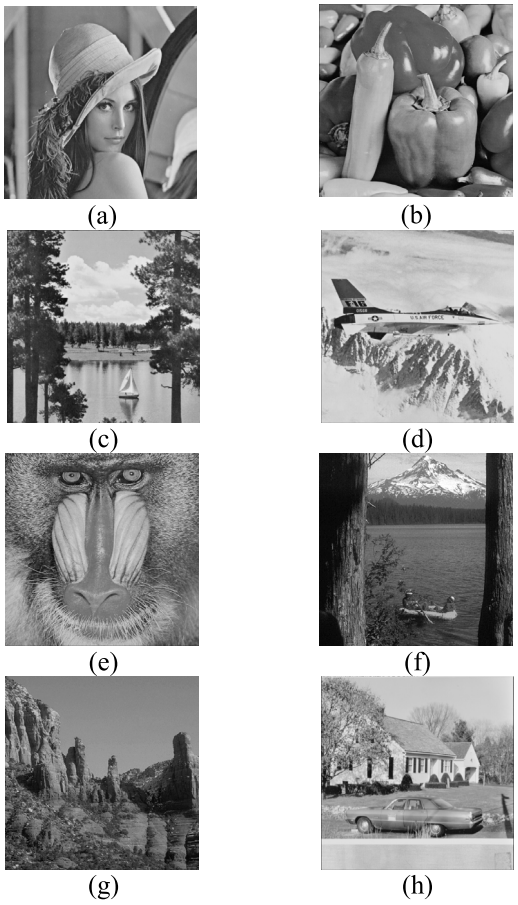


FIGURE 7. (a)Lena; (b) Pepper; (c) Sailboat; (d) Airplane; (e) Baboon; (f) Lake; (g) Red Rock; (h) House.

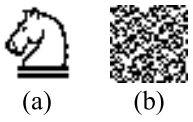


FIGURE 8. (a) original binary watermark 32×32 pixels; (b) scrambled watermark image.

with lower computational time motivate us to work on a new watermarking technique.

2) Embedding watermark on the transformed domain has been applied in many digital watermarking schemes. Embedding on the low frequency domain may reduce the quality of watermarked images. Furthermore, embedding the watermark on the high frequency domain will not be suitable in case of JPEG compression due to quantizing the high frequency domain by quantization tables. Embedding on the middle frequency domain may affect the image texture. It motivates us to find a new embedding technique with suitable locations on the middle frequency domain for embedding the watermark, providing minimum distortion to the watermarked images.

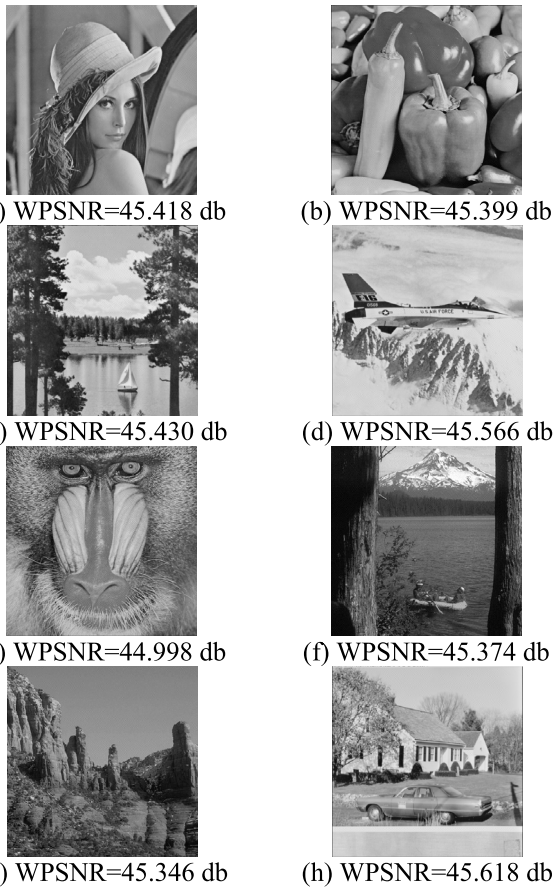


FIGURE 9. Watermarked images (a)Lena; (b) Pepper; (c) Sailboat; (d) Airplane; (e) Baboon; (f) Lake; (g) Red Rock; (h) House.

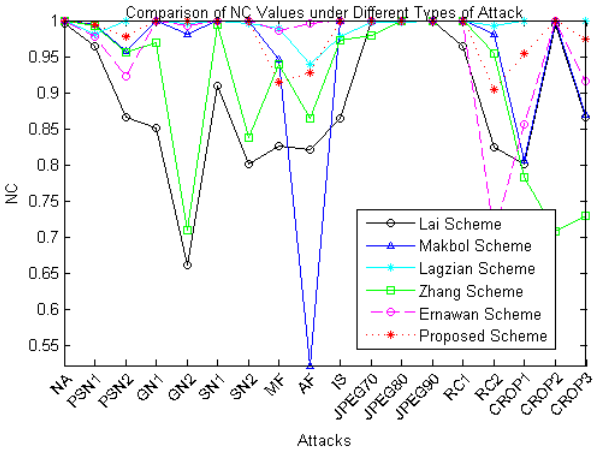


FIGURE 10. Illustration of NC values under different attacks.

3) The human visual system (HVS) is less sensitive to the less image information (lowest entropy). Hence, researchers utilize the entropy values to identify the embedding regions. This approach has been confirmed by [5] scheme and [6] scheme that perform embedding on the lowest entropy providing high imperceptibility, since the image blocks with the lowest entropy values

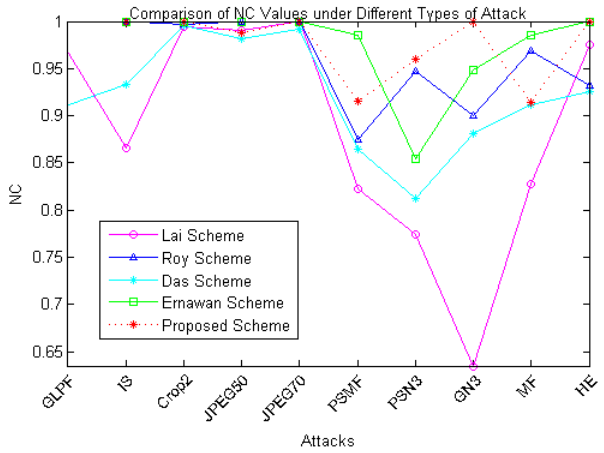
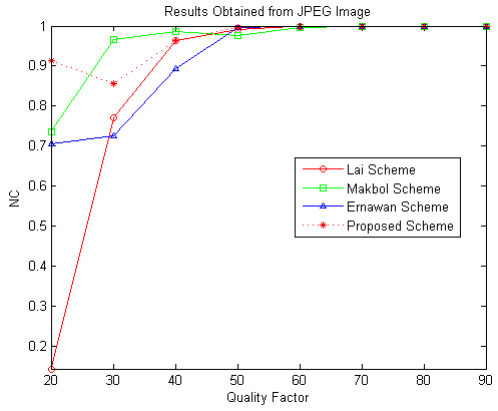
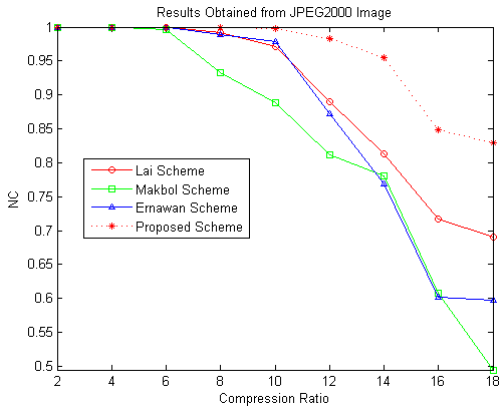


FIGURE 11. Illustration of NC values under different attacks.



(a)



(b)

FIGURE 12. Illustration of NC values under different levels of (a) JPEG; (b) JPEG2000 compression.

carry the least information of the image [20]. Therefore, our scheme also utilizes the HVS entropy to choose the suitable blocks for watermark embedding.

III. RELEVANT TECHNIQUES

The properties of the human visual system (HVS) can be utilized to reduce visibility of the watermark. Thus, the properties can be used to determine the image-regions, which do not incur significant distortions after the watermark bits are embedded. HVS properties can be described in terms of entropy and edge entropy. These methods were implemented by [5] and [6]. HVS entropy with n-state can be defined by:

$$HVS_{Entropy} = \left(-\sum_{i=1}^{n} p_i \log_2(p_i) + \sum_{i=1}^{n} p_i \exp^{1-p_i} \right) \quad (1)$$

where p_i is the occurrence probability of i-th pixel with $0 \leq p_i \leq 1$ and $1\text{-}p_i$ is the uncertainty of the pixel.

A. ARNOLD TRANSFORM

The Arnold transformation is given by [21], [22]:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod N \quad (2)$$

where (x', y') is the pixel position after the transformation and (x, y) is the original pixel position of the image. the modulus operation is denoted by *mod* with a divisor with N where N represents the period of Arnold transform. The inverse Arnold

TABLE 2. Nomenclature of geometrical attacks on the watermarked images for evaluating robustness.

Abbreviation	Attack's Description	Abbreviation	Attack's Description
NA	No Attack	IS	Image Sharpening
GLPF	Gaussian Low Pass Filter (3,3)	JPEG20	JPEG (Q=20)
PSN1	Pepper and Salt Noise, density 0.001	JPEG50	JPEG (Q=50)
PSN2	Pepper and Salt Noise, density 0.005	JPEG60	JPEG (Q=60)
PSN3	Pepper and Salt Noise, density 0.01	JPEG70	JPEG (Q=70)
GN1	Gaussian Noise 0.0001	JPEG80	JPEG (Q=80)
GN2	Gaussian Noise 0.0005	JPEG90	JPEG (Q=90)
GN3	Gaussian Noise variance=0.001	JPEG2000-12	JPEG2000 with CR=12
SN1	Speckle Noise 0.0001	RC1	Rescaling (2, 0.5)
SN2	Speckle Noise 0.0005	RC2	Rescaling (0.5, 2)
SN3	Speckle Noise 0.003	Crop1	Cropping (top 25%)
MF	Median Filter	Crop2	Cropping (middle 25%)
AF	Average Filter	Crop3	Cropping (right 25%)
WF	Wiener Filter	PSMF	Combinational Attacks Pepper & Salt (density=0.003) and Median Filter (3,3)
ADJ	Adjust	HE	Histogram equalization
PN	Poisson Noise	SHP	Sharpening
PSM	Combination Pepper & Salt (density=0.003) and Median Filter (3,3)	JPEGCROP	Combination JPEG and Centre Cropping

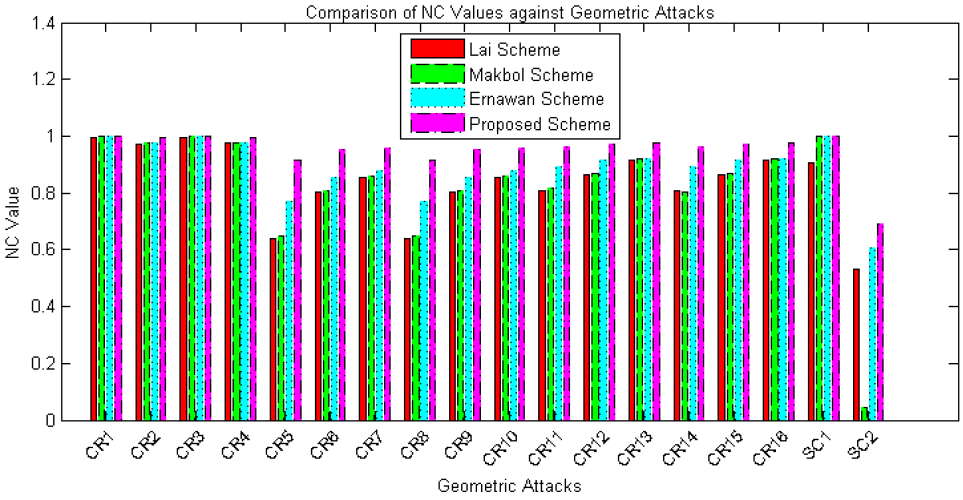


FIGURE 13. Illustration of NC values under geometric attacks.

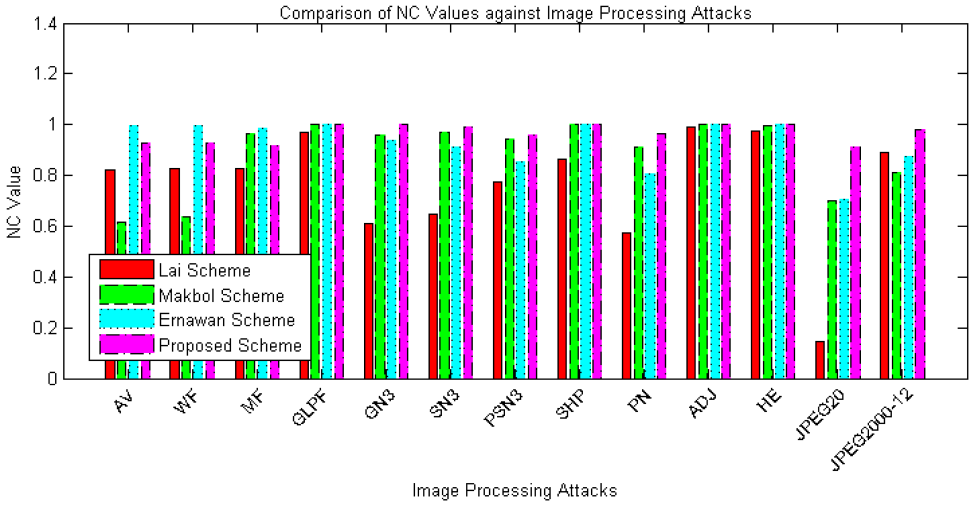


FIGURE 14. Comparison of NC values under image processing attacks.

transformation is defined as:

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} \bmod N \tag{3}$$

B. TCHEBICHEF MOMENTS

Tchebichef moments are computed using Tchebichef polynomials. For a given set $\{t_n(x)\}$ of input values (image intensity values) with size N, M=8, the forward TMT with an order of $m+n$ is given as follows:

$$T_{mn} = \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} \frac{t_m(x)}{\rho(m,M)} f(x,y) \frac{t_n(y)}{\rho(n,N)}$$

$$T_{mn} = \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} k_m(x) f(x,y) k_n(y) \tag{4}$$

for $m, n = 0, 1, 2, \ldots, N-1$ and $f(x, y)$ denotes the intensity value at the pixel position (x, y) in the image. The term $t_n(x)$ is defined using the following recursive relation [23]:

$$t_0(x) = 1, \tag{5}$$

$$t_1(x) = \frac{2x+1-N}{N}, \tag{6}$$

$$t_n|(x) = \frac{(2n-1)\cdot t_1(x)\cdot t_{n-1}(x) - (n-1)\left(1-\frac{(n-1)^2}{N^2}\right)\cdot t_{n-2}(x)}{n} \tag{7}$$

for $n = 2, 3, ..., N-1$. Thus, $t_n(x)$ of 8×8 orthogonal T Tchebichef polynomials is evaluated as (8), as shown at the bottom of page 10, where the scale factor for the polynomial of degree n is defined as follows:

$$\beta(n,N) = N^n \tag{9}$$

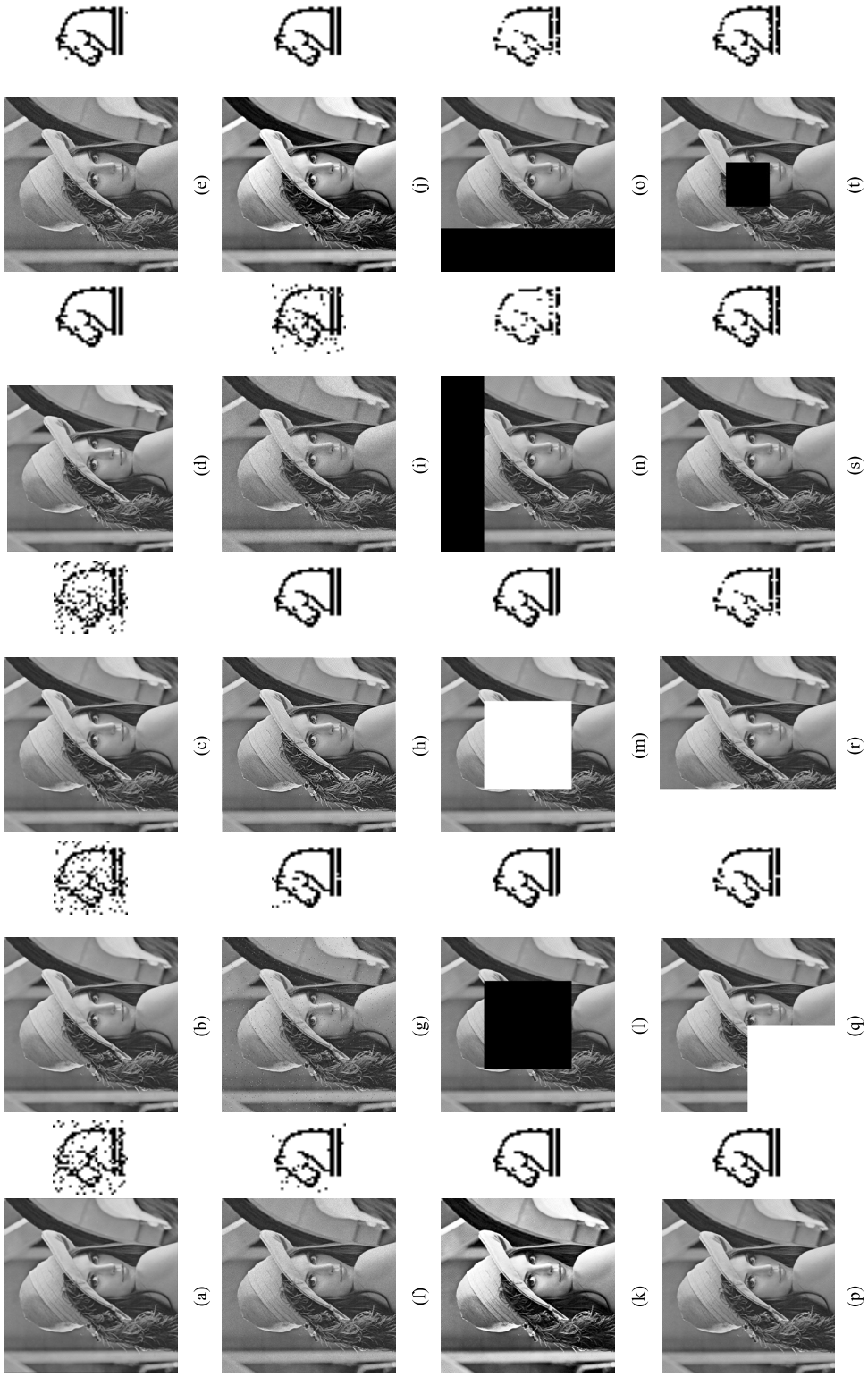


FIGURE 15. Recovery of a watermark image after attacks on a watermarked image (a) Average Filter (3,3) (b) Wiener Filter (3,3) (c) Median Filter (3,3) (d) Gaussian Low Pass Filter (3,3) (e) Gaussian Noise (var=0.001) (f) Speckle Noise (var=0.003) (g) Pepper and Salt Noise (density=0.001) (h) Sharpening (i) Poisson Noise (j) Adjust (k) Histogram Equalization Attack (l) Centred Cropping 50% (256×256 by black) (m) Centred Cropping 50% (256×256 by white) (n) Cropping rows off 25% (128 rows by black) (o) Cropping columns off 25% (128 columns by black) (p) Scaling 0.8 (q) Cropping bottom left corner 256x256 with white (r) Cropping columns off 25% (128 columns by white) (s) JPEG with $QF = 50$ (t) Combination JPEG with QF=50 and Centre Cropping 25%.

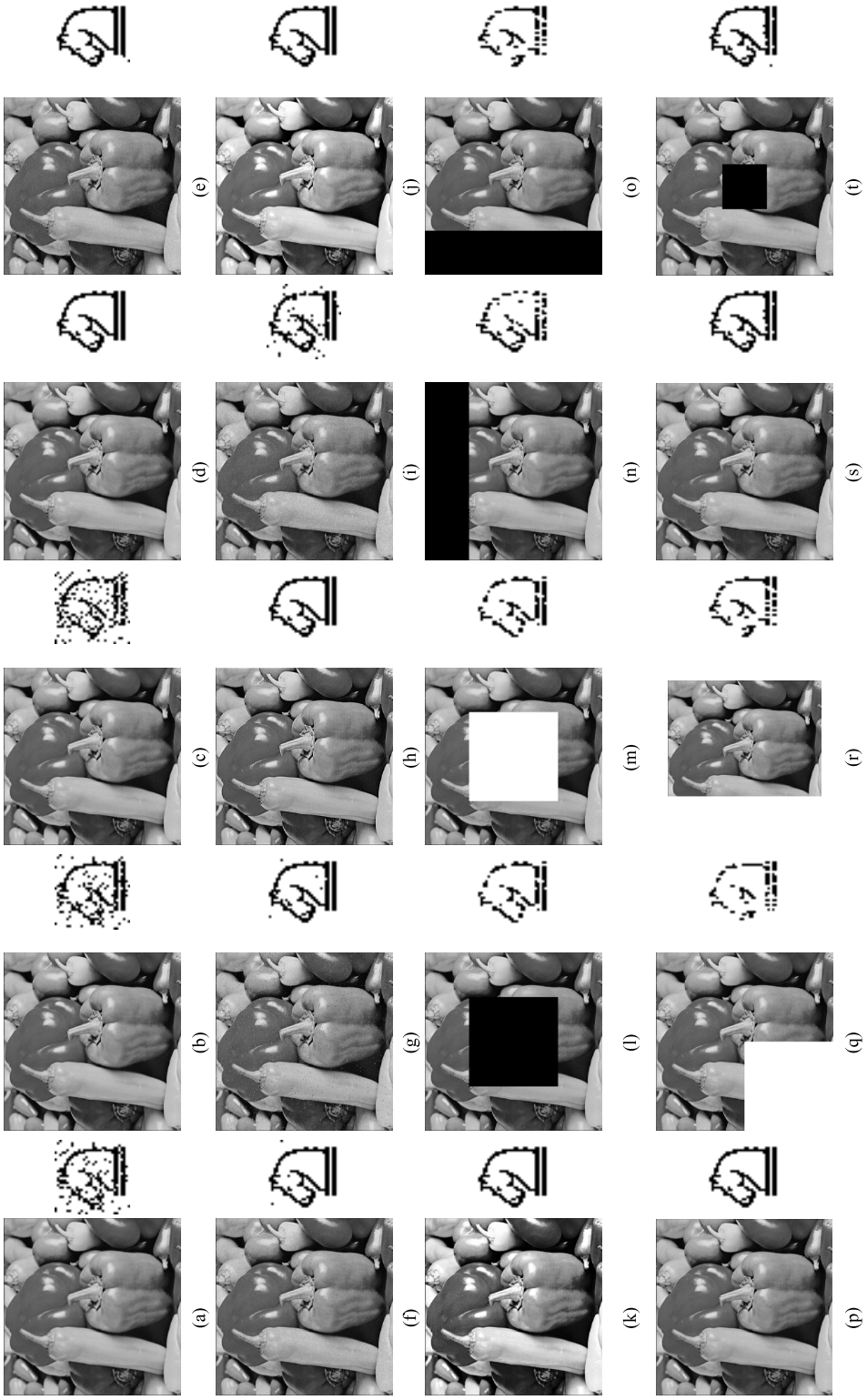


FIGURE 16. Recovery of a watermark image after attacks on a watermarked image (a) Average Filter (3,3) (b) Wiener Filter (3,3) (c) Median Filter (3,3) (d) Gaussian Low Pass Filter (3,3) (e) Gaussian Noise (var=0.001) (f) Speckle Noise (var=0.003) (g) Pepper and Salt Noise (density=0.001) (h) Sharpening (i) Poisson Noise (j) Adjust (k) Histogram Equalization Attack (l) Centred Cropping 50% (256×256 by black) (m) Centred Cropping 50% (256×256 by white) (n) Cropping rows off 25% (128 rows by black) (o) Cropping columns off 25% (128 columns by black) (p) Scaling 0.8 (q) Cropping bottom left corner 256x256 with white (r) Cropping columns off 25% (128 columns by white) (s) JPEG with QF=50 (t) Combination JPEG with $QF = 50$ and Centre Cropping 25%.

TABLE 3. Abbreviation of geometrical attacks on watermarked images for evaluating robustness.

Abbreviation	Attack's Description	Abbreviation	Attack's Description
CR1	Center Cropping 25% (128x128 by black)	CR12	Cropping off 25% (128 columns by black)
CR2	Center Cropping 50% (256x256 by black)	CR13	Cropping off 12.5% (64 columns by black)
CR3	Center Cropping 25% (128x128 by white)	CR14	Cropping off 50% (256 columns by white)
CR4	Center Cropping 50% (256x256 by white)	CR15	Cropping off 25% (128 columns by white)
CR5	Cropping off 50% (256 rows by black)	CR16	Cropping off 12.5% (64 columns by white)
CR6	Cropping off 25% (128 rows by black)	CR17	Cropping top left corner (white, 256x256 pixels)
CR7	Cropping off 12.5% (64 rows by black)	CR18	Cropping top right corner (white, 256x256 pixels)
CR8	Cropping off 50% (256 rows by white)	CR19	Cropping bottom left corner (white, 256x256 pixels)
CR9	Cropping off 25% (128 rows by white)	CR20	Cropping bottom right corner (white, 256x256 pixels)
CR10	Cropping off 12.5% (64 rows by white)	SC1	Scaling 0.8
CR11	Cropping off 50% (256 columns by black)	SC2	Scaling 0.25

Then we define squared-norm $\rho(\cdot)$ using set $\{t_n(x)\}$ that

$$\rho(n,N) = \sum_{i=0}^{N-1}\{t_i(x)\}^2 = \frac{N\cdot\left(1-\frac{1^2}{N^2}\right)\cdot\left(1-\frac{2^2}{N^2}\right)\cdot\left(1-\frac{3^2}{N^2}\right)\cdots\left(1-\frac{n^2}{N^2}\right)}{2n+1} \tag{10}$$

The description of squared-norm $\rho(\cdot)$ and the properties of orthogonal Tchebichef polynomials can be found in the work of [24]. The inverse TMT is given as follows:

$$\tilde{f}(x,y) = \sum_{m=0}^{M-1}\sum_{n=0}^{N-1} k_m(x)T_{mn}k_n(y) \tag{11}$$

where M is the maximum order of moments and $\tilde{f}(x,y)$ implies the reconstructed intensity distribution.

TABLE 4. Imperceptibility performance of the proposed watermarking scheme.

Host images	PSNR	WPSNR	SSIM
Lena	40.845	45.418	0.990
Pepper	40.792	45.399	0.988
Sailboat	40.864	45.430	0.988
Airplane	40.975	45.566	0.988
Baboon	40.438	44.998	0.992
Lake	40.517	45.374	0.989
Red rock	40.776	45.346	0.986
House	41.031	45.618	0.988

IV. PROPOSED SCHEME

In this scheme, first, the host image is split into non-overlapping blocks of 8×8 pixels. Tchebichef transform is used on each block to construct the Tchebichef moments which were considered for less computational complexity and better imperceptibility of the watermarked image. Psychovisual threshold using HVS entropy was used to find the ideal embedding locations as discussed in sub-section A The watermark logo is scrambled by Arnold transform and the scrambled watermark bits are embedded into the host image with a secret key. The muddle watermark cannot be recovered without the secret key, even an attacker successfully extracts the watermark from the host image. Our embedding and extraction techniques are provided in sections B and C.

A. PSYCHOVISUAL THRESHOLD

Psychovisual threshold can be measured by reconstruction error for each moment order [25]. Referring to Figure 1, one calculates the difference between the reconstruction errors - one with visual threshold and the other with the quantization values. We notice a significant gap in moments between the orders 6 and 7. Modifying coefficients between the moment orders may not give significant effect to the watermarked image reconstruction. Thus, the gap can be utilized for embedding the watermark bits as shown in the figure. Due to limited coefficients in moment order 6 to 7, we select the coefficients pairs of ($U_{3,5}$, $U_{4,4}$), ($U_{3,6}$, $U_{4,5}$), ($U_{5,4}$, $U_{6,3}$) for watermark embedding as the coefficients have less effect to the reconstruction errors as shown in Figure 2.

Then, the selected locations are ordered in a vector form as shown in Figure 3. The embedding process on these locations is described in the next section.

$$t_n(x) = \begin{bmatrix} 1.000 & 1.000 & 1.000 & 1.000 & 1.000 & 1.000 & 1.000 & 1.000 \\ -0.875 & -0.625 & -0.375 & -0.125 & 0.125 & 0.375 & 0.625 & 0.875 \\ 0.656 & 0.093 & -0.281 & -0.468 & -0.468 & -0.281 & 0.093 & 0.656 \\ -0.410 & 0.293 & 0.410 & 0.175 & -0.175 & -0.410 & -0.293 & 0.410 \\ 0.205 & -0.380 & -0.087 & 0.263 & 0.263 & -0.087 & -0.380 & 0.205 \\ -0.076 & 0.252 & -0.186 & -0.164 & 0.164 & 0.186 & -0.252 & 0.076 \\ 0.019 & -0.096 & 0.173 & -0.096 & -0.096 & 0.173 & -0.096 & 0.019 \\ -0.002 & 0.016 & -0.050 & 0.084 & -0.084 & 0.050 & -0.016 & 0.002 \end{bmatrix} \tag{8}$$

B. PROPOSED EMBEDDING TECHNIQUE

Algorithm 1 presents the step-by-step description of the watermark embedding process. Visual illustration of block schematic diagram is shown in Figure 4.

The proposed technique uses two thresholds: α for the first coefficient, and ß for the second coefficient. Based on some criteria presented in Algorithm 2, α and ß are set as negative or positive values. The embedding process is illustrated in Figure 4.

for $u = 0$, 1, and 2, $M(2u)$ represents $M(0)$, $M(2)$ and $M(4)$ and $M(2u+1)$ denotes $M(1)$, $M(3)$ and $M(5)$. α and ß present variant threshold for watermark embedding. If $A(2u) < 0$ or $A(2u+1) < 0$, the threshold value is negative, otherwise the threshold is positive. Watermark bits are embedded according to the above rules.

C. PROPOSED EXTRACTION TECHNIQUE

The following steps in the Algorithm 3 describe the procedure of the watermark extraction process. The schematic block diagram of extracted watermark is shown in Figure 5.

D. OPTIMAL THRESHOLD

In this section, we discuss the procedure to find the optimal threshold for embedding the watermark. The optimal threshold T is obtained from the tradeoff between robustness (NC values of the extracted watermark) and imperceptibility (SSIM values from the watermarked image) using standard JPEG compression as shown in Figure 6. In the figure, we observe that the threshold parameter plays an important role as it relates to the effect of robustness and imperceptibility levels. Thus, the optimal parameter T can be calculated using the tradeoff between SSIM and NC values of the watermarked image. The following procedure is used to find T:

i. The parameter is increased at a rate of 1.
ii. Selected coefficients of Tchebichef moments as shown in Figure 3 are evaluated using the rules in Algorithm 2.
iii. NC and SSIM are calculated for each threshold parameter.
iv. T is found using the tradeoff between SSIM and NC values.

As mentioned above procedure, the threshold is incremented by 1 at a time and evaluated by standard JPEG compression. JPEG compression is used for evaluation purpose due to its huge applications. The experimental results reveal the optimal threshold for Lai's scheme as about 0.016, Makbol's scheme with DWT-SVD is about 0.027, while the proposed TMT threshold is about 48.

V. EXPERIMENTAL SETUP AND EVALUATION

We use MATLAB R2014a operating under Windows 10 on Intel Core i5-6200U CPU @ 2.30GHz 2.40 GHz processor with 16-GB RAM to carry out the experiments on the proposed technique. Eight images of size 512×512 pixels with 8 bits per pixel are selected as host images as given in Figure 7. A binary watermark image of size 32×32 pixels is

Algorithm 1 Embedding Process

Input: Host image; watermark;

Pre-processing:

Step 1: The host image with size 512×512 pixels is split into non-overlapping blocks of size 8×8 pixels.

Step 2: Calculate the HVS entropy of each block as described in Equation (3).

Step 3: A watermark with 1024 bits is scrambled using Arnold transform before embedding the watermark.

Step 4: Select 1024 of 4096 blocks, possessing lowest HVS entropy values and save their x and y coordinates.

Watermark embedding:

Step 5: Compute two-dimensional TMT for each non-overlapping selected block. Each TMT blocks is arranged as zig-zag order as shown in Figure 2. The TMT coefficients pairs of ($U_{3,5}$, $U_{4,4}$), ($U_{3,6}$, $U_{4,5}$), ($U_{5,4}$, $U_{6,3}$) are stored in $M(u)$, where $u = 0, 1, \ldots, 5$.

Step 6: Each watermark bit is embedded according to the following rules:
Rule 1: if the $M(u)$ coefficient is the negative value, the threshold must be negative value, and the vice versa.
Rule 2: for u: 0 to 3, the binary watermark bit = 1, then if absolute value of $M(2u)$ is less than absolute value of $M(2u+1)$, swap the values between $M(2u)$ and $M(2u+1)$ in each pair, thus $M(2u)$ is added by a threshold β. if absolute value of $M(2u)$ is greater than absolute value of $M(2u+1)$, thus $M(2u)$ is added by a threshold α and manage the value of $M(2u+1)$.
Rule 3: for u: 0 to 3, the binary watermark bit = 0, then if absolute value of $M(2u)$ is less than absolute value of $M(2u+1)$, $M(2u)$ is added by a threshold β, thus manage the value of $M(2u+1)$ as the original value. If absolute value of $M(2u)$ is greater than absolute value of $M(2u+1)$, swap the values between $M(2u)$ and $M(2u+1)$ in each pair, thus $M(2u+1)$ is added by a threshold α. The detail description of the proposed embedding is given in Algorithm 2.

Post-processing:

Step 7: The modified TMT coefficients $M(u)$ for $u = 0, 1, \ldots, 5$ are reconstructed in the two-dimensional matrix of size 8x8.

Step 8: Apply the inverse TMT on each selected 1024 blocks.

Step 9: Merge all the modified selected blocks to reconstruct the watermarked image.

Output: Watermarked image

Algorithm 2 Proposed Embedding Technique

```
W = 1;
for u = 0 to 2 do
    if (M(2u) < 0) then
        α = −T;
    else
        α = T;
    end (if)
    if (M(2u + 1)<0) then
        ß=−T;
    else
        ß=T;
    end (if)
    if W <length (Watermark) then
        if Watermark (W) = 1 then
            if (|M(2u)| < |M(2u + 1)|) then
                S = M(2u);
                M(2u) = M(2u + 1)+ß;
                M(2u + 1) = S;
            else
                M(2u) = M(2u) + α;
                M(2u + 1) = M(2u + 1);
            end (if)
        else
            if (|M(2u)| < |M(2u + 1)|) then
                M(2u) = M(2u)+ß;
                M(2u + 1) = M(2u + 1);
            else
                S = M(2u);
                M(2u) = M(2u + 1);
                M(2u + 1) = S + α;
            end (if)
        end (if)
    end (if)
    W = W + 1;
end (for)
```

used for embedding into the host images. A binary watermark and the corresponding muddle watermark obtained from Arnold transform are shown in Figure 8.

A host image is split into non-overlapping blocks of size 8×8. HVS entropy value is computed for each block, and the blocks are rearranged in higher oder of entropy with the block coordinates. The blocks with the lower HVS entropy values are chosen for embedding the watermark. Note that the number of selected blocks should be the same as the number of watermark bits to facilitate complete embedding. A binary watermark is scrambled by Arnold transform, then it is converted into a vector for embedding watermark bits. Each chosen block is transformed using 8×8 Tchebichef moments. As mentioned earlier, referring to Tchebichef psychovisual threshold, the best locations for embedding watermark are $M(4,4)$, $M(3,5)$, $M(6,3)$, $M(5,4)$ and $M(4,5)$, $M(3,6)$. The scrambled watermark is embedded into the best locations by some specific rules as explained in Algorithm 2. Performance-evaluation metrics of the proposed watermarking technique are provided in the next section.

Algorithm 3 Watermark Extraction Process

Input: Watermarked image;

Pre-processing:

Step 1: The watermarked image is divided into non-overlapping blocks of size 8×8 pixels. The x and y coordinates are utilized to determine the selected blocks i.e., embedded blocks.

Step 2: Use TMT for each selected blocks.

Step 3: Perform zig-zag order to find selected TMT coefficients $M(u)$for $u = 0, 1, \ldots, 5$.

Watermark extraction:

Step 4: For each bit of extracted watermark, watermark extraction follow the rules:
Rule 1: for u: = 0 to 3, if the different between absolute value $M(2u)$ and absolute value of $M(2u + 1)$ is larger than 0, then binary watermark bit is set as 1.
Rule 2: for u: = 0 to 3, if the different between absolute value $M(2u)$ and absolute value of $M(2u + 1)$ is lesser than 0, then binary watermark bit is set as 0.

Post-processing:

Step 5: The extracted watermark $W(s)$ for $s = 0, 1, \ldots, 1024$ are reconstructed in the two-dimensional matrix of size 32×32.

Step 6: Use inverse Arnold transform to obtain the extracted watermark.

Output: Recovered watermark

A. PERFORMANCE EVALUATION

Imperceptibility and robustness of the embedded watermark under different image transformations need to be estimated to assess the performance of a watermarking technique. To measure the quality of a watermarked image (imperceptibility), we use Peak Signal-to-Noise Ratio (PSNR) and weighted PSNR defined as follows:

$$MSE = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}[g(i,j) - f(i,j)]^2 \tag{12}$$

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right) \tag{13}$$

$$WPSNR = 10\log_{10}\left(\frac{255^2}{\sqrt{MSE} \times NVF}\right) \tag{14}$$

TABLE 5. NC values of the recovered watermark for different attacks on lena image watermarked by different schemes.

Attack	Lai [5]	Makbol et al. [6]	Lagzian et al. [9]	Zhang et al. [16]	Ernawan & Kabir [19]	Our Scheme
No attack	0.9961	1	1	1	1	**1**
Pepper and Salt Noise 0.001	0.9648	**0.9941**	0.9812	0.9923	0.9773	0.9938
Pepper and Salt Noise 0.005	0.8669	0.9580	**0.9993**	0.9566	0.9234	0.9781
Gaussian Noise 0.0001	0.8515	1	0.9988	0.9693	1	**1**
Gaussian Noise 0.0005	0.6616	0.9802	0.9963	0.7099	0.9922	**1**
Speckle Noise 0.0001	0.9089	1	0.9991	0.9944	1	**1**
Speckle Noise 0.0005	0.8012	1	0.9960	0.8379	1	**1**
Median Filter [3×3]	0.8272	0.9467	**0.9891**	0.9386	0.9854	0.9147
Average Filter [3×3]	0.8223	0.5234	0.9402	0.8641	**0.9951**	0.9278
Image Sharpening	0.8653	1	0.9770	0.9724	1	**1**
JPEG (Q=70)	1	0.9990	0.9973	0.9793	1	**1**
JPEG (Q=80)	1	1	0.9976	0.9986	1	**1**
JPEG (Q=90)	1	1	0.9990	1	1	**1**
Rescaling (2, 0.5)	0.9635	1	0.9991	1	1	**1**
Rescaling (0.5, 2)	0.8252	0.9812	**0.9925**	0.9538	0.7056	0.9042
Cropping (top 25%)	0.8014	0.8060	**1**	0.7828	0.8564	0.9541
Cropping (middle 25%)	0.9941	0.9990	1	0.7083	1	**1**
Cropping (right 25%)	0.8658	0.8703	**1**	0.7297	0.9168	0.9737

$$NVF = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\frac{1}{1+\theta\sigma_x^2(i,j)} \tag{15}$$

$$\sigma_x^2(i,j) = \frac{1}{(2l+1)^2}\sum_{m=-l}^{l}\sum_{n=-l}^{l}(x(i+m,j+n)-\bar{x}(i,j))^2 \tag{16}$$

$$\theta = \frac{D}{\sigma_{x\,\max}^2} \tag{17}$$

where σ_x^2 is a maximum local variance of the image; $f(i,j)$ and $g(i,j)$ represent the pixel values at position (i,j) of the host and watermarked images, respectively; and $D \in [50, 100]$. The Structural SIMilarity index (SSIM) is defined by:

$$SSIM(x,y) = \frac{(2xy+c_1)(2\sigma_{xy}+c_2)}{(x^2+y^2+c_1)(\sigma_x^2+\sigma_y^2+c_2)} \tag{18}$$

where two constants $c_1 = (k_1L)^2$ and $c_2 = (k_2L)^2$ are taken to avoid numerical error for division with weak denominator, where $L = 255$ (i.e., 8 bits for each pixel), $k_1 = 0.01$ and $k_2 = 0.03$ are taken. We notice that the higher PSNR, WPSNR and SSIM values provide greater imperceptibility of a watermark in the host image. An extracted watermark is quantitatively measured using normalized cross-correlation (NC) and Bit Error Rate (BER) which are defined as follows:

$$NC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}W(i,j).W^*(i,j)}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}W(i,j)^2\sum_{i=1}^{M}\sum_{j=1}^{N}W^*(i,j)^2}} \tag{19}$$

$$BER = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}W(i,j)\oplus W^*(i,j)}{M\times N} \tag{20}$$

where $\oplus$ stands for the exclusive OR operation; the number of rows and the number of columns of the watermark image are given by M and N, respectively; $W^*(i,j)$ is the pixel value at position (i,j) of the extracted watermark; and $W(i,j)$ is the pixel value at position (i,j) of the original watermark. The NC value converging to one implies that the extracted watermark is completely accurate. A smaller BER value indicates higher robustness of the watermark image.

TABLE 6. NC values of the proposed and existing schemes for watermarked lena image after various attacks.

Attacks	Lai [5]	Roy & Pal [17]	Das et al. [18]	Ernawan & Kabir [19]	Our scheme
Gaussian Low Pass Filter (3,3)	0.967	1	0.911	1	**1**
Image Sharpening	0.865	1	0.932	1	**1**
Centred Cropping 25% (128x128 by white)	0.994	0.996	0.995	1	**1**
JPEG (QF=50)	0.990	**1**	0.981	0.999	0.988
JPEG (QF=70)	1	1	0.991	1	**1**
Combinational Attacks Pepper & Salt (density=0.003) and Median Filter (3,3)	0.822	0.874	0.864	**0.985**	0.915
Pepper & Salt noise, density = 0.01	0.774	0.946	0.812	0.853	**0.960**
Gaussian Noise variance=0.001	0.634	0.899	0.881	0.948	**1**
Median Filter with filter size 3x3	0.827	0.968	0.911	**0.985**	0.914
Histogram Equalization	0.974	0.931	0.925	1	**1**

B. TYPES OF ATTACK

To measure the robustness, our scheme is evaluated by simulating different attacks on the watermarked images.

TABLE 7. Computational complexity among Lai's scheme, Makbol's scheme and the proposed scheme.

Images	Embedding (seconds)			Extraction (seconds)		
	Lai [5]	Makbol et al. [6]	Proposed	Lai [5]	Makbol et al. [6]	Proposed
Lena	2.1406	13.4688	1.9844	0.7344	5.5000	0.2813
Pepper	2.0156	12.3125	1.6406	0.7188	5.2188	0.2656
Sailboat	2.0469	13.4844	1.7656	0.7656	5.2656	0.3125
Airplane	2.0625	12.5000	1.7656	0.8281	5.1250	0.2969
Baboon	2.2188	14.8438	1.6563	0.8125	5.3125	0.2188
Lake	2.2500	12.6406	1.7813	0.7188	5.2344	0.2500
Red Rock	2.0156	12.8281	1.7344	0.8438	5.1094	0.2031
House	2.0781	12.6250	1.6406	0.7969	5.1563	0.2656

TABLE 8. Ber values of the proposed and existing schemes for watermark recovery from stirmark benchmark.

JPEG Compression	Lai [5]	Makbol et al. [6]	Ernawan & Kabir [20]	Our scheme
40	0.156	**0.016**	0.155	0.182
50	0.270	0.034	**0.002**	0.019
60	0.366	0.015	0	**0**
70	0.281	0.001	0	**0**
80	0.136	0	0	**0**
90	0.059	0	0	**0**
100	0.010	0	0	**0**

The attacks are categorized into image-processing- and geometrical attacks as listed in Tables 1-2.

VI. EXPERIMENTAL RESULTS

We now discuss the experimental results in detail. The results of imperceptibility, robustness and computational time are given in Tables and Figures. The results are also compared to the existing watermarking schemes.

A. IMPERCEPTIBILITY RESULTS

Imperceptibility is the invisibility of embedded watermark, indicating visual non-distortion of host image after embedding the watermark image into the host image.

Imperceptibility of a watermarked image is estimated by SSIM, PSNR and WPSNR values. SSIM, PSNR and WPSNR values of the proposed scheme are listed in Table 3. The visual watermarked images are shown in Figure 9.

B. ROBUSTNESS RESULTS

Robustness of our scheme was evaluated with different simulated attacks on the watermarked images using normalized cross-correlation (NC) value. NC values from extracted watermark after various attacks is presented in Table 6. The same result is also given in the plots of Figure 10 for comparison at a glance.

Table 6 provides the NC values of the recovered watermark under different attacks on Lena image watermarked using the proposed scheme and the schemes of Lai, Makbol et al. Zhang et al., and Ernawan and Kabir. It can be checked that overall, the Lai scheme produces the worst result followed by the Zhang scheme. However, the Makbol scheme provides better result except for two cases – average filter and cropping (top 25%) as shown in the table. In particular, among the schemes, it is the most vulnerable scheme to average filter. Overall, the Lagzian and Ernawan schemes produce good results; however, the Ernawan scheme significantly suffers from scaling attacks (rescaling (0.5, 2)). On an average, our technique outperforms most of the schemes. However, for cropping, scaling and filtering, the Lagzian scheme appears to be slightly better. Our technique is compared to existing watermarking techniques of Roy and Pal [17] and Das *et al.* [18] as presented in Table 5. Comparison to our scheme is visualized in the plots of Figure 11.

In Li *et al.* [7] presented a feature for scaling the intensity of embedding the watermark by gain factor. The watermark is embedded in the middle Tchebichef moment with scaling factor about 40. Although the authors are successful in improving the robustness to affine signal processing attacks, that scheme can recovered the watermark after Gaussian low pass filter with NC about 0.9791.

In this research, our scheme demonstrates improvement of the robustness to Gaussian low pass filter, since the NC value is equal to one after Gaussian low pass filter attack. Referring to Table 5, our scheme shows an improvement on the extracted watermark in terms of NC value toward Gaussian low pass filter, image sharpening, cropping, salt and pepper noise, Gaussian noise and histogram equalization than the Roy scheme, Das scheme and Lai scheme. The robustness of our technique compared to the other schemes against JPEG and JPEG2000 is shown in Figures 12.

Figures 12 provide the NC values of the extracted watermark with different levels of JPEG and JPEG2000 compression on Lena image watermarked by our scheme and the other schemes developed by Lai, Makbol et al., and Ernawan and Kabir. It is noticed from the figures that for JPEG compression, the proposed scheme is initially (i.e., with a quality factor, QF=20) the best in the schemes. But when QF increases, the Makbol scheme gives better result. However, the other schemes are worse than the proposed scheme. When QF>48, our scheme performs the best. For JPEG2000, our scheme clearly outperforms other schemes. The comparison of NC values among Lai's scheme [5], Makbol's scheme [6],

TABLE 9. Recovered watermark images after simulated image-processing attacks on the host images watermarked by attacks for Lai's scheme, Makbol's scheme and our scheme.

Image Processing Attack	Lena			Pepper		
	Lai's Scheme	Makbol's scheme	Our Scheme	Lai's Scheme	Makbol's scheme	Our Scheme
No attack						
Average Filter (3,3)						
Wiener Filter (3,3)						
Median Filter (3,3)						
Gaussian Low Pass Filter (3,3)						
Gaussian Noise (var=0.005)						
Gaussian Noise (var=0.003)						
Gaussian Noise (var=0.001)						
Speckle Noise (var=0.01)						
Speckle Noise (var=0.005)						
Speckle Noise (var=0.003)						
Speckle Noise (var=0.001)						
Pepper and Salt Noise (density=0.01)						
Pepper and Salt Noise (density=0.005)						
Pepper and Salt Noise (density=0.003)						
Pepper and Salt Noise (density=0.001)						
Sharpening						
Poisson Noise						
Adjust						
Histogram Equalization Attack						

TABLE 10. Recovered watermark images after simulated geometrical attacks on the host images watermarked by Lai's scheme, Makbol's scheme and our scheme.

Geometrical Attack	Lena			Pepper		
	Lai's Scheme	Makbol's scheme	Our Scheme	Lai's Scheme	Makbol's scheme	Our Scheme
Centred Cropping 25% (128x128 by black)						
Centred Cropping 50% (256x256 by black)						
Centred Cropping 25% (128x128 by white)						
Centred Cropping 50% (256x256 by white)						
Cropping rows off 50% (256 rows by black)						
Cropping rows off 25% (128 rows by black)						
Cropping rows off 12.5% (64 rows by black)						
Cropping rows off 50% (256 rows by white)						
Cropping rows off 25% (128 rows by white)						
Cropping rows off 12.5% (64 rows by white)						
Cropping columns off 50% (256 columns by black)						
Cropping columns off 25% (128 columns by black)						
Cropping columns off 12.5% (64 columns by black)						
Cropping columns off 50% (256 columns by white)						
Cropping columns off 25% (128 columns by white)						
Cropping columns off 12.5% (64 columns by white)						
Scaling 0.8						
Scaling 0.5						
Croping column off 25% at top-left corner by white						
25% Cropping at top-right corner by white						
25% Cropping at bottom-left corner by white						
25% Cropping at bottom-right corner by white						
Combination Pepper & Salt (density=0.003) and Median Filter (3,3)						

TABLE 11. Watermark recovery images under different levels of compressed image for Lai's scheme, Makbol's scheme and our scheme.

Compression Attack	Lena			Pepper		
	Lai's Scheme	Makbol's scheme	Our Scheme	Lai's Scheme	Makbol's scheme	Our Scheme
JPEG with *QF* =50						
JPEG with *QF* =60						
JPEG with *QF* =70						
JPEG with *QF* =80						
JPEG with *QF* =90						
Combination JPEG and Centre Cropping						
JPEG2000 with *CR*=2						
JPEG2000 with *CR*=4						
JPEG2000 with *CR*=6						
JPEG2000 with *CR*=8						
JPEG2000 with *CR*=10						
JPEG2000 with *CR*=12						
JPEG2000 with *CR*=14						
JPEG2000 with *CR*=16						
JPEG2000 with *CR*=18						

Ernawan & Kabir's scheme [19], and the proposed scheme is shown in Figures 13 and 14.

Figures 13-14 plot the bar graphs of NC values under different geometric and image-processing attacks on the watermarked Lena image with the proposed scheme and the other schemes developed by Lai, Makbol et al. and Ernawan & Kabir. It can be checked that our technique has a good robustness after various attacks. The mean NC value was 0.96, which indicates a good visual quality in the extracted watermarks. The plots demonstrate that our scheme is the most robust under geometric and image-processing attacks.

In these experiments, our scheme is also evaluated by standard software checkmark [26]. This software is used to test the robustness performance of the proposed scheme. The results obtained from Stirmark software [26] are listed in Table 7.

C. COMPUTATIONAL TIME

Computational time of the proposed watermarking technique was evaluated to assess its performance. It is mentioned earlier that the experiments were conducted on MATLAB 2014a running on a CPU Intel Core i5-6200U CPU @ 2.30GHz 2.40 GHz processor with 16-GB RAM under Windows 10 operating system. Computational complexity in seconds is provided for the proposed scheme in Table 6. In the table, we notice that our scheme requires the least computational time followed by Lai and Makbol schemes. The computational cost of embedding is higher than that of extraction. Makbol's scheme has the highest computational cost. The watermarked images after attacked is shown in Figures 15 and 16. The recovered watermark images after simulated attacked are depicted in Tables 8, 9 and 10.

Our scheme is suitable for embedding a watermark into the grayscale or luminance channel. If, in this scheme, embedding a watermark is made into chrominance channels, the watermark would be destroyed in case of image compression due to quantization process. A large amount of quantization values for chrominance channels may damage the embedded watermark image. The proposed scheme produces slightly less invisibility (measured by PSNR value) than the scheme by Ernawan [20], while our scheme significantly improved robustness performance against noise addition and JPEG 2000.

VII. CONCLUSION

This paper presents an image watermarking technique built on Tchebichef moments for copyright protection. HVS entropy was calculated for each image block and the blocks with lower entropy are selected for watermark embedding. Psychovisual threshold is used to determine the lower entropy that is resilient against JPEG compression. Arnold transform is used to the scramble watermark image and the scrambled watermark bits are embedded into the host image. In the proposed scheme, the watermark is embedded by modifying certain coefficients of Tchebichef moments of the embedding blocks. The proposed scheme provides average imperceptibility of 40 dB and robustness with NC value of 0.88 under JPEG compression with QF=10. We conducted further tests on the proposed technique under different attacks and is compared to the existing watermarking schemes. Our scheme provides satisfactory performance against JPEG compression, image sharpening, noise addition, median filter and image cropping. It is noticed that our technique has better robustness than the existing techniques under image-processing attacks. Our method cannot be used for embedding into chrominance channels, since embedding into chrominance channels would damage the watermark due to large quantization values associated with chrominance channels. Our scheme can be used for embedding watermark into the grayscale image or luminance channel. Thus, a grayscale image is most suitable for the proposed scheme. For the future work, further improvement may be made by enhancing sufficient level of imperceptibility and robustness under rotational and translational attacks.

REFERENCES

[1] N. Singhal, Y.-Y. Lee, C.-S. Kim, and S.-U. Lee, "Robust image watermarking using local Zernike moments," *J. Vis. Commun. Image Represent.*, vol. 20, no. 6, pp. 408–419, Aug. 2009.
[2] G. A. Papakostas, E. D. Tsougenis, and D. E. Koulouriotis, "Near optimum local image watermarking using Krawtchouk moments," in *Proc. IEEE Int. Conf. Imag. Syst. Techn.*, Jul. 2010, pp. 464–467.
[3] E. D. Tsougenis, G. A. Papakostas, D. E. Koulouriotis, and V. D. Tourassis, "Performance evaluation of moment-based watermarking methods: A review," *J. Syst. Softw.*, vol. 85, no. 8, pp. 1864–1884, Aug. 2012.
[4] G. A. Papakostas, E. D. Tsougenis, and D. E. Koulouriotis, "Moment-based local image watermarking via genetic optimization," *Appl. Math. Comput.*, vol. 227, pp. 222–236, Jan. 2014.
[5] C.-C. Lai, "An improved SVD-based watermarking scheme using human visual characteristics," *Opt. Commun.*, vol. 284, no. 4, pp. 938–944, Feb. 2011.
[6] N. M. Makbol, B. E. Khoo, and T. H. Rassem, "Block-based discrete wavelet transform-singular value decomposition image watermarking scheme using human visual system characteristics," *IET Image Process.*, vol. 10, no. 1, pp. 34–52, Jan. 2016.
[7] J. Li, Z. Zhang, D. Wang, and X. Zhang, "A blind and robust digital watermarking algorithm based on discrete orthogonal tchebichef moment," in *Proc. Int. Conf. Comput. Inf. Sci.*, 2014, pp. 365–370.
[8] F. Ernawan, M. N. Kabir, M. Fadli, and Z. Mustaffa, "Block-based tchebichef image watermarking scheme using psychovisual threshold," in *Proc. 2nd Int. Conf. Sci. Technol.-Comput.*, Oct. 2016, pp. 6–10.
[9] S. Lagzian, M. Soryani, and M. Fathy, "Robust watermarking scheme based on RDWT-SVD: Embedding data in all subbands," in *Proc. Int. Symp. Artif. Intell. Signal Process. (AISP)*, Jun. 2011, pp. 48–52.
[10] N. M. Makbol and B. E. Khoo, "Robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition," *Int. J. Electron. Commun.*, vol. 67, no. 2, pp. 102–112, Feb. 2013.
[11] H.-C. Ling, R. C.-W. Phan, and S.-H. Heng, "Comment on 'robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition,'" *Int. J. Electron. Commun.*, vol. 67, no. 10, pp. 894–897, Oct. 2013.
[12] E. Yavuza and Z. Telatarb, "Comments on 'sssa digital watermarking scheme based on singular value decomposition and tiny genetic algorithm,'" *Digit. Signal Process.*, vol. 23, no. 4, pp. 1335–1336, Jul. 2013.
[13] X.-P. Zhang and K. Li, "Comments on 'an SVD-based watermarking scheme for protecting rightful ownership,'" *IEEE Trans. Multimedia*, vol. 9, no. 2, pp. 421–423, Feb. 2007.
[14] A. Mishra, C. Agarwal, A. Sharma, and P. Bedi, "Optimized gray-scale image watermarking using DWT–SVD and firefly algorithm," *Expert Syst. Appl.*, vol. 41, no. 17, pp. 7858–7867 Dec. 2014.
[15] M. Ali and C. W. C. W. Ahn, "Comments on 'optimized gray-scale image watermarking using DWT-SVD and firefly algorithm,'" *Expert Syst. Appl.*, vol. 42, no. 5, pp. 2392–2394, Apr. 2015.
[16] H. Zhang, C. Wang, and X. Zhou, "A robust image watermarking scheme based on SVD in the spatial domain," *Future Internet*, vol. 9, no. 45, p. 45, Aug. 2017.
[17] S. Roy and A. K. Pal, "A blind DCT based color watermarking algorithm for embedding multiple watermarks," *AEU Int. J. Electron. Commun.*, vol. 72, pp. 149–161, Feb. 2017.
[18] C. Das, S. Panigrahi, V. K. Sharma, and K. K. Mahapatra, "A novel blind robust image watermarking in DCT domain using inter-block coefficient correlation," *Int. J. Electron. Commun.*, vol. 68, no. 3, pp. 244–253, Mar. 2014.
[19] F. Ernawan and M. N. Kabir, "A robust image watermarking technique with an optimal DCT-psychovisual threshold," *IEEE Access*, vol. 6, pp. 20464–20480, 2018.
[20] S. P. Maity and M. K. Kundu, "Perceptually adaptive spread transform image watermarking scheme using Hadamard transform," *Inf. Sci.-Inform. Comput. Sci., Intell. Syst., Appl. Int. J.*, vol. 181, no. 3, pp. 450–465, Feb. 2011.
[21] N. A. Loan, N. N. Hurrah, S. A. Parah, J. W. Lee, J. A. Sheikh, and G. M. Bhat, "Secure and robust digital image watermarking using coefficient differencing and chaotic encryption," *IEEE Access*, vol. 6, pp. 19876–19897, 2018.

[22] A. Shehab, M. Elhoseny, K. Muhammad, A. K. Sangaiah, P. Yang, H. Huang, and G. Hou, "Secure and robust fragile watermarking scheme for medical images," *IEEE Access*, vol. 6, pp. 10269–10278, 2018.
[23] F. Ernawan, N. Kabir, and K. Z. Zamli, "An efficient image compression technique using tchebichef bit allocation," *Optik*, vol. 148, pp. 106–119, Nov. 2017.
[24] F. Ernawan, "Tchebichef image watermarking along the edge using YCoCg-R color space for copyright protection," *Int. J. Electr. Comput. Eng.*, vol. 9, no. 3, pp. 1850–1860, Jun. 2019.
[25] F. Ernawan, N. Kabir, and J. M. Zain, "Bit allocation strategy based on Psychovisual threshold in image compression," *Multimedia Tools Appl.*, vol. 77, no. 11, pp. 13923–13946, Jun. 2018.
[26] F. Petitcolas. (2002). *Stirmark Benchmark*. [Online]. Available: https://www.petitcolas.net/fabien/watermarking/stirmark/

FERDA ERNAWAN was born in Semarang, Central Java, Indonesia, in 1988. He received the master's degree in software engineering and intelligence and the Ph.D. degree in image processing from the Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, in 2011 and 2014, respectively. He is currently a Senior Lecturer with the Faculty of Computer Systems & Software Engineering, Universiti Malaysia Pahang. His research interests include image compression, and digital watermarking and steganography. (Scopus ID: 53663438800).

MUHAMMAD NOMANI KABIR received the M.Sc. degree in computational sciences in engineering and the Ph.D. degree in computer science from the University of Braunschweig, Germany. He is currently a Senior Lecturer with the Faculty of Computer Systems & Software Engineering, Universiti Malaysia Pahang, Malaysia. His research interests include issues related to modeling and simulation, computational methods, image processing, and computer networks.