A High Payload Steganography Mechanism Based on Wavelet Packet Transformation and Neutrosophic Set

Randa Atta, Mohammad Ghanbari

PII: S1047-3203(18)30057-9
DOI: https://doi.org/10.1016/j.jvcir.2018.03.009
Reference: YJVCI 2156

To appear in: *J. Vis. Commun. Image R.*

Received Date: 14 June 2017
Revised Date: 3 February 2018
Accepted Date: 3 March 2018

Please cite this article as: R. Atta, M. Ghanbari, A High Payload Steganography Mechanism Based on Wavelet Packet Transformation and Neutrosophic Set, *J. Vis. Commun. Image R.* (2018), doi: https://doi.org/10.1016/j.jvcir.2018.03.009

A High Payload Steganography Mechanism Based on Wavelet Packet Transformation and Neutrosophic Set

Randa Atta[1] and Mohammad Ghanbari[2,3], Life Fellow, IEEE

[1] Electrical Engineering Department, Port Said University, Port Said, 42523, Egypt
E-mail: r.atta@eng.psu.edu.eg
[2] School of Electrical and Computer Engineering, College of Engineering, University of Tehran, Tehran, Iran, E-mail, ghan@ut.ac.ir
[3] School of Computer Science and Electronic Engineering, University of Essex, Colchester, UK, CO4 3SQ, E-mail: ghan@essex.ac.uk

Abstract

In this paper a steganographic method is proposed to improve the capacity of the hidden secret data and to provide an imperceptible stego-image quality. The proposed steganography algorithm is based on the wavelet packet decomposition (WPD) and neutrosophic set. First, an original image is decomposed into wavelet packet coefficients. Second, the generalized parent-child relationships of spatial orientation trees for wavelet packet decomposition are established among the wavelet packet subbands. An edge detector based on the neutrosophic set named (NSED) is then introduced and applied on a number of subbands. This leads to classify each wavelet packet tree into edge/non-edge tree to embed more secret bits into the coefficients in the edge tree than those in the non-edge tree. The embedding is done based on the least significant bit substitution scheme. Experimental results demonstrate that the proposed method achieves higher embedding capacity with better imperceptibility compared to the published steganographic methods.

Key Words— Image Steganography, Wavelet Packet Transformation, Neutrosophic Set, Edge Detection.

1. Introduction

Due to the development of computer networks, internet and digital media, the information security has become increasingly important. Several techniques such as cryptography, steganography, coding, are widely used in the field of information security to manipulate information messages such as data hiding. The information security systems provide two main disciplines: information encryption and information hiding [19, 20]. Information encryption, or cryptography, is a process of scrambling the data such that it cannot be understood. On the other hand, information hiding, as the name implies is to make sure the added information is invisible. It can be further classified into watermarking and steganography [19, 20]. Watermarking is used to protect the copyright and it guarantees the integrity of the transmitted data.

Steganography is a technique of hiding an information message into a cover object (as a text, image, video, or audio segment) such that a human observer cannot perceive that message. Among the different kind of cover objects, the digital image is commonly used as a host image to convey information message in it. Steganographic system starts hiding information by indicating the redundant bits in the cover image, the bits which can be modified without destroying the object. These redundant bits are replaced with data from the secret message to create a stego-image.

Unlike the watermarking techniques in which the robustness against attacks is its objective, the steganography techniques pay more attention to the three aspects: capacity, imperceptibility and security against steganalysis. Capacity (payload) refers to the number of secret bits which can be embedded in the cover image. Imperceptibility refers to inability of observer to distinguish between cover image and stego-image. Thus, designing an effective steganography scheme requires maintaining the imperceptibility of the important data, increasing the payload rate and ensuring security against steganalysis. Many steganalytic methods are used to detect the existence of hidden message in the cover images such as visual and statistical attacks [23-25]. In [25], Fridrich et al. have employed a dual statistical method to detect the presence of hidden message in the cover images.

In the literature, several image steganography techniques have been proposed [1–22] and they can be classified into two categories of spatial domain techniques and frequency-domain techniques. In the spatial domain steganography techniques [1-12], the secret messages are embedded directly into the cover image. One of these techniques is based on the least-significant-bit (LSB) substitution by utilizing some rules to replace LSBs of the cover image with the secret message [1–3]. Although these methods are simple and typically achieve high capacity with low computational complexity, their embedding capacity is not satisfactory. Some studies [5-12] have taken into account the characteristics of the human visual system to improve the embedding capacity. These methods usually embed more secret message into areas with higher spatial variations such as edges than the smooth areas since visibility of the embedded data around edges and highly detailed areas can be masked. Some of these methods discriminate between edged areas/pixels and smooth areas/pixels by utilizing either pixel-value differencing (PVD) [4-6, 9-10] or edge detectors [11, 12] such as Canny and fuzzy edge detectors.

On the other hand, several frequency domain techniques [13-18] have been proposed to obtain large capacity steganography and maintaining high fidelity (invisibility) simultaneously. In the frequency domain methods, the cover image is transformed into frequency domain coefficients using one of the most popular transforms such as the discrete wavelet transform (DWT), wavelet packet, and Discrete Cosines Transform (DCT). These transform coefficients are manipulated to hide the secret message among themselves. The stego-image is then obtained by applying the inverse transformation. In [13], a DCT-based steganographic method for images was proposed. The method takes into consideration the similarities of the DCT coefficients between the adjacent image blocks to embed the secret message by quantizing the difference of the coefficients instead of the coefficients themselves. In [14], an adaptive data hiding technique based on discrete wavelet transform was proposed. The cover image is partitioned into 8×8 non overlapping blocks and the Haar wavelet transform is then applied on each block. A data hiding capacity function is defined to determine the capacity of the embedding secret message in the transform coefficients. In [15] a similar adaptive data hiding technique with an optimum pixel adjustment algorithm (OPA) was proposed to minimize the embedding error. Bhattacharyya et al. [16] introduced a steganographic scheme based on integer wavelet transform (IWT) through a lifting scheme. In this method, the stego-image is obtained by using the pixel mapping method (PMM) to embed two bits of the secret message into the selected subband coefficients. However, the quality of the stego-image and the size of the payload produced using this method are low. Consequently, for further improvement in the hiding capacity, Seyyedi and Ivanov [17] also proposed a steganography technique based on integer wavelet transform. The cover image is divided into 8×8 non-overlapping blocks and 2D IWT is applied to each block. The coefficients in each transformed block are then partitioned into two subsets and the secret message is embedded in the proper subset.

The key aim in all of the image steganography methods whether spatial or transform is to increase the data hiding capacity without causing any noticeable distortions in the cover image. Therefore, in this paper, a steganographic technique based on WPD and neutrosophic set (NS) is proposed. The proposed approach has the following advantages: 1) the approach is hierarchical which facilitates constructing wavelet packet trees (WPTs), the status of each tree (which consists of a number of coefficients) is represented by only one bit. This leads to preserve the quality of the stego-image; 2) the embedded secret message is hardly detectable by the human visual system (HVS) due to adding more embedding bits in the edge trees than the non-edge ones; 3) high payload is hidden due to the proposed Neutrosophic Set-based Edge Detector (NSED); and 4) the proposed method is robust against statistical RS, pixel difference histogram and universal steganalysis.

The remainder of the paper is organized as follows: the introduced edge detection approach is given in Section 2. Section 3 describes the proposed embedding and extraction procedures. In Section 4, experimental results are presented, and, finally, the paper is concluded in Section 5.

2. Neutrosophic set-based edge detection (NSED)

Edge detection is an important issue in image processing and analysis. It is used in a wide range of applications such as image enhancement, recognition, compression, retrieval, watermarking, hiding, and segmentation [26]. Numerous methods of edge detection have been proposed to detect edges in still images. Among them the gradient-based edge detection methods such as Sobel, Canny, Robert, Prewitt are most popular. In these methods, a pixel is classified as an edge if the value of its gradient is greater than a threshold. The performance of these methods is limited because they are very sensitive to noise.

Recently fuzzy logic-based edge detection techniques have also been proposed [27-30]. The image in reality is fuzzy and the edges are not clear since each pixel of an image has a degree of belonging to a region or a boundary. Fuzzy theory has been applied into edge detection due to its powerful ability to deal with the ambiguity within an image. Amarunnishad et al. [27] proposed a simple fuzzy complement edge operator which is able to detect a large number of edge pixels in an image and it provides a better visual quality edge image than the competitive fuzzy edge detector (CFED) proposed by Liang and Looney [28]. To increase the number of edge pixels, Chen et al [11] proposed a hybrid edge detector. In this method, the 'Canny' edge detector and the fuzzy complement edge operator were combined. Several methods have been proposed based on fuzzy rules [29, 30]. In most of these methods, adjacent pixels around a center are assumed to be in some classes. Fuzzy system inference is then implemented using an appropriate membership function defined for each class. In [29], a simple fuzzy logic-based edge detection algorithm was proposed. The algorithm scans the image using a 2×2 pixels window. Fuzzy inference system has four inputs, which are the four pixels within the scanning window, and one output that decides whether the pixel under consideration is “black”, “white” or “edge” pixel. This method uses sixteen fuzzy rules to investigate discontinuity of adjacent points around a specific pixel. For a better edge detection performance, a similar method was proposed in [30] with a modification to the number of inputs, where eight inputs are used and produced from the scanning the image using a 3×3 pixels window. The trapezoidal and the triangular membership functions are then used for the inputs and the output respectively. Finally, existence of edges is determined by considering the membership values and applying fuzzy rules. Although fuzzy logic-based edge detection algorithms are more flexible and robust than the gradient-based edge detection methods, they are more computationally expensive.

To overcome the drawbacks of the existing edge detection methods, in this paper an edge detection method is developed based on neutrosophic set theory. Since the proposed image steganography technique is based on wavelet transform, WPD of the cover image is first transformed into the neutrosophic set (NS). α-mean and β-enhancement operations are then defined and employed to reduce the indeterminacy degree of the image, which is measured by the entropy of the indeterminate set. Finally, the edges are obtained in the neutrosphic set (NS) domain based on the gradients in two orthogonal directions. Details of the neutrosophic set and the introduced edge detection approach will be discussed in the next subsections.

2.1 Neutrosophic image

Florentin Smarandache [31] proposed neutrosophic set (NS) as a new branch of philosophy dealing with the origin, nature, and scope of neutralities. In neutrosophy theory, every event not only has a certain degree of truth, but it also has a falsity degree and an indeterminacy degree which are independent from each other. It considers a theory, event, concept, or entity {A} in relation to its opposite {Anti-A} and the neutrality {Neut-A}, which is neither {A} nor {Anti-A}. Neutrosophy is the basis of neutrosophic sets and neutrosophic statistics. In a neutrosophic set, a set A is represented by three subsets: {A}, {Neut-A} and {Anti-A}, which are defined as truth, indeterminacy, and false subsets, respectively. NS provides a powerful tool to deal with the indeterminacy which is described using a membership. It was applied to image processing techniques, such as image segmentation, thresholding and denoising.

An image is transformed into neutrosophic domain where a neutrosophic image P_{NS} is defined by three membership sets T, I and F. In other words, a pixel $P(i, j)$ in the image domain is transformed into the neutrosophic domain, $P_{NS}(i, j) = \{T(i, j), I(i, j), F(i, j)\}$, where $T(i, j)$, $I(i, j)$ and $F(i, j)$ are the membership values belonging to true (edge pixel) set, indeterminate set and false (non-edge pixel) set, respectively, which are defined as follows [32, 33]:

$$T(i,j)=\frac{\bar{g}(i,j)-\bar{g}_{\min}}{\bar{g}_{\max}-\bar{g}_{\min}}. \qquad (1)$$

$$\bar{g}(i,j)=\frac{1}{w\times w}\sum_{m=i-w/2}^{i+w/2}\sum_{n=j-w/2}^{j+w/2}g(m,n), \qquad (2)$$

$$I(i,j)=\frac{\delta(i,j)-\delta_{\min}}{\delta_{\max}-\delta_{\min}}, \qquad (3)$$

$$\delta(i,j)=abs(g(i,j)-\bar{g}(i,j)), \qquad (4)$$

$$F(i,j)=1-T(i,j), \qquad (5)$$

where $g(i, j)$ is the intensity value of the pixel at (i, j), $\bar{g}(i,j)$ is the local mean value of $g(i, j)$ in a window of $w\times w$ pixels and $\delta(i,j)$ is the absolute value of the difference between intensity value $g(i, j)$ and its local mean value $\bar{g}(i,j)$ at coordinate (i, j). The value of $I(i, j)$ is used to measure the indeterminacy degree of element $P_{NS}(i, j)$. When T and F are correlated with I, the changes in T and F affect the pixel distribution of element in I and its entropy. α-mean and β-enhancement operations are then performed to reduce the set indeterminacy in the NS image.

First, the α-mean operation for P_{NS}, which is the mean value between the pixel neighbors in NS ($\bar{P}_{NS}(\alpha)$), is defined as:

$$\bar{P}_{NS}(\alpha) = P(\bar{T}(\alpha), \bar{I}(\alpha), \bar{F}(\alpha)), \qquad (6)$$

$$\bar{T}(\alpha) = \begin{cases} T & \text{if } I < \alpha, \\ \bar{T}_\alpha & \text{otherwise}, \end{cases} \qquad (7)$$

$$\bar{T}_\alpha(i,j) = \frac{1}{w \times w} \sum_{m=i-w/2}^{i+w/2} \sum_{n=j-w/2}^{j+w/2} T(m,n), \qquad (8)$$

$$\bar{F}(\alpha) = \begin{cases} F & \text{if } I < \alpha, \\ \bar{F}_\alpha & \text{otherwise}, \end{cases} \qquad (9)$$

$$\bar{F}_\alpha(i,j) = \frac{1}{w \times w} \sum_{m=i-w/2}^{i+w/2} \sum_{n=j-w/2}^{j+w/2} F(m,n), \qquad (10)$$

$$\bar{I}_\alpha(i,j) = \frac{\bar{\delta}_T(i,j) - \bar{\delta}_{T\min}}{\bar{\delta}_{T\max} - \bar{\delta}_{T\min}}, \qquad (11)$$

$$\bar{\delta}_T(i,j) = abs(\bar{T}(i,j) - \bar{\bar{T}}(i,j)), \qquad (12)$$

$$\bar{\bar{T}}(i,j) = \frac{1}{w \times w} \sum_{m=i-w/2}^{i+w/2} \sum_{n=j-w/2}^{j+w/2} \bar{T}(m,n), \qquad (13)$$

where $\bar{\delta}_T(i,j)$ is the absolute value of the difference between the local mean intensity value of *T*(*i,j*) ($\bar{T}(i,j)$) and its local mean value $\bar{\bar{T}}(i,j)$. After performing the α-mean operation, the entropy of the indeterminate subset *I* is increased and then the distribution of the elements in *I* becomes more uniform.

Second, the β-enhancement operation for P_{NS}, $P'_{NS}(\beta)$, is computed as:

$$P'_{NS}(\beta) = P(T'(\beta), I'(\beta), F'(\beta)), \qquad (14)$$

$$T'(\beta) = \begin{cases} T & \text{if } I < \beta, \\ T'_\beta & \text{if } I \geq \beta, \end{cases} \qquad (15)$$

$$T'_\beta(i,j) = \begin{cases} 2T^2(i,j) & \text{if } T(i,j) \leq 0.5, \\ 1 - 2(1 - T(i,j))^2 & \text{if } T(i,j) > 0.5, \end{cases} \qquad (16)$$

$$I'_\beta(i,j) = \frac{\delta'_T(i,j) - \delta'_{T\min}}{\delta'_{T\max} - \delta'_{T\min}}, \qquad (17)$$

$$\delta'_T(i,j) = abs(T'(i,j) - \bar{T}'(i,j)), \qquad (18)$$

$$\bar{T}'(i,j) = \frac{1}{w \times w} \sum_{m=i-w/2}^{i+w/2} \sum_{n=j-w/2}^{j+w/2} T'(m,n), \qquad (19)$$

where $\delta'_T(i,j)$ is an absolute value of the difference between the intensity value $T'(i,j)$ and its local mean value $\bar{T}'(i,j)$. After the β- enhancement operation, the set *T* becomes more distinct and is suitable for edge detection.

2.2. Neutrosophic edge detector

In this paper, a secret message is embedded into a cover image on the wavelet domain to improve the robustness. A 2-level wavelet packet decomposition (WPD) is performed on a cover image. This results in an approximation subband (AA) and a number of detailed subbands. Only AH, AV and AD subbands are transformed into the neutrosophic domain NS using Eqs. (1)–(5). The indeterminacy of the NS image P_{NS} is then decreased using the α-mean and β-enhancement operations on subset T of each subband using Eqs.(6)–(19) until the entropy of the indeterminate subset I of each subband becomes unchanged. Finally, the horizontal and vertical gradients (G_x and G_y) of the pixels in T of each subband are used to evaluate whether the pixels belong to edge pixels or not, as follows:

$$eg(i,j) = \sqrt{G_x^2 + G_y^2}$$

$$E(i,j) = \begin{cases} 1 & \text{if } eg(i,j) > \gamma, \\ 0 & \text{otherwise,} \end{cases} \qquad (20)$$

where eg is the magnitude of the gradients. Sobel operator was used to calculate G_x and G_y. The threshold value of gradient γ was selected to determine whether the pixels were edge pixels or non-edge pixels. The general procedure of the introduced neutrosophic set-based edge detection (NSED) algorithm is shown in Fig. 1.

3. Proposed Stegnographic Scheme

In the proposed method, after performing 2-level of WPD, wavelet packet tree (WPT) is constructed as shown in Fig. 2. There are 16 subbands of three WPTs (T_1, T_2, and T_3) rooted in the lowest frequency or the coarsest scaled subband. The coefficient at the coarsest scaled subband is called root (R). The coefficient at the coarsely scaled subband is called the parent, and all the coefficients corresponding to the same spatial location at the next finer scaled subbands of similar orientation are called children. The root coefficients, in the approximation subband (AA), are not modified during the embedding process since they are the most important coefficients and any modifications on them can lead to more distortion of stego-image quality. The secret message is embedded in the coefficients of the three WPTs (T_1, T_2, and T_3) corresponding to parent-children coefficients by using LSB substitution.

Let R denote the node representing the lowest frequency subband (AA). It represents the root node of an overall tree consisting of three primary T_1, T_2, and T_3 which represent the coarsest high frequency subbands (AH, AV, AD) respectively. In other words, in the wavelet packet trees (WPTs) each parent subband node is followed by exactly four children subbands of similar orientation at the next finer resolution. Thus, each coefficient of the parent node is associated with four coefficients, one coefficient of each child node, at the same spatial location. The secret message bits are embedded into three primary trees starting from T_1, T_2, and T_3. Each WPT includes five coefficients, where for example the primary tree T_1 consists of one C_1 coefficient in the AH subband and four coefficients (c_{11}, c_{12}, c_{13}, and c_{14}) one in each subband HA, HH, HV, and HD, respectively.

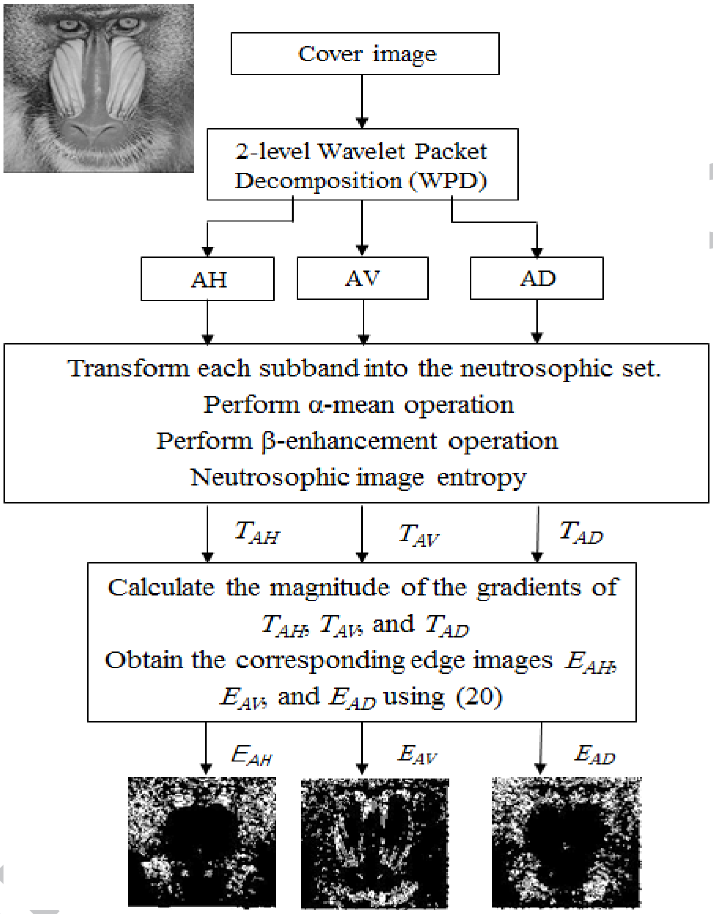
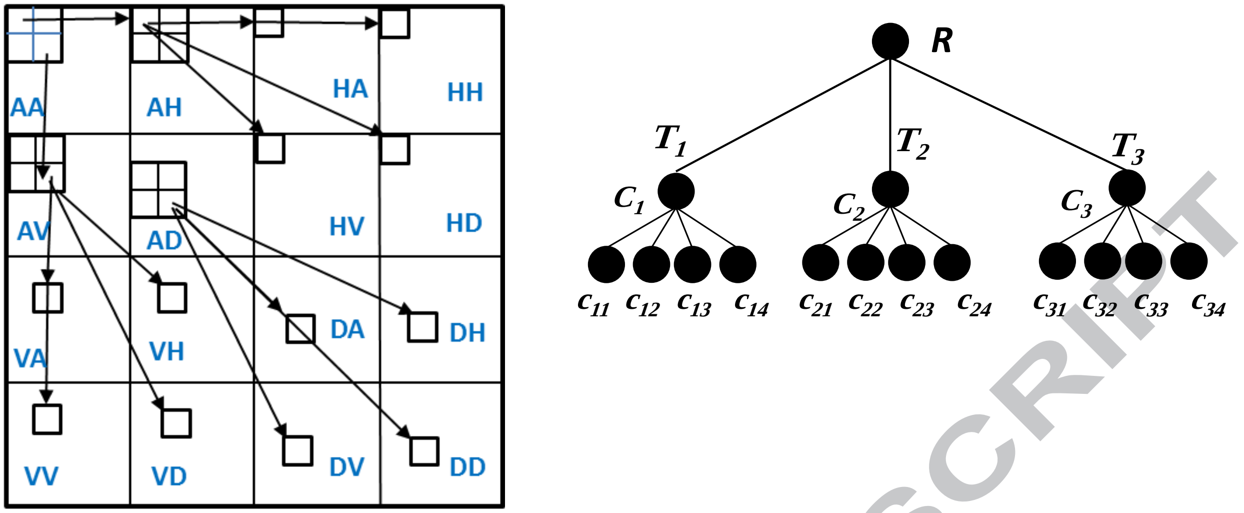

Cover image
2-level Wavelet Packet Decomposition (WPD)
AH
AV
AD
Transform each subband into the neutrosophic set.
Perform α-mean operation
Perform β-enhancement operation
Neutrosophic image entropy
T_{AH}
T_{AV}
T_{AD}
Calculate the magnitude of the gradients of T_{AH}, T_{AV}, and T_{AD}
Obtain the corresponding edge images E_{AH}, E_{AV}, and E_{AD} using (20)
E_{AH}
E_{AV}
E_{AD}

Fig. 1. Flow chart of the introduced Neutrosophic set-based edge detection (NSED).


AA
AH
HA
HH
AV
AD
HV
HD
VA
VH
DA
DH
VV
VD
DV
DD
R
T_1
T_2
T_3
C_1
C_2
C_3
c_{11} c_{12} c_{13} c_{14}
c_{21} c_{22} c_{23} c_{24}
c_{31} c_{32} c_{33} c_{34}

(a)

(b)

Fig. 2. Example of parent–children relations across subbands. (a) two-level wavelet packet decomposition (WPD). (b) Wavelet packet (WP) tree for a 2-level WPD of (a).

3.1. Embedding procedure

The first stage of the embedding process is to apply the presented NSED edge detection algorithm explained in Section 2.2 on the parent subband nodes (AH, AV, and AD) to obtain the corresponding edge images E_{AH}, E_{AV}, and E_{AD} respectively. These edge images have the same sizes of the subbands AH, AV, and AD. The second stage is to determine the type of each primary tree according to the type of each pixel in the edge images as follows: If a pixel in an edge image is defined as edge/non-edge pixel, the wavelet coefficient in the corresponding (a coarse scale) parent node at the same spatial location is also an edge/non-edge coefficient. Then all the wavelet descendent coefficients of the same orientation in the same spatial location at finer scaled subbands are likely to be edge/non-edge coefficients. Therefore, the corresponding primary WPT is also defined as edge/non-edge tree. The coefficients C_1, C_2, and C_3 in the subbands AH, AV, and AD are used to store the status of the three primary trees T_1, T_2, and T_3, respectively. The status of each primary tree, T_i is defined as ‘1’/'0' if T_i is an edge/non-edge tree. Unlike other embedding algorithms [11] and [12], where the status of each pixel is stored, the status of each primary tree is represented by one bit and is stored inside the LSB of coefficient C_i. This leads to maintain the quality of the stego-image.

After embedding the status of a primary tree in the LSB of coefficient C_i, the last stage of the embedding process is to embed the secret message bits into each primary tree starting from T_1, then T_2 and finally T_3. For instance, to embed the secret message bits into T_1, a bit of the secret message is embedded into the second LSB of C_1. The remaining secret bits are then embedded into the four descendent/children coefficients (c_{11}, c_{12}, c_{13}, and c_{14}) at finer scaled subbands (HA, HH, HV, and HD) according to the type of the primary tree T_1. If the type of tree is non-edge then k bits of the secret message are inserted into each child coefficient using the LSBs substitution technique. But if the type of tree is edge then k+1 LSBs in each descendent coefficient are replaced with k+1 secret message bits. That is because due to human visual masking at edges, the edge coefficient has higher priority to embed more embedding bits than the non-edge coefficient. Unlike [11], only one parameter k represents the number of non-edge's in the proposed scheme.

To explain the proposed embedding algorithm in detail, suppose a primary tree T_1 is taken out of a WPT which its root R is located at a spatial coordinate (x, y). Its five coefficients $C_1(x, y)$, $c_{11}(x, y)$, $c_{12}(x, y)$, $c_{13}(x, y)$, and $c_{14}(x, y)$ have values of -42, -18, 2, 21, and -3, respectively. The binary representation of each wavelet coefficient is the binary representation of the absolute value of the wavelet coefficient concatenated with a bit representing the sign bit which is located at the most significant bit (MSB). In other words, each wavelet coefficient is represented by (n+1) bits, where n is the number of bits used to represent the maximum magnitude of the wavelet coefficients $c_{\max}$ and equals $n = \lfloor \log_2 c_{\max} \rfloor$. In addition, one bit is used to represent the sign bit. If the wavelet coefficient is positive, the sign bit is 0, otherwise it is 1. Suppose that n=10, therefore the binary representation of these wavelet coefficients at T_1 are $(\underline{\mathbf{1}}0000101010)_2$, $(\underline{\mathbf{1}}0000010010)_2$, $(\underline{\mathbf{0}}0000000010)_2$, $(\underline{\mathbf{0}}0000010101)_2$, and $(\underline{\mathbf{1}}0000000011)_2$. Assume that based on the proposed edge detector, pixel $P_1(x, y)$ in E_{AH} is determined as an edge pixel (i.e. its value is one). The status of T_1 at (x, y) becomes an edge tree and its value is stored in the LSB of coefficient $C_1(x, y)$. In this case the coefficient value -42 which equals $(10000101010)_2$ is replaced by -43 which equals $(1000010101\mathbf{1})_2$. Also, assume that k is set to two and the secret message bitstream to be embedded in tree T_1 is '**0**10111000111011…' (where the bold bit means the first secret message bit entering to the embedding algorithm). The first secret message bit '0' will be embedded into the second LSB of coefficient $C_1(x, y)$ after embedding the status. So, the new value of this coefficient -43= $(1000010101\mathbf{1})_2$ becomes -41= $(100001010\mathbf{0}1)_2$. Since this tree is an edge tree and k=2, the three (k+1) LSBs of coefficients $c_{11}(x, y)$, $c_{12}(x, y)$, $c_{13}(x, y)$, and $c_{14}(x, y)$ are replaced with the following secret message bits '101', '110', '001', and '110', respectively. The new values of these coefficients become -21=$(10000010\mathbf{101})_2$, 6=$(00000000\mathbf{110})_2$, 17=$(00000010\mathbf{001})_2$, and -6=$(10000000\mathbf{110})_2$. Similarly, the secret message is embedded into trees T2 and T3 based on the type of each tree. The entire embedding procedure in this example is shown in Fig. 3. The embedding algorithm can be summarized as follows:

Input: Cover image C of size $N \times M$ pixels and a secret message SE.

Output: Stego- image S.

Step 1: Read cover image C and Apply cover image adjustment to C as in [17].

Step 2: Read the secret message SE.

Step 3: Perform two levels WPD on the cover image *C*.

Step 4: Perform neutrosophic edge detector (NSED) on the subbands *AH*, *AV*, and *AD* to obtain the corresponding edge images E_{AH}, E_{AV}, and E_{AD}, respectively.

Step 5: Construct the three primary trees T_1, T_2, and T_3. Determine the type of each tree based on the edge images E_{AH}, E_{AV}, and E_{AD}.

Step 6: secret message bits are first embedded in T_1 as follows:

Step 6.1: Embed the type of T_1 (edge/non-edge) in the LSB of C_1.

Step 6.2: Start embedding the secret message bits, where the first secret message bit is embedded into the second LSB of coefficient C_1.

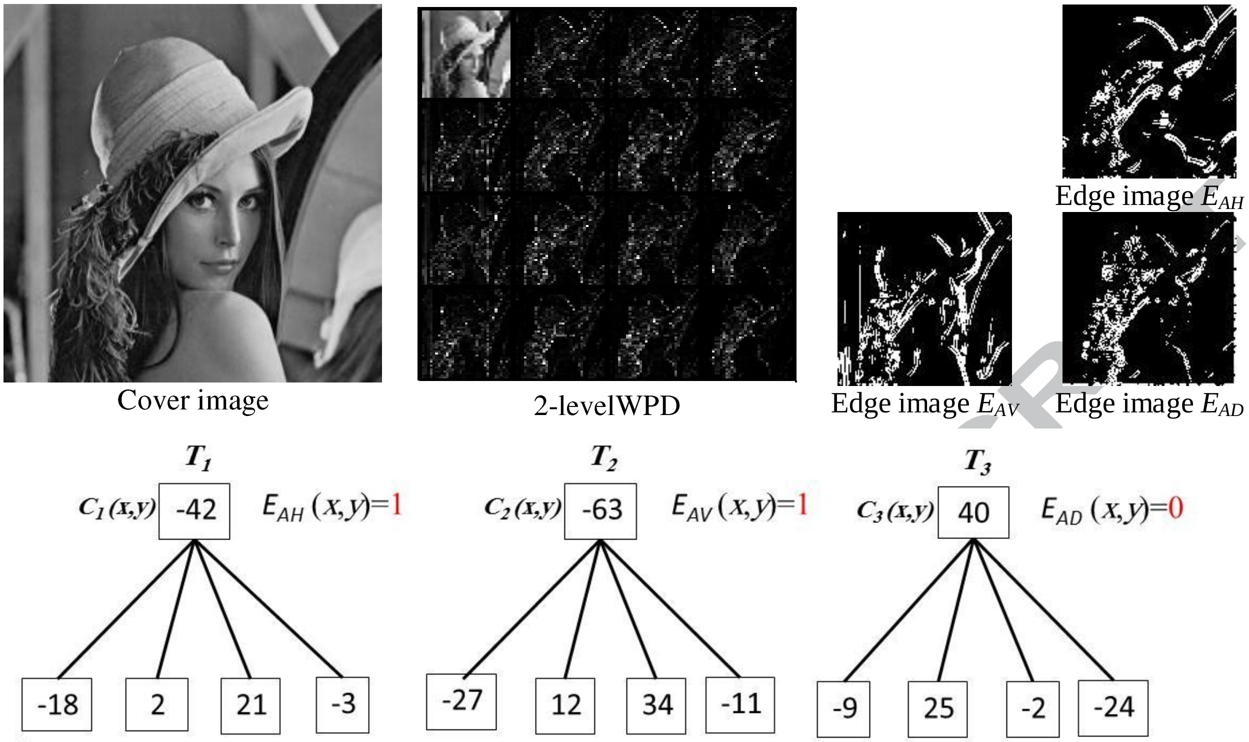
Step 6.3: If the type of T_1 is non-edge then embed *k* secret message bits into *k* LSBs of each coefficient c_{11}, c_{12}, c_{13}, and c_{14}, else embed *k*+1 secret message bits into each of these coefficients.

Step 7: Repeat Step 6 for T_2 and T_3.

Step 8: Perform inverse wavelet packet transform to obtain stego-image *S*.

3.2. Extracting procedure

In the extraction, the secret message bits embedded into each tree can be retrieved. Upon receiving a stego-image from a sender, the receiver receives the parameter *k* and uses the extraction algorithm to obtain the secret message as follows: First, a 2-level WPD is performed on the stego-image *S* and the wavelet packet trees are constructed to generate T_1, T_2, and T_3. Second, the status of the primary tree T_1 is extracted from the LSB of coefficients C_1 in subband AH. The secret message bits are retrieved by first extracting the first bit of this message from the second LSB of C_1. The following bits of the secret message are then extracted based on the type of the primary tree. If the status of T_1 is non-edge, then *k* LSBs are extracted from each coefficient c_{11}, c_{12}, c_{13}, and c_{14} in subbands HA, HH, HV, and HD, respectively. Otherwise *k*+1 LSBs are extracted from these coefficients. Finally, the secret message bits are recovered from the primary trees T_2 and T_3 in the same way. The extracted bits are concatenated to obtain the embedded secret message bits *SE*.



k=2

Secret message bitstream is '0101110001110110010111001011100110 0011...'

For T_1:

$C_1(x,y) = -42 = (\underline{1}0000101010)_2 \rightarrow (1000010100\mathbf{1})_2 = -41$

$c_{11}(x,y) = -18 = (\underline{1}0000010010)_2 \rightarrow (10000010\mathbf{101})_2 = -21$

$c_{12}(x,y) = 2 = (\underline{0}0000000010)_2 \rightarrow (00000000\mathbf{110})_2 = 6$

$c_{13}(x,y) = 21 = (\underline{0}0000010101)_2 \rightarrow (00000010\mathbf{001})_2 = 17$

$c_{14}(x,y) = -3 = (\underline{1}0000000011)_2 \rightarrow (10000000\mathbf{110})_2 = -6$

For T_3:

$C_3(x,y) = 40 = (\underline{0}0000101000)_2 \rightarrow (0000010101\mathbf{0})_2 = 42$

$c_{31}(x,y) = -9 = (\underline{1}0000001001)_2 \rightarrow (100000010\mathbf{11})_2 = -11$

$c_{32}(x,y) = 25 = (\underline{0}0000011001)_2 \rightarrow (000000110\mathbf{00})_2 = 24$

$c_{33}(x,y) = -2 = (\underline{1}0000000010)_2 \rightarrow (000001000\mathbf{11})_2 = 3$

$c_{34}(x,y) = -24 = (\underline{1}0000011000)_2 \rightarrow (100000110\mathbf{00})_2 = -24$

For T_2:

$C_2(x,y) = -63 = (\underline{1}0000111111)_2 \rightarrow (1000011111\mathbf{1})_2 = -63$

$c_{21}(x,y) = -27 = (\underline{1}0000011011)_2 \rightarrow (10000011\mathbf{100})_2 = -28$

$c_{22}(x,y) = 12 = (\underline{0}0000001100)_2 \rightarrow (00000001\mathbf{101})_2 = 13$

$c_{23}(x,y) = 34 = (\underline{0}0000100010)_2 \rightarrow (00000100\mathbf{110})_2 = 38$

$c_{24}(x,y) = -11 = (\underline{1}0000001011)_2 \rightarrow (10000001\mathbf{010})_2 = -10$

Fig. 3. An example of the proposed embedding algorithm.

4. Experimental Results

Several experiments were performed to evaluate the efficiency of the proposed data hiding algorithm in terms of data hiding payload and fidelity benchmarks. In these experiments, 256-grayscale images of 128×128 and 512×512 pixel resolutions were used. The secret message was generated randomly. The fidelity (invisibility) of a secret message using a steganography method is measured by various similarity metrics such as Mean Squared Error (MSE) and Peak Signal to Noise Ratio (PSNR). In this paper, the quality of stego-image is evaluated subjectively by the human visual system (HVS). Moreover, the objective quality of the stego-image is measured in term of the PSNR, defined as:

$$PSNR = 10\log_{10}\frac{255^2}{MSE}, \qquad (21)$$

where MSE is the mean squared error of the stego-image $S(i,j)$ with respect to the cover image $C(i,j)$. For an $N\times M$ size image, MSE is defined as:

$$MSE = \frac{1}{N\times M}\sum_{i=1}^{N}\sum_{j=1}^{M}(C(i,j)-S(i,j))^2. \qquad (22)$$

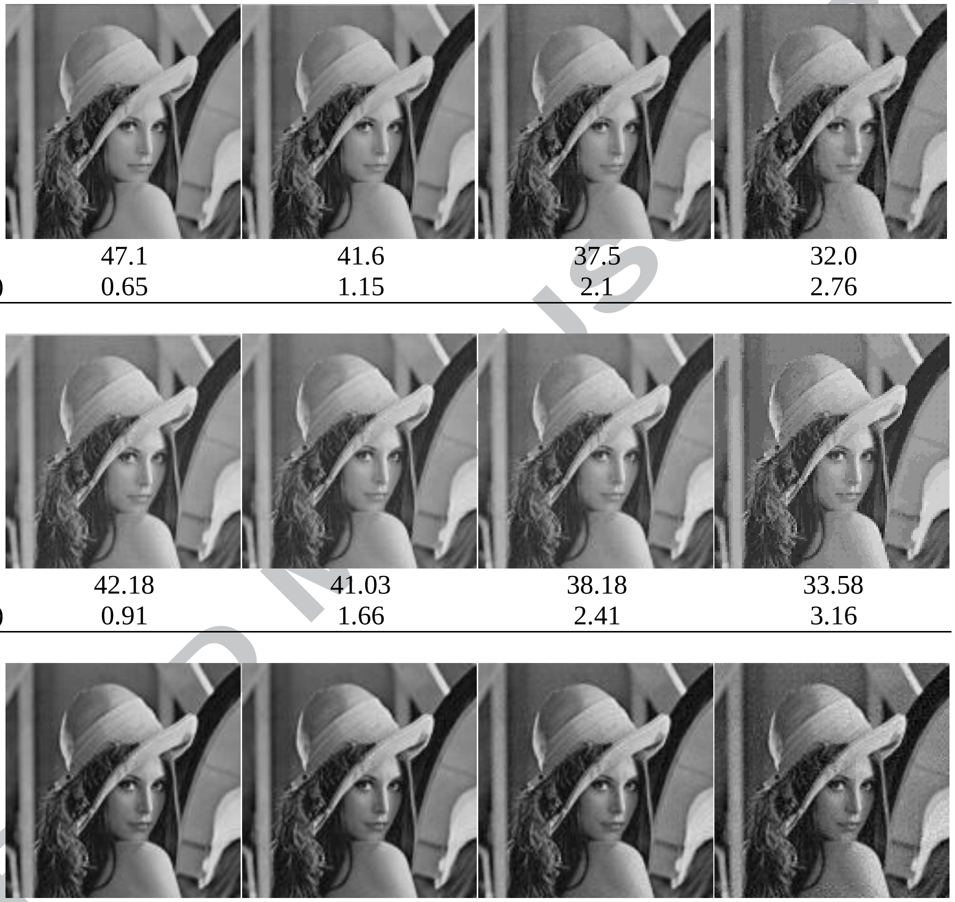
Another evaluation criterion of a steganography method is the capacity (data payload) that can be defined as the number of secret bits that can be hidden in the cover image pixels. It is given as:

$$payload\,(bpp) = \frac{Embedded\ \ bits}{N\times M}. \qquad (23)$$

The embedding capacity depends on the steganography method and the texture of the cover image. It is given either in absolute measurement such as bits per pixel (bpp) or in relative percentage.

4.1 Embedding capacity and perceptual quality analysis

The performance of the proposed data hiding algorithm was compared with the well-known spatial-based and wavelet-based approaches of data hiding. The spatial-based methods include Chen et al [11] and Tseng et al [12] methods, both utilize edge detectors. They also include Wu and Tsai's [9] and Wu et al [10] methods, both perform pixel-value differencing (PVD) to discriminate between edge and smooth pixels. Figs. 4-9 show the visual quality of the stego-images generated by the proposed scheme, Chen [11] and Tseng [12] methods. These figures also compare the data hiding capacity (payload) and the corresponding PSNR of the proposed method with the methods of Chen and Tseng. For these methods, *k* LSBs of each non-edge pixel are replaced by the secret image while *k*+1, *k*+2, and a proper number of edge LSBs that is greater than *k* and achieve minimal distortion for each 4×4 block used for the proposed, Chen and Tseng methods, respectively. In these figures, the results of Lena image are only provided for method of Chen [11] because it has no results for other images. As can be seen from these figures that the quality of the stego-images generated by the proposed method (especially at *k*<=3) are higher than those generated by the methods of Chen and Tseng. Moreover, the unintended observers will not be able to perceive the existence of the hidden message in the stego-images. It is also observed that the proposed scheme achieves higher PSNR value with preserving higher embedding payloads compared to the other methods.



		k=1	*k*=2	*k*=3	*k*=4
Chen et al' scheme [11]	PSNR (dB)	47.1	41.6	37.5	32.0
	Payload (bpp)	0.65	1.15	2.1	2.76
Tseng et al' scheme [12]	PSNR (dB)	42.18	41.03	38.18	33.58
	Payload (bpp)	0.91	1.66	2.41	3.16
Proposed	PSNR (dB)	**47.9923**	**43.9953**	**37.8979**	31.2724
	Payload (bpp)	**1.1077**	**1.8577**	**2.6077**	**3.3577**

Fig. 4. Performance comparison of the proposed, Chen and Tseng algorithms based on edge detectors on 128×128 Lena cover image.

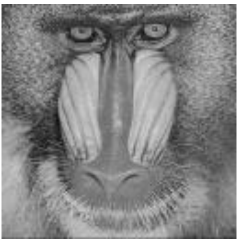
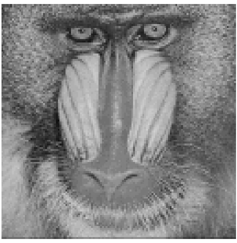
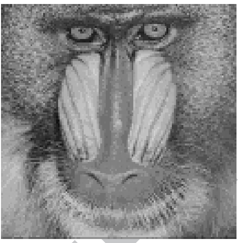
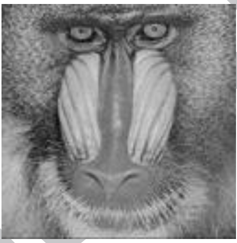
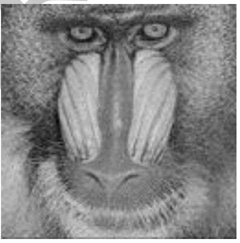
		k=1	*k*=2	*k*=3	*k*=4
Tseng et al' scheme [12]					
	PSNR (dB)	41.47	40.22	37.04	32.47
	Payload (bpp)	1.06	1.80	2.56	3.32
Proposed					
	PSNR (dB)	**48.2059**	**44.4381**	**39.073**	**32.4385**
	Payload (bpp)	**1.0938**	**1.8438**	**2.593**	**3.3438**

Fig. 5. Performance comparison of the proposed and Tseng algorithms based on edge detectors on 128×128 Baboon cover image.

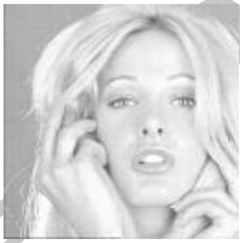
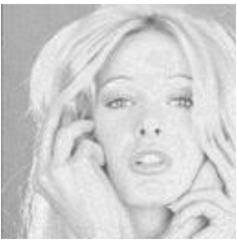
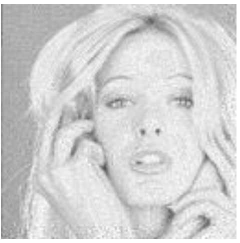
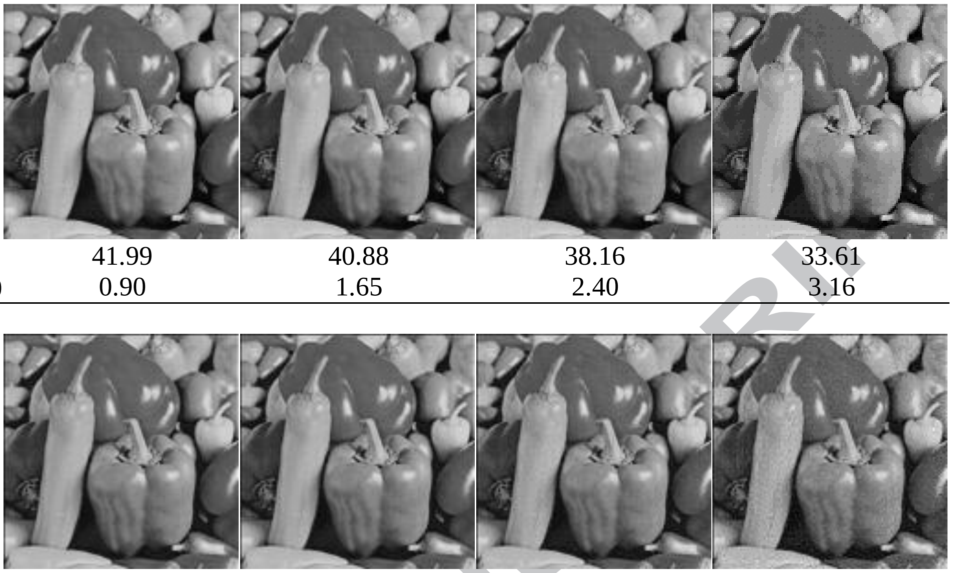
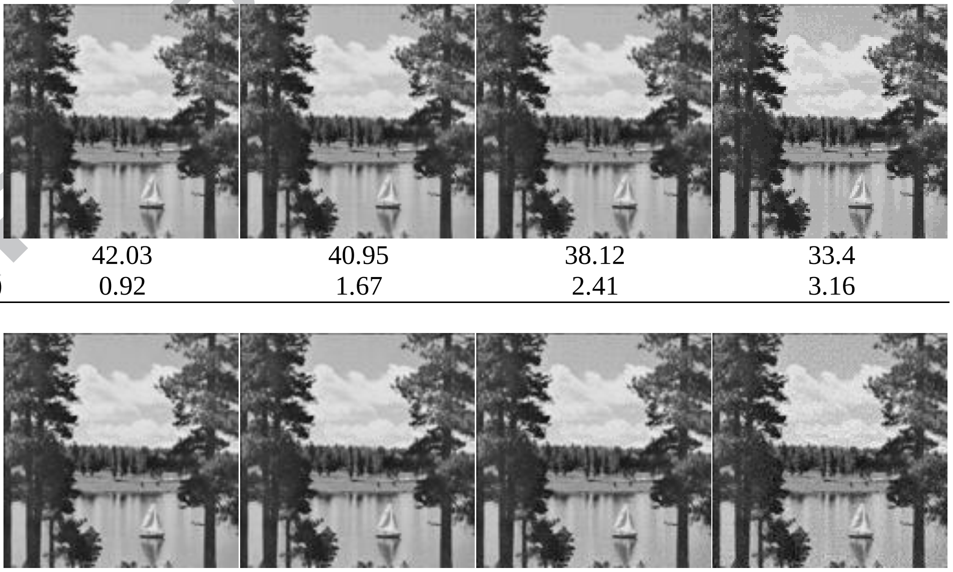
		k=1	*k*=2	*k*=3	*k*=4
Tseng et al' scheme [12]					
	PSNR (dB)	41.94	40.75	37.84	32.77
	Payload (bpp)	0.93	1.68	2.43	3.18
Proposed					
	PSNR (dB)	**48.1412**	**44.1685**	**37.8818**	31.2576
	Payload (bpp)	**1.0957**	**1.8457**	**2.5957**	**3.3457**

Fig. 6. Performance comparison of the proposed and Tseng algorithms based on edge detectors on 128×128 Tiffany cover image.



		k=1	*k*=2	*k*=3	*k*=4
Tseng et al' scheme [12]	PSNR (dB)	41.99	40.88	38.16	33.61
	Payload (bpp)	0.90	1.65	2.40	3.16
Proposed	PSNR (dB)	**48.2975**	**44.4831**	**38.4235**	31.7221
	Payload (bpp)	**1.0725**	**1.8225**	**2.5725**	**3.3225**

Fig. 7. Performance comparison of the proposed and Tseng algorithms based on edge detectors on 128×128 Peppers cover image.



		k=1	*k*=2	*k*=3	*k*=4
Tseng et al' scheme [12]	PSNR (dB)	42.03	40.95	38.12	33.4
	Payload (bpp)	0.92	1.67	2.41	3.16
Proposed	PSNR (dB)	**48.1340**	**44.3644**	**38.5412**	31.9394
	Payload (bpp)	**1.1008**	**1.8508**	**2.6008**	**3.3508**

Fig. 8. Performance comparison of the proposed and Tseng algorithms based on edge detectors on 128×128 Lake cover image.

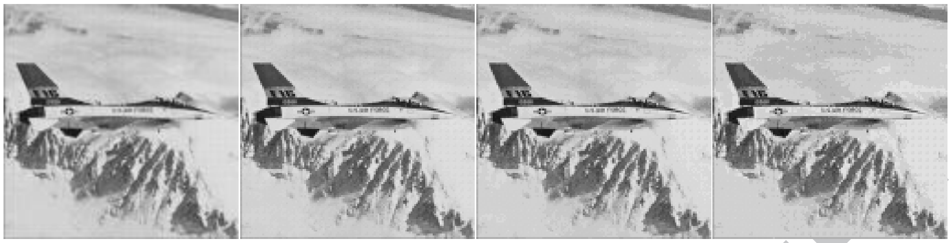
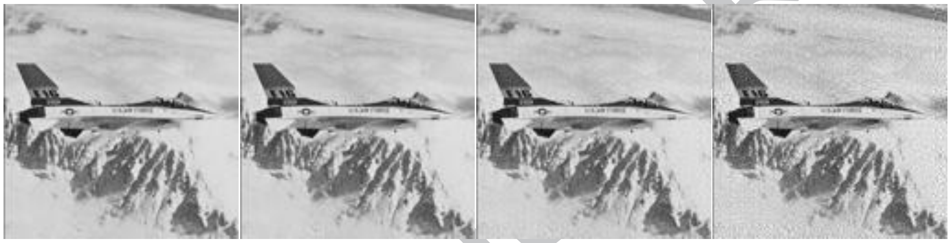
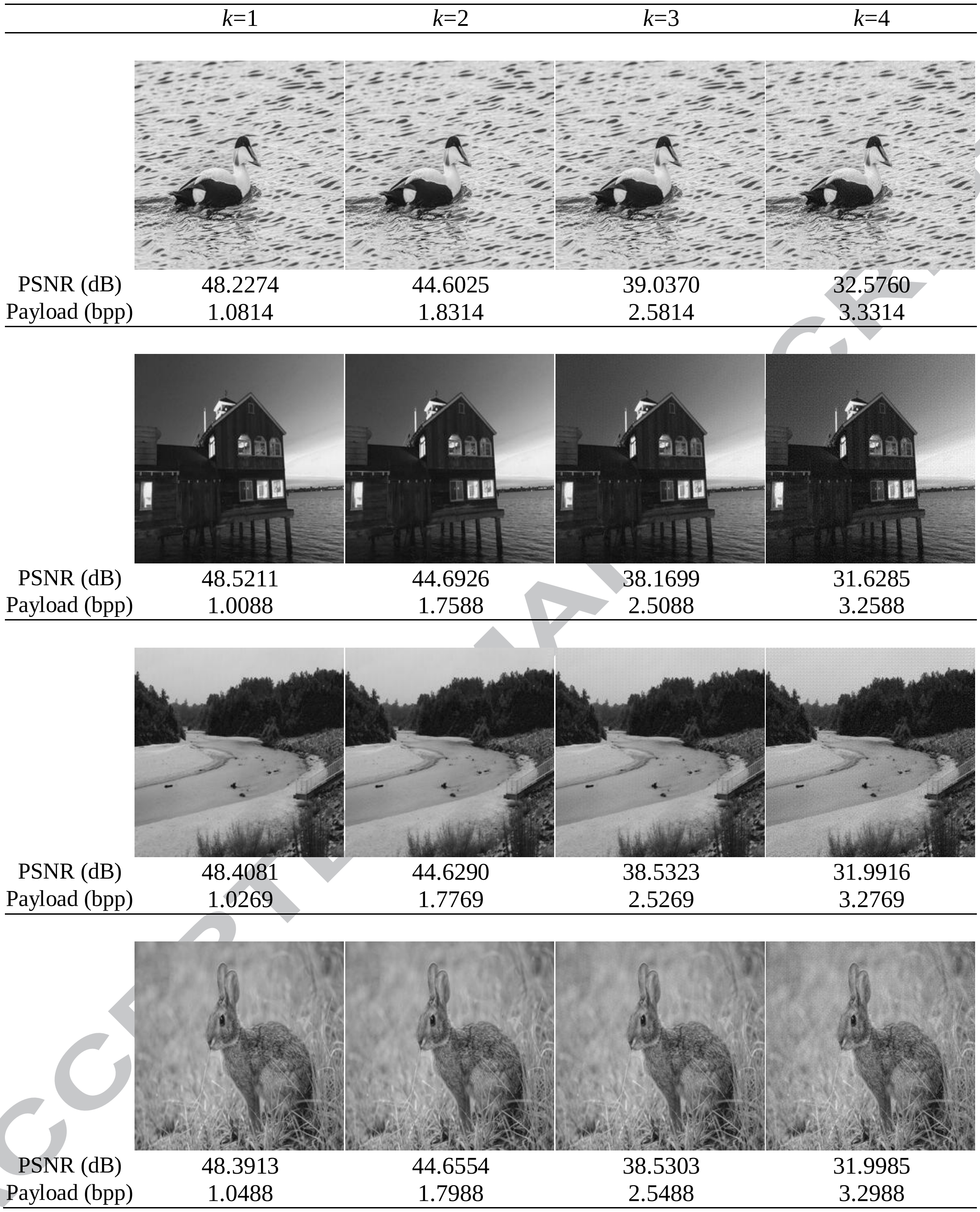
		k=1	*k*=2	*k*=3	*k*=4
Tseng et al' scheme [12]					
	PSNR (dB)	42.10	41.02	38.16	33.60
	Payload (bpp)	0.90	1.65	2.40	3.15
Proposed					
	PSNR (dB)	**48.1884**	**44.1542**	**37.9409**	31.4595
	Payload (bpp)	**1.0803**	**1.8303**	**2.5803**	**3.3303**

Fig. 9. Performance comparison of the proposed and Tseng algorithms based on edge detectors on 128×128 Jet cover image.

The performance of the proposed algorithm was also tested using some natural images downloaded from the available Photo Galleries https://photogallery.sc.egov.usda.gov/res/sites/photogallery/ and https://www.flickr.com/photos/. The selected images were resampled to 256×256 pixel resolutions and converted into grayscale. Fig. 10 shows the visual quality, PSNR of the stego-images and the payload obtained by the proposed method using various *k* values.

Furthermore, the message capacity (in bytes) and PSNR of the proposed, Wu and Tsai [9] and Wu et al [10] methods are tabulated in Table 1. The results in this table were obtained when the proposed method was implemented at *k*=3. Two LSBs in the smoothed areas of PVD methods of [9] and [10] were used. The proposed algorithm achieves PSNR gain of about 0.6-5.73 dB and about 0.39- 5.83 dB over the Wu [9] and Wu et al [10] methods, respectively for most cover images. However, for Lena image, using lower value of *k* (*k*=2) as shown in Table 3, the proposed algorithm achieves PSNR gain over the other methods [9] and [10] while providing higher embedding capacity. Moreover, for the cover images Couple and Airplane, the proposed method at the same embedding capacity of Wu et al's method [10] (i.e., the embedding process in the proposed method is stopped when its embedding capacity is reached to that obtained from [10]), the PSNR values of the proposed method for both images are 39.73 and 39.66 dB, respectively.



	k=1	*k*=2	*k*=3	*k*=4
PSNR (dB)	48.2274	44.6025	39.0370	32.5760
Payload (bpp)	1.0814	1.8314	2.5814	3.3314
PSNR (dB)	48.5211	44.6926	38.1699	31.6285
Payload (bpp)	1.0088	1.7588	2.5088	3.2588
PSNR (dB)	48.4081	44.6290	38.5323	31.9916
Payload (bpp)	1.0269	1.7769	2.5269	3.2769
PSNR (dB)	48.3913	44.6554	38.5303	31.9985
Payload (bpp)	1.0488	1.7988	2.5488	3.2988

Fig. 10. Results of the proposed algorithm using various *k* values for four natural images.

Table 1 also shows the percentage increase of the hidden message capacity (Δ) of the proposed algorithm over the other algorithms which is given by:

$$\Delta = \frac{HC_{Pro} - HC_{Oth}}{HC_{Oth}} \times 100\ \% , \qquad (24)$$

where HC_{Pro} and HC_{Oth} are the hidden message capacity obtained by using the proposed algorithm and other algorithms, respectively. It is clear from Table 1 that the proposed method provides approximately 60% and 25% on average higher hiding capacity than Wu and Tsai [9] and Wu et al [10] methods, respectively, at the same time achieving higher PSNR values for most cover images. Moreover, performance comparison of the proposed method to the state of the art method, parity-bit pixel value difference (PBPVD) [4], that is based on PVD was presented in Table 2. It is clear that the proposed method provides more data hiding capacity and better PSNR values especially with the images containing complex contents. Moreover, as shown in Table 2 when the proposed method was tested using the same embedding capacity obtained from PBPVD [4] method, it achieves an averaged PSNR gain of approximately 1.1 dB over the PBPVD method.

The proposed method was further compared with some existing wavelet-based approaches of data hiding algorithms, include the baseline [18] and Seyyedi [17] methods, both are based on IWT. Table 3 summarizes the results of the mentioned methods. It can be seen that the proposed method significantly outperforms the other existing wavelet based methods. It increases the data hiding capacity and also improves the stego-image quality.

Table 1: Performance comparison of the proposed algorithm and the algorithms based on pixel-value differencing (PVD).

Cover images (512×512)	Wu and Tsai's method [9]		Wu et al's method [10]		Proposed k=3		Gain over Wu-Tsai [9]		Gain over Wu et al [10]	
	Capacity (bytes)	PSNR (dB)	Capacity (bytes)	PSNR (dB)	Capacity (bytes)	PSNR (dB)	Δ (%)	ΔPSNR (dB)	Δ (%)	ΔPSNR (dB)
Lena	51219	38.94	66064	38.80	**82960**	38.7735	61.97	-0.17	25.58	-0.03
Baboon	57146	33.43	68007	33.33	**84902**	**39.1598**	48.57	5.73	24.84	5.83
Peppers	50907	37.07	66032	37.50	**82615**	**39.0963**	62.29	2.03	25.11	1.60
Jet	51224	37.42	66256	37.63	**83709**	**38.0219**	63.42	0.60	26.34	0.39
Boat	52635	34.89	66622	35.01	**84058**	**38.3187**	59.69	3.43	26.17	3.31
Couple	51604	38.81	66167	39.07	**83831**	38.8176	62.45	0.007	26.69	-0.25
Airplane	49739	40.13	65756	40.18	**81714**	38.6548	64.41	-1.47	24.27	-1.52

Table 2: Performance comparison of the proposed algorithm and PBPVD [4] algorithm based on PVD.

Cover images (512×512)	PBPVD [4]		Proposed k=3		Proposed k=3	
	Capacity	PSNR	Capacity	PSNR	Capacity	PSNR

	(bytes)	(dB)	(bytes)	(dB)	(bytes)	(dB)
Lena	70403	39.09	70403	39.5322	82960	38.7735
Baboon	78973	35.06	78973	39.5244	84902	39.1598
Peppers	70322	39.30	70322	39.8716	82615	39.0963
Jet	69241	38.95	69241	38.9495	83709	38.0219
Boat	73130	37.49	73130	38.8939	84058	38.3187
Lake	73422	37.59	73422	39.3047	84619	38.6834
Elaine	72075	39.14	72075	40.1993	82539	39.4403
Couple	72214	37.75	72214	39.4285	83831	38.8176
Truck	69352	40.56	69352	39.1736	84635	38.4235

Table 3: Performance comparison of the proposed algorithm and the algorithms based on IWT.

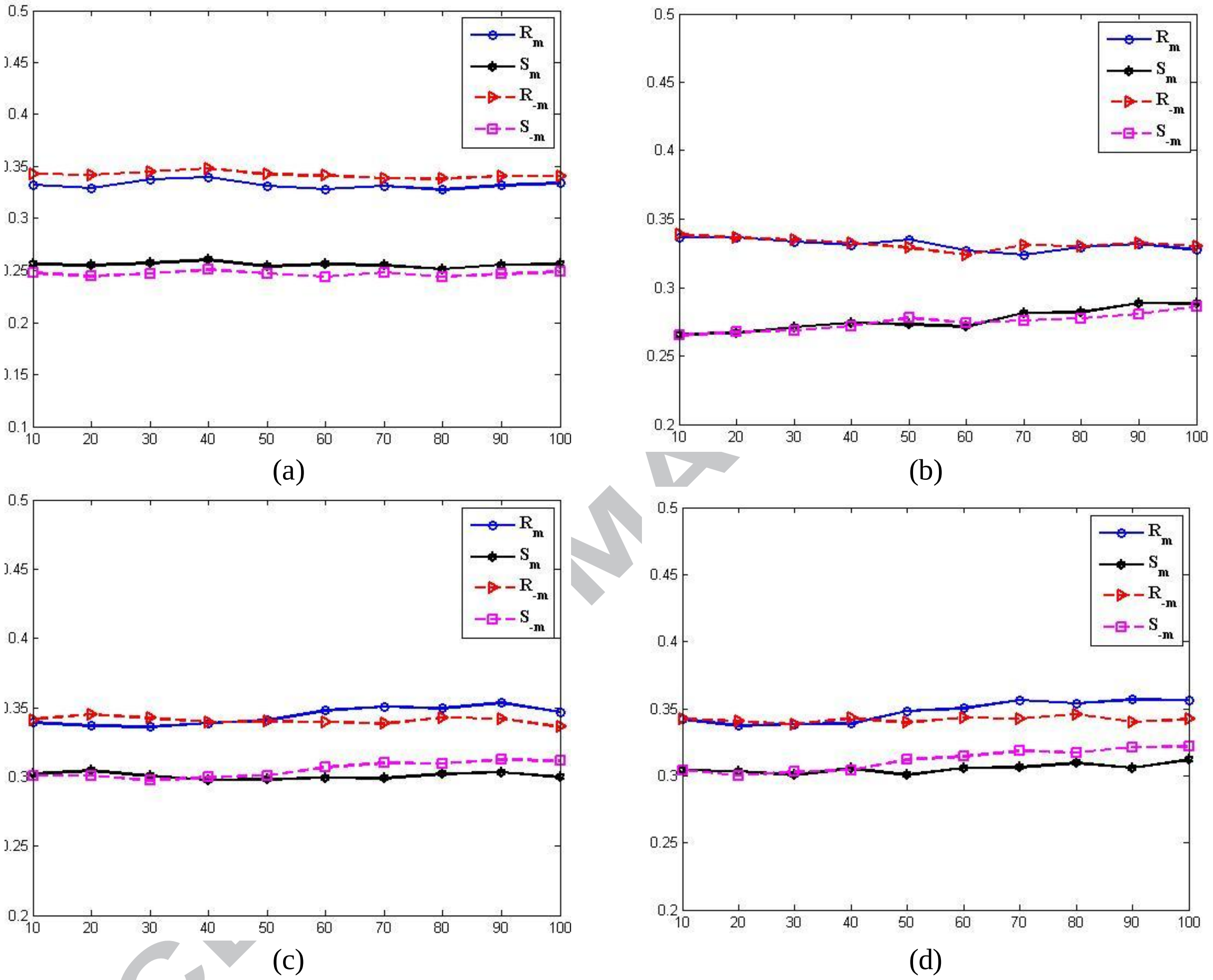
Cover images (512×512)	Baseline method using IWT [18]		Seyyedi's method based on IWT [17]		Proposed *k*=2		Proposed *k*=3	
	Capacity (bytes)	PSNR (dB)	Capacity (bytes)	PSNR (dB)	Capacity (bytes)	PSNR (dB)	Capacity (bytes)	PSNR (dB)
Lena	10688	36.64	50000	40.54	**58384**	**44.9149**	82960	38.7735
Baboon	1865	32.76	50000	38.07	**60326**	**44.5983**	84902	39.1598
Peppers	8661	29.11	50000	40.64	**58040**	**45.0397**	82615	39.0963
Jet	11748	36.30	40000	40.18	**59133**	**44.4391**	83709	38.0219
Couple	10610	29.83	N/A	N/A	**59255**	**44.7313**	83831	38.8176
Boat	N/A	N/A	50000	39.40	**59482**	**44.5880**	84058	38.3187

4.2 Security against statistical RS-steganalysis

The RS-steganalysis method was proposed in [25] to exploit the correlation of images in the spatial domain. In RS Analysis, all the pixels of a cover image are partitioned into three groups: the regular group R_m or R_{-m}, the singular group S_m or S_{-m}, and the unusable group. This steganalysis is based on discrimination function (DF) with two flipping masks, m and $–m$, where m = [0110] and $-m$ = [0 − 1 – 1 0]. The parameters R_m, R_{-m}, S_m and S_{-m} are used to find the magnitude of pixel block using DF function. The RS statistical analysis will not detect the hidden message in the cover image when $R_m \cong R_{-m} > S_m \cong S_{-m}$. Otherwise, the cover image has hidden message, where in this case R_{-m} and S_m increases, whereas R_m and S_{-m} decreases and the image becomes insecure by RS analysis.

The security of the proposed method against the statistical RS steganalysis method [25] is shown in Fig. 11. In this figure, the x-axis represents the percentage of data hiding capacity in the stego-image and the y-axis indicates the percentage of the regular and singular pixel groups with masks m and $-m$. From the RS-diagram shown in Fig. 11 the singular and regular parameters of the stego-images are close to each other between the curves R_m and R_{-m}, and between S_m and S_{-m} even when increasing the embedding capacity. This proves that the proposed method is secure against statistical RS-analysis.

The differences of RS detection results between R_m and R_{-m}, and between S_m and S_{-m} for the Chen et al. and the proposed methods at k equals 2 and 3 and with 100% embedding capacity are illustrated in Table 4. The results in this table indicate that the proposed method retains slightly smaller average differences in regular groups (1.166%) and singular groups (1.256%) for all images (at *k*=2) as compared to Tseng et al' method [12]. That means fewer artifacts can be detected which demonstrates the ability of the proposed method to resist against RS-steganalysis.



(a)

(b)

(c)

(d)

Fig. 11. RS-analysis graphs by the proposed method of stego-images. (a) Lena *k*=2; (b) Lena *k*=4; (c) Baboon *k*=2; (d) Baboon *k*=4.

Table 4: Differences of RS-steganalysis detection between the singular and regular parameters for stego-images.

Images (128×128)	*k*=2				*k*=3			
	Tseng et al' scheme [12]		Proposed		Tseng et al' scheme [12]		Proposed	
	$\mid R_m - R_{-m} \mid$	$\mid S_m - S_{-m} \mid$	$\mid R_m - R_{-m} \mid$	$\mid S_m - S_{-m} \mid$	$\mid R_m - R_{-m} \mid$	$\mid S_m - S_{-m} \mid$	$\mid R_m - R_{-m} \mid$	$\mid S_m - S_{-m} \mid$
Lena	0.0092	0.0098	0.0071	0.0073	0.0168	0.0104	0.0079	0.0071
Baboon	0.0199	0.0119	0.011	0.0119	0.0086	0.0174	0.0186	0.0202
Peppers	0.0074	0.0162	0.014	0.0174	0.0134	0.0159	0.0125	0.0125
Jet	0.0223	0.0174	0.0042	0.008	0.0186	0.0083	0.0109	0.0129

tiff	0.0235	0.0165	0.0101	0.004	0.0235	0.0165	0.0028	0.0073
Lake	0.0174	0.0095	0.0236	0.0268	0.0061	0.0018	0.014	0.0082
Average	0.016617	0.01355	**0.011667**	**0.012567**	0.0145	0.011717	**0.011117**	**0.011367**

4.3 Security under pixel difference histogram analysis

A pixel difference histogram is one of the steganalysis methods to expose the secret message in stego-images. It is calculated by taking the differences of neighboring pixels between cover and stego-image. Fig. 12 shows the pixel difference histograms of the cover images (Lena and Baboon) and their corresponding stego-images using the proposed method with the maximum embedding capacity. It is observed that the pixel difference histogram of the stego-image produced by the proposed method followed the curve of cover image pixel difference histogram.

The absolute difference value between the difference histograms for the respective cover and stego images (*δh*) is used to measure the similarity between the two difference histograms. A smaller *δh* means that the absolute difference between the difference histograms is small and thereby the embedding secrete message is hardly detected. Table 5 shows the results of *δh* obtained using the PBPVD [4], Khodaei et al. [22] and proposed methods. The average value of *δh* of the proposed method (3297.625) is lowest compared to Khodaei et al. [22] (7102.125) and the PBPVD [4] (3452.5) methods. That implies that the proposed method reduces the detectable artifacts under pixel difference histogram steganalysis detection attacks.

Table 5: Comparing the values of the absolute difference between the difference histograms (*δh*) of different methods.

Images (512×512)	Khodaei et al. [22]	PBPVD [4]	Proposed k=3
Lena	9000	4652	3155
Baboon	2387	1390	574
Peppers	5501	1401	6864
Jet	14914	9083	4364
Boat	3147	568	432
Lake	4095	848	3095
Couple	6915	3677	1684
Truck	10858	6001	6213
Average	7102.125	3452.5	**3297.625**

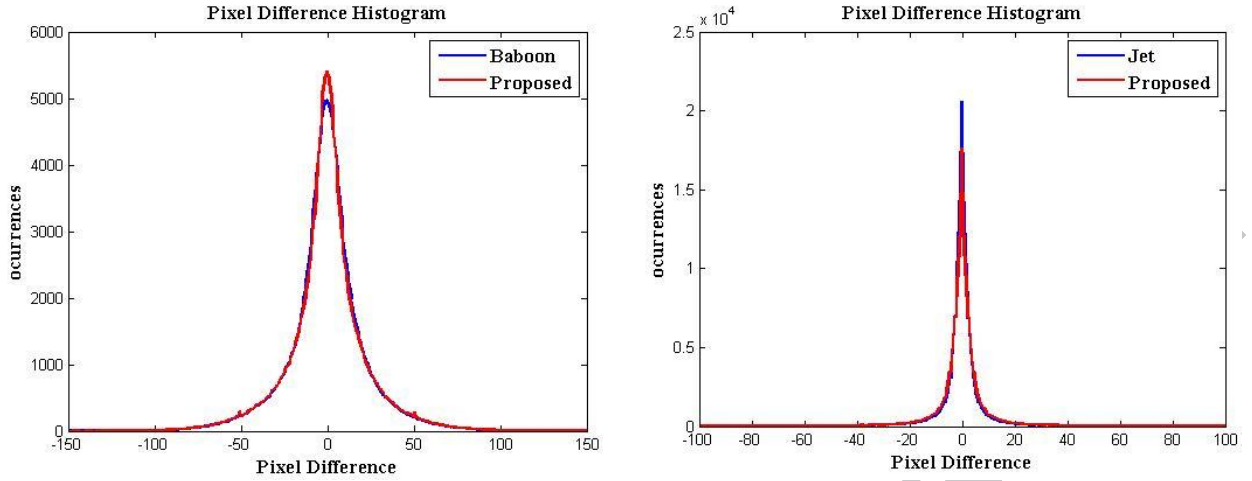


Fig. 12. Pixel difference histogram analysis of the cover and theirs corresponding stego-images of the proposed method.

4.4 Security against universal steganalysis

Universal steganalysis is also known as blind steganalysis which is the modern approach to attack the stego images without any prior knowledge about the type of the used steganographic algorithm. These blind detectors are built using machine learning, such as using a classifier trained on the extracted features from the cover and stego images to identify the differences between the cover and stego features. There are many steganalysis features that are suitable for detection of spatial and JPEG steganography. Among spatial domain feature sets, the second-order subtractive pixel adjacency matrix (SPAM) [34] and the spatial rich model (SRM) [35] were proposed. In [36], a feature set named discrete cosine transform residual (DCTR) was proposed for steganalysis of JPEG images. These extracted features were based on undecimated DCT coefficients and trained as binary classifiers implemented using the FLD ensemble [37].

In this section, several experiments were carried out on BOSSbase 1.01 [38] to evaluate the performance of the proposed method. The database contains 10,000 grayscale 512×512 images. 1000 images were selected randomly from this database. Table 6 illustrates the average PSNR and payload obtained by the proposed method using various *k* values. Moreover, the security of the proposed steganographic algorithm against the universal analysis was tested and compared to JPEG steganographic algorithms which are nsF5 [39] and the state-of-the-art JPEG domain UNIWARD [40], referred to as J-UNIWARD. These steganographic methods were selected for the purpose of comparison as these methods and the proposed method perform data hiding in the transform domain. Steganalysis was implemented using DCTR feature set with T = 4 and dimensionality of 8000 features as recommended in [36] and the linear classifier called LSMR (Least Squared Minimum-Residual) [41]. Experiments were carried out on the selected images with JPEG quality factor 75. The codes for the selected steganographic methods, feature extractor and classifier) are available for download from http://dde.binghamton.edu/download/. The proposed method was tested at payloads ranging from 0.2 to 1.0 bits per pixel (bpp) which were obtained at k=1, while JPEG-domain methods were tested on the same payloads expressed in bits per non-zero AC DCT coefficient (bpnzAC).

In this paper, the detection accuracy is measured using the minimal total error probability under equal priors (equal a priori probabilities of a cover or stego image) and it is given by [37]:

$$P_E = \min_{P_{FA}} \frac{1}{2}(P_{FA} + P_{MD}), \qquad (25)$$

where P_{FA} and P_{MD} are the false alarm and missed detection probabilities, respectively. The detection accuracy is obtained on the test set averaged over ten 50/50 splits of the database (i.e., a 50/50 split for training and testing was used).

Table 7 shows the detection error for the proposed, J-UNIWARD and nsF5 steganographic methods. It is clear from this table that the J-UNIWARD is more undetectable than the proposed and nsF5 methods for payloads ≤ 0.6. For larger payloads, the proposed method is more secure than the other methods by more than 5% in terms of the detection error. This is because the proposed method is designed to embed larger payloads.

Table 6: The average PSNR and payload for the proposed algorithm applied on 1000 images at various k values.

	k=1	k=2	k=3
Average PSNR (dB)	48.3294	44.2818	38.0542
Average Payload (bpp)	1.0467	1.7967	2.5467

Table 7: Detection error P_E for the proposed, nsF5 and J-UNIWARD steganographic methods.

Steganography Method	Payload				
	0.2	0.4	0.6	0.8	1.0
nsF5	0.2283	0.0117	0.0033	0.0000	0.0000
J-UNIWARD	**0.4250**	**0.3450**	**0.2333**	0.1233	0.0683
Proposed	0.2667	0.2600	0.2117	**0.1750**	**0.1400**

5. CONCLUSION

In this paper a data hiding algorithm based on wavelet packet decomposition and neutrosophic set was proposed. In the algorithm, WPD is performed on the cover image and parent-children relationships of wavelet packet coefficients across the subbands are taken into consideration to construct the WPTs. The presented neutrosophic set-based edge detector (NSED) assists the proposed data hiding algorithm in determining the type of each WPT as edge/non-edge tree. This leads to embed more secret bits into the coefficients in the edge tree than those in the non-edge tree and then to generate a better quality stego-image. Experimental results have shown that the proposed scheme gives better embedding payload, subjective and objective quality of stego-images than the other well-known spatial-based and wavelet-based embedding methods. Furthermore, the proposed method resists the RS detection attack, the pixel difference histogram analysis and universal steganalysis.

REFERENCES

[1] C.K. Chan, L.M. Cheng, Hiding data in images by simple LSB substitution, Pattern Recognition 37(3) (2004) 469-474.

[2] S. Chutani, H. Goyal, LSB embedding in spatial domain- a review of improved techniques, Int. J. Comput. Appl. 3 (1) (2012) 153-157.

[3] J. Fridrich, M. Goljan, R. Du, Detecting LSB steganography in color and gray-scale images, IEEE Multimedia 8(4) (2001) 22-28.

[4] M. Hussain, A.W.A. Wahab, A.T.S. Ho, N. Javed, K-H. Jung, A data hiding scheme using parity-bit pixel value differencing and improved rightmost digit replacement, Signal Processing: Image Communication 50 (2017) 44–57.

[5] H.-W. Tseng, H.-S. Leng, A steganographic method based on pixel-value differencing and the perfect square number, Journal of Applied Mathematics (2013) 1-8.

[6] C.M. Wang, N.I. Wu, C.S. Tsai, M.S. Hwang, A high quality steganographic method with pixel-value differencing and modulus function, The Journal of Systems and Software 81 (1) (2008) 150-158.

[7] Y.K. Lee, L.H. Cheng, High capacity image steganographic model, IEE Vision, Image and Signal Processing 147(3) (2000) 288-294.

[8] X. Zhang, S. Wang, Steganography using multiple-base notational system and human vision sensitivity, IEEE Signal Process. Lett. 12(1) (2005) 67-70.

[9] D.C. Wu, W.H. Tsai, A steganographic method for images by pixel-value differencing, Pattern Recognition Letters 24(9) (2003) 1613-1626.

[10] H.-C. Wu, N.-I. Wu, C.-S. Tsai, M.-S. Hwang, Image steganographic scheme based on pixel-value differencing and LSB replacement methods, IEE Vision, Image and Signal Processing 152(5) (2005) 611-615.

[11] W.J. Chen, C. C. Chang, T. Le, High payload steganography mechanism using hybrid edge detector, Expert Systems with Applications 37(4) (2010) 3292-3301.

[12] H-W. Tseng, H-S. Leng, A high-payload block-based data hiding scheme using hybrid edge detector with minimal distortion, IET Image Processing 8(11) (2014) 647-654.

[13] R. Chu, X. You, X. Kong, X. Ba, A DCT-based image steganographic method resisting statistical attacks, Proc. Int. conf. Acoustics, Speech, and Signal Processing (2004) V-953-6.

[14] B.L. Lai, L.W. Chang, Adaptive data hiding for images based on Haar discrete wavelet transform, Advances in Image and Video Technology (2006) 1085-1093.

[15] R. El Safy, H.H. Zayed, A. El Dessouki, An adaptive steganographic technique based on integer wavelet transform, Int. Conf. Networking and Media Convergence (2009) 111-117.

[16] S. Bhattacharyya, G. Sanyal, Data hiding in images in discrete wavelet domain using PMM, Int. Journal of Electrical and Computer Engineering 5(6) (2010) 597-606.

[17] S.A. Seyyedi, N. Ivanov, High payload and secure steganography method based on block partitioning and integer wavelet transform, Int. Journal of Security and Its Applications 8(4) (2014)183-194.

[18] G. Xuan, J. Zhu, Y.Q. Shi, Z. Ni, W. Su, Distortionless data hiding based on integer wavelet transform, IEE Electronic Letters 38(25) (2002) 1646-1648.

[19] A. Cheddad, J. Condell, K. Curran, P. Mc Kevitt, Digital image steganography: survey and analysis of current methods, Signal Process. 90 (2010) 727–752.

[20] M. Hussain, A.W.A. Wahab, N. Javed, K-H. Jung, Hybrid data hiding scheme using right-most digit replacement and adaptive least significant bit for digital images, Symmetry 8(6) (2016) 1-21.

[21] X. Liao, Q-Y. Wen, J. Zhang, A steganographic method for digital images with four-pixel differencing and modified LSB substitution, journal of Visual Communication and Image Representation 22(1) (2011) 1-8.

[22] M. Khodaei, K. Faez, New adaptive steganographic method using least-significant bit substitution and pixel-value differencing, IET Image Process. 6 (2012) 677–686.

[23] J. Fridrich, M. Goljan, Practical steganalysis of digital images-state of the art, In Proc. SPIE Photonics imaging, Conference on Security and Watermarking of Multimedia Contents 4675 (2002) 1–13.

[24] N. Provos, Defending against statistical steganalysis, In Proceedings of the 10th conference on USENIX security symposium 10 (2001).

[25] J. Fridrich, M. Goljan, R. Du, Detecting LSB steganography in color and gray-scale images, IEEE Multimedia 8 (2001) 22–28.

[26] D. Ziou, S. Tabbone, Edge detection techniques – an overview, Pattern Recogn. Image Anal. 8 (1998) 537-559.

[27] T.M. Amarunnishad, V.K. Govindan, A.T. Mathew, A fuzzy complement edge operator, Int. Conf. Advanced Computing and Communications (2006) 344-348.

[28] L.R. Liang, C. G. Looney, Competitive fuzzy edge detection, Applied Soft Computing 3 (2003) 123-137.

[29] E.K. Kaur, E.V. Mutenja, E.S. Gill, Fuzzy logic based image edge detection algorithm in Matlab, International Journal of Computer Applications 1(22) (2010) 55-58.

[30] Suryakant, N. Kushwaha, Edge detection using fuzzy logic in Matlab, International Journal of Advanced Research in Computer Science and Software Engineering 2(4) (2012) 38-40.

[31] F. Smarandache, A unifying field in logics neutrosophic logic. neutrosophy, neutrosophic set, neutrosophic probability, third ed., American Research Press, 2003.

[32] Y. Guo, H.D. Cheng, New neutrosophic approach to image segmentation, Pattern Recognition 42(5) (2009) 587-595.

[33] Y. Guo, A. Sengür, A novel image edge detection algorithm based on neutrosophic set, Computers and Electrical Engineering 40(8) (2014) 3-25.

[34] T. Pevný, P. Bas, J. Fridrich, Steganalysis by subtractive pixel adjacency matrix, IEEE Trans. Inform. Forensics and Security 5(2) (2010) 215–224.

[35] J. Fridrich, J. Kodovský, Rich models for steganalysis of digital images, IEEE Trans. Inform. Forensics and Security 7(3) (2012) 868 –882.

[36] V. Holub, J. Fridrich, Low-complexity features for JPEG steganalysis using undecimated DCT, IEEE Trans. Information Forensics and Security 10(2) (2015) 219–228.

[37] J. Kodovský, J. Fridrich, V. Holub, Ensemble classifiers for steganalysis of digital media. *IEEE Transactions* Information Forensics and Security 7(2) (2012) 432–444.

[38] P. Bas, T. Filler, T. Pevný, Break our steganographic system: the ins and outs of organizing boss, International workshop on Information Hiding, LNCS 6958 (2011) 59–70.

[39] J. Fridrich, T. Pevný, J. Kodovský, Statistically undetectable JPEG steganography: Dead ends challenges, and opportunities, in ACM 9th workshop on Multimedia & security, (2007) 3–14.

[40] V. Holub, J. Fridrich, T. Denemark, Universal distortion function for steganography in an arbitrary domain, EURASIP Journal on Information Security 2014(1) (2014) 1–13.

[41] R. Cogranne, V. Sedighi, J. Fridrich, T. Pevný, Is Ensemble Classifier Needed for Steganalysis in High-Dimensional Feature Spaces?, IEEE International workshop on Information Forensics and Security (WIFS), Rome, Italy (2015) 16–19.

Highlights

- A steganographic technique based on wavelet packet decomposition (WPD) and neutrosophic set is proposed.
- An edge detector based on the neutrosophic set named (NSED) is introduced.
- An original image is decomposed into wavelet packet trees.
- Each wavelet packet tree is classified into edge/non-edge tree to embed more secret bits.
- The proposed method achieves higher embedding capacity with better imperceptibility compared to the recently published approaches.