Journal of King Saud University – Computer and Information Sciences xxx (2018) xxx–xxx

Contents lists available at ScienceDirect

Journal of King Saud University – Computer and Information Sciences

journal homepage: www.sciencedirect.com

Reversible steganographic method based on interpolation by bivariate linear box-spline on the three directional mesh

Amine Benhfid, El Bachir Ameur *, Youssef Taouil

Research Team MSISI – LaRIT, Department of Computer Science, Faculty of Sciences, Ibn Tofail University, Kenitra, Morocco

ARTICLE INFO

Article history:
Received 7 May 2018
Revised 20 August 2018
Accepted 17 September 2018
Available online xxxx

MSC 2018:
03C40
68P20
94A08
00A05
68P30

ABSTRACT

Data hiding is the discipline of hiding information into digital media. A reversible steganographic method allows to extract data from the stego file as well as to retrieve the cover file. This paper proposes a reversible steganographic method based on interpolation by linear box-splines on the three directional mesh. Secret data is hidden in the error between the cover and interpolated pixels. To have better imperceptibility, we search for the nearest value to the cover pixel that can dissimulate data; this was achieved with two techniques: Optimal Pixel Adjustment Procedure and Message Adaptive Error. The proposed method is tested through experiments on a variety of images and compared to prior works. Results indicate a large capacity of hiding and good values of PSNR. The proposed work was also tested by steganalysis attacks; results show a low detectability rate. We find in the comparison that the proposed work surpasses the literature in the capacity of hiding with an equivalent level of imperceptibility.

1. Introduction

Steganography is a data hiding technique, it consists of the dissimulation of a secret information into digital files so that an intended recipient can extract it successfully. These files can be texts, images, audio or videos; However, the most utilized one is image since it is shared widely everyday on the networks services; and most importantly because of the insensibility of the human visual system to small changes within images. The main objective of a steganographic system is that no one shall suspect the existence of the hidden information. The dissimulation of a secret data produces a new image which is called the stego image. To achieve the objective of steganography, it is primordial to keep as low as possible the distortions brought upon the cover image by the dissimulation process.

The steganographic system is evaluated by the imperceptibility, the capacity and the security. The imperceptibility is reached when the human eye can not distinguish between the cover and the stego images. The capacity is the maximum number of bits of the secret data that can be hidden in the cover image without causing perceptible artifacts. The security refers to the undetectability of the secret data inside the stego image.

The most common and well-known steganographic method is called least significant bit (LSB) substitution; it embeds secret data by substituting the LSB of a pixel by the secret bit (Bender et al., 1996). Many optimized LSB methods have been proposed later to break the uniformity of the histogram in this technique (Wang et al., 2001; Chan and Chen, 2004; Lin et al., 2009). It is a good steganographic mechanism since the changes in a least significant bits yield few changes in the original image. The human perceptibility is sensitive to big changes in the pixels of the smooth areas; while it is not sensitive to changes in the edge areas. In Fridrich et al. (2001), authors describe a very accurate and reliable method that can detect LSB embedding in randomly scattered pixels in both 24-bit color images and 8-bit gray-scale or color images. Not all pixels in a cover image can tolerate equal amount of changes without causing noticeable distortion. Hence, to improve the quality of the stego images, several adaptive methods have been proposed in which the amount of bits to be embedded in each pixel is variable (Wu and Tsai, 2003; Wu et al., 2005; Liao et al., 2011).

In reversible steganography, both the secret information and the cover image are retrieved by the recipient; this condition is required in some applications of steganography. In Jung and Yoo

* Corresponding author.
E-mail address: ameurelbachir@yahoo.fr (E.B. Ameur).
Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

https://doi.org/10.1016/j.jksuci.2018.09.016
1319-1578/

(2009), a reversible data hiding scheme based on interpolation is proposed. The scaling up allows to find the pixels of interpolation; those pixels are used to construct the interpolated pixels. Then, data is hidden in the error between the initial and the interpolated pixels. The obtained capacity is good, but it could be improved. In Wang et al. (2013), the algorithm utilized the same methodology while the hiding is based on the histogram shifting. The maximum capacity is not very large for interpolation based steganography; and this lack in the capacity is not compensated in PSNR. The steganographic scheme proposed in Hu and Li (2015) is based on extended interpolation; the capacity is enlarged by maximizing the error between neighboring pixels. The obtained capacity and imperceptibility are good but require improvement. Authors in Lee and Huang (2012) designed an efficient information hiding scheme based on interpolation by neighboring pixels (INP) in order to increase the payload. In Tang et al. (2014), the proposed high-Capacity Reversible Steganography (CRS) improved the capacity of hiding obtained by the INP scheme. In Ou et al. (2012), authors proposed a reversible watermarking based on optional prediction-error histogram modification to improve the watermarked image fidelity (or quality) at high embedding rate. In Pei et al. (2013), the proposed algorithm improved the embedding capacity by using histogram shifting and adaptive embedding. In Hu and Li (2015), a high capacity image steganographic scheme based on an extended interpolation method is proposed. In the premise of image quality assurance, the proposed scheme increases the capacity by maximizing the difference between neighbouring pixels.

In this paper, a reversible steganographic scheme based on interpolation by bivariate box-splines on the three directional mesh is proposed. To enlarge the capacity without degrading the imperceptibility, data is dissimulated into the difference between the interpolated pixel and either the maximum or the minimum of the four interpolation reference pixels. We choose between the minimum and maximum pixels the one that gives the greater difference with the interpolated pixel. Firstly, the secret data is added to the interpolated pixels as an error;which is adapted in order to have stego pixels as near as possible to the cover pixels. Secondly, data is hidden by substituting the *LSBs* of the interpolated pixels; then the Optimal Pixel Adjustment Procedure (OPAP) is utilized to minimize the difference between the obtained pixel and the cover pixel. To test the performance of the proposed work, experiments were accomplished on images with different degrees of complexity; and comparison to existing works was carried out. The proposed work provides very large capacity with a good compromise to PSNR. The proposed work is also tested by steganalysis attacks; results indicate a very low rate of detectability. Compared to literature, results show that the proposed scheme has large capacity of hiding while keeping the PSNR at a good level.

The remaining of the paper is organized as follows: Section 2 presents the utilized interpolation methods. In Section 3, the proposed scheme is explained in details. Section 4 discusses experimental results of tests and comparison to literature. Section 5 concludes the paper.

2. Related works

2.1. Neighbour mean interpolation (NMI)

Jung et al. proposed in Jung and Yoo (2009) the neighbour mean interpolation (NMI) hiding method. This scheme enlarges an original image to generate a predicted image and then embeds secret information in the predicted image to obtain the stego-image. The receiver reduces the stego image and extracts the secret information from it. Jung et al.'s scheme is shown schematically in Fig. 1; Fig. 1 (a) shows the original image O. A predicted pixel I is inserted between any two horizontal or vertical pixels. Fig. 1 (b) depicts the pixel reference C and Fig. 1 (c) shows the interpolated image. The predicted pixel I is computed as follows:

$$I_{(i,j)} = \begin{cases} \left\lfloor \frac{(O_{(ij-1)}+O_{(ij+1)})}{2} \right\rfloor & \text{if } i = 2m, j = 2n+1 \\ \left\lfloor \frac{(O_{(i-1,j)}+O_{(i+1,j)})}{2} \right\rfloor & \text{if } i = 2m+1, j = 2n \\ \left\lfloor \frac{(O_{(i-1,j-1)}+O_{(i-1,j)}+O_{(ij-1)})}{3} \right\rfloor & \text{otherwise,} \end{cases} \quad (1)$$

where m and n are the height and width of the cover image C, and (i,j) denotes the pixel's position. The secret message is then concealed into the predicted pixel to generate the stego pixel. The receiver reduces the stego image to recover the original image and extracts the secret message from the stego-image. In Fig. 1 (a), the reference pixels of the original image are $O_{(0,0)} = 145, O_{(0,1)} = 56, O_{(1,0)} = 116$ and $O_{(1,1)} = 101$. Suppose that the secret message is $msg = (00111110100000)_2$. We calculate the interpolation pixels $I_{(0,1)}, I_{(1,0)}$ and $I_{(1,1)}$ using the Eq. (1).

We find that $I_{(0,1)} = \frac{145+49}{2} = 97$ and $I_{(1,0)} = \frac{145+77}{2} = 111$ respectively. The virtual predictive value of the intermediate pixel $I_{(1,1)}$ is the average of $C_{(0,0)}$, $I_{(0,1)}$ and $I_{(1,0)}$, we find that $I_{(1,1)} = (145 + 97 + 111)/3 = 118$.

Next, the differences E_1, E_2 and E_3 are calculated by subtracting the references pixel $C_{(0,0)}$ from the three virtual predicted values $I_{(0,1)}, I_{(1,0)}$ and $I_{(1,1)}$. The equation is as follows:

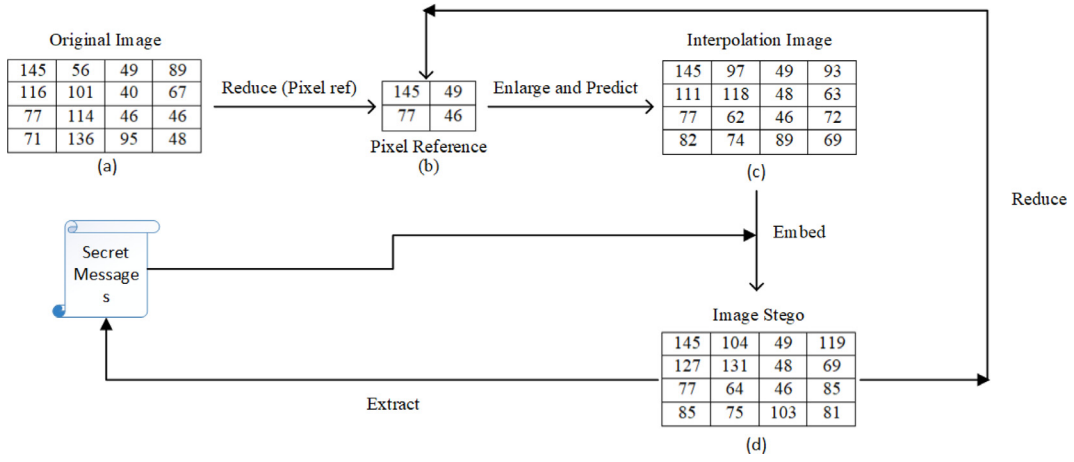


Fig. 1. Steps of NMI method using numerical values.

Please cite this article in press as: Benhfid, A., et al. Reversible steganographic method based on interpolation by bivariate linear box-spline on the three directional mesh. Journal of King Saud University – Computer and Information Sciences (2018), https://doi.org/10.1016/j.jksuci.2018.09.016

$$\begin{cases} E_1 = |I_{(0,1)} - C_{(0,0)}| \\ E_2 = |I_{(1,0)} - C_{(0,0)}| \\ E_3 = |I_{(1,1)} - C_{(0,0)}|. \end{cases}$$

Following the same example above, the differences are $E_1 = 145 - 97 = 48, E_2 = 145 - 111 = 34$ and $E_3 = 145 - 118 = 27$. By applying $\log_2$ on these differences, we find the decimal value L_i as follows: $L_1 = [\log_2(48)] = 5; L_2 = [\log_2(34)] = 5$ and $L_3 = [\log_2(27)] = 4$. Each L_i denotes how much bits of the secret message will be hidden in its corresponding interpolated pixel.

Now, we create the stego image using the interpolation image and the secret message *msg*. Since $L_1 = 5$, we embed 5 bits of the secret message $msg = (00111)_2 = 7$ into $I_{(0,1)} = 97$. Thus, $S_{(0,1)} = 97 + 7 = 104$. Using the same method we obtain the other pixels of stego image.

2.2. Interpolation by neighboring pixels (INP)

In Lee and Huang (2012) proposed a hiding scheme based on interpolation by neighbouring pixels (INP). In their scheme, the virtual predicted value I is the average of the reference pixel $C_{(0,0)}$ and average of two adjacent pixels as the virtual predicted value. The formula is as follows:

$$I_{(i,j)} = \begin{cases} \left\lfloor \frac{O_{(i,j-1)} + (O_{(i,j-1)} + O_{(i,j+1)})/2}{2} \right\rfloor & \text{if } i = 2m, j = 2n+1 \\ \left\lfloor \frac{O_{(i-1,j)} + (O_{(i-1,j)} + O_{(i+1,j)})/2}{2} \right\rfloor & \text{if } i = 2m+1, j = 2n \\ \left\lfloor \frac{I_{(i-1,j)} + I_{(i,j-1)}}{2} \right\rfloor & \text{otherwise.} \end{cases} \quad (2)$$

The example used in this section is the same as the example in Section 2.1. Using the Eq. (2), we obtain $I_{(0,1)} = \frac{145+(145+49)/2}{2} = 121$ and $I_{(1,0)} = \frac{145+(145+77)/2}{2} = 128$. The virtual predictive value of the intermediate pixel is the average of $I_{(0,1)}$ and $I_{(1,0)}$, we get $I_{(1,1)} = \frac{121+128}{2} = 125$. Next, the difference is computed to calculate the length of the secret message that can be concealed into the pixel. The difference is the distance between the maximum value and the predicted value. The maximum value is the largest one in the block of four original pixels, it is computed as follows:

$$Max = \max\{C_{(0,0)}, C_{(0,1)}, C_{(1,0)}, C_{(1,1)}\}.$$

The differences E_i are obtained by subtracting the predicted values from this maximum value.

$$\begin{cases} E_1 = |Max - I_{(0,1)}| \\ E_2 = |Max - I_{(1,0)}| \\ E_3 = |Max - I_{(1,1)}|. \end{cases}$$

For example, we consider $Max = \max\{145, 49, 77, 46\} = 145$; we obtain $E_1 = 24, E_2 = 17$ and $E_3 = 20$.

2.3. High-capacity reversible steganography (CRS)

Tang et al. proposed in Tang et al. (2014) a high-capacity reversible steganography (CRS) scheme. They improved the INP scheme by using two values $C_{\min}$ and $C_{\max}$ in the calculation of the predicted values I. These two values are computed as follows:

$$C_{\max} = \max\{C_{(i,j)}, C_{(i,j+1)}, C_{(i+1,j)}, C_{(i+1,j+1)}\},$$

$$C_{\min} = \min\{C_{(i,j)}, C_{(i,j+1)}, C_{(i+1,j)}, C_{(i+1,j+1)}\}.$$

The maximum value $C_{\max}$ and the minimum value $C_{\min}$ are used to compute the reference value AD as can be seen in the following equation:

$$AD = \left\lfloor \frac{3 \times C_{\min} + C_{\max}}{4} \right\rfloor \quad (3)$$

The predicted value $I_{(i,j)}$ is calculated using the neighboring pixels and the value AD defined in Eq. (3):

$$I_{(i,j)} = \begin{cases} \left\lfloor \frac{AD + (O_{(i,j-1)} + O_{(i,j+1)})/2}{2} \right\rfloor & \text{if } i = 2m, j = 2n+1 \\ \left\lfloor \frac{AD + (O_{(i-1,j)} + O_{(i+1,j)})/2}{2} \right\rfloor & \text{if } i = 2m+1, j = 2n \\ \left\lfloor \frac{O_{(i-1,j-1)} + I_{(i-1,j)} + I_{(i,j-1)}}{3} \right\rfloor & \text{otherwise.} \end{cases} \quad (4)$$

The differences $E_k(i,j)$ are computed by the comparison between the virtual predicted value I and the mean value of $C_{\max}$ and $C_{\min}$. The formula is given as follows:

$$E_1(i,j) = \begin{cases} C_{\max} - I_{(i,j+1)} & \text{if} I_{(i,j+1)} < \frac{C_{\min}+C_{\max}}{2} \\ I_{(i,j+1)} - C_{\min} & \text{if} I_{(i,j+1)} \geqslant \frac{C_{\min}+C_{\max}}{2}, \end{cases}$$

$$E_2(i,j) = \begin{cases} C_{\max} - I_{(i+1,j)} & \text{if} I_{(i+1,j)} < \frac{C_{\min}+C_{\max}}{2} \\ I_{(i+1,j)} - C_{\min} & \text{if} I_{(i+1,j)} \geqslant \frac{C_{\min}+C_{\max}}{2}, \end{cases} \quad (5)$$

$$E_3(i,j) = \begin{cases} C_{\max} - I_{(i+1,j+1)} & \text{if} I_{(i+1,j+1)} < \frac{C_{\min}+C_{\max}}{2} \\ I_{(i+1,j+1)} - C_{\min} & \text{if} I_{(i+1,j+1)} \geqslant \frac{C_{\min}+C_{\max}}{2}. \end{cases}$$

3. Proposed scheme

To control the image quality, the proposed scheme considers the complexity of the reduced pixels to adjust the length of the secret message. High-complexity areas are associated with long secret messages, whereas smooth areas are associated with short secret messages. This variance is used to judge whether an area is smooth or complex.

In this section, we introduce the interpolation method by bivariate linear box-spline on three directional mesh, which guaranties that the interpolation error E has an approximation order of $O(h^2)$ where h is the mesh step. Based on this interpolation method, we propose a reversible steganographic scheme that hides the secret data in the error between the cover and the interpolated pixels. In order to improve the imperceptibility by finding the nearest value to the cover pixel that can dissimulate data, we use Optimal Pixel Adjustment Procedure (OPAP) and Message Adaptive Error (MAE) methods.

3.1. Interpolation by linear box spline on three directional mesh

Let Δ be the three directional mesh which is the uniform triangulation of the plane whose set of vertices is $\mathbb{Z}^2$ and whose edges are parallel to the three directions $e_1 = (1,0), e_2 = (0,1)$ and $e_3 = (1,1)$ as shown in Fig. 2. Let us denote $S_n^r(\Delta)$ the space of piecewise polynomial functions of degree n and class C^r defined on Δ. A function f is said to be of class C^r if the derivatives $f', \ldots, f^{(r)}$ exist and are continuous.

The interpolation problem in the space $S_n^r(\Delta)$ consists of determining the interpolate operator:

$$I = \sum_{\alpha \in \mathbb{Z}^2} c_\alpha \mathbb{B}(. - \alpha)$$

which interpolates a given function f on the vertices of the triangulation Δ,

$$I(i,j) = f(i,j) \quad (6)$$

Please cite this article in press as: Benhfid, A., et al. Reversible steganographic method based on interpolation by bivariate linear box-spline on the three directional mesh. Journal of King Saud University – Computer and Information Sciences (2018), https://doi.org/10.1016/j.jksuci.2018.09.016

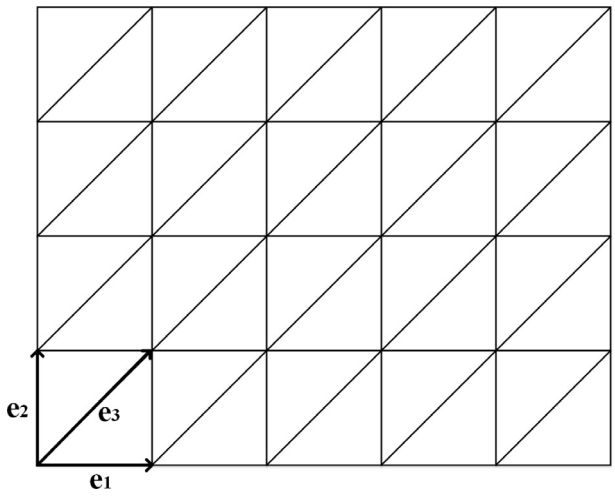


Fig. 2. Three directional mesh Δ.

where $\mathbb{B}$ is the B-spline in $S_n^r(\Delta)$ of compactly support on Δ. This problem is equivalent to determine the coefficients $\{c_\alpha\}$, see Unser (1999), De Boor et al. (1993), De Boor et al. (1983) and Chui (1988). In this section, our interest is the interpolation problem in the space $S_1^0(\Delta)$ of bivariate linear spline function on the three directional mesh Δ. For this, we define firstly the box-spline which forms the basis of this space.

The Haar bivariate box-spline is defined by the following equation:

$$\mathbb{B}_1(x,y) := \chi_{[0,1)^2}(x,y) = \begin{cases} 1 & \text{if}(x,y) \in [0,1)^2 \\ 0 & \text{if}(x,y) \in \mathbb{R}^2 \setminus [0,1)^2, \end{cases}$$

from which we see that $\mathbb{B}_1$ is a piecewise constant polynomial function; its support is shown in Fig. 3a. It is discontinuous around the boundary of its support and assumes the constant value 1 in the interior of its support $(0,1)^2$ as shown in Fig. 3b.

The bivariate linear box spline on the three directional mesh of the plane, called Courant Hat box spline, is defined by integrating $\mathbb{B}_1$ along the e_3 direction. We obtain the hat form shown in Fig. 4b while the support is shown in Fig. 4a.

$$\mathbb{B}_2(x,y) := \int_0^1 \mathbb{B}_1(x-t, y-t)dt, \forall (x,y) \in \mathbb{R}^2. \tag{7}$$

An explicit computation of the equation above leads to:

$$\mathbb{B}_2(x,y) = \begin{cases} y & \text{if } (x,y) \in A \\ x & \text{if } (x,y) \in B \\ 1+y-x & \text{if } (x,y) \in C \\ 2-x & \text{if } (x,y) \in D \\ 2-y & \text{if } (x,y) \in E \\ 1+x-y & \text{if } (x,y) \in F \\ 0 & \text{otherwise.} \end{cases} \tag{8}$$

The family $\{\mathbb{B}_2(.-\alpha), \alpha \in \mathbb{Z}^2\}$ forms a basis of the space $S_1^0(\Delta)$ of piecewise linear polynomial on the three directional mesh Δ.

Let $h \in \mathbb{R}_+^*, p, q \in \mathbb{N} \setminus \{0,1\}$, and let Δ_{pq} be the restriction of the uniform triangulation $h\Delta$ on a rectangular domain $\Omega = [0, ph] \times [0, qh]$. Let $V = \{v_{ij} = (ih, jh)/i = 0, \cdots, p/j = 0, \cdots, q\}$ be the set of $(p+1) \times (q+1)$ interpolation points in the rectangular domain Ω.

Since the Courant Hat box spline $\mathbb{B}_2$ satisfies $\mathbb{B}_2(1,1) = 1$ and $\mathbb{B}_2(i,j) = 0$ for all other vertices of Δ, then we obtain an explicit formula of the interpolation operator I_h

$$I_h = \sum_{\alpha \in \Delta_{p,q}} f(\alpha)\mathbb{B}_2(.h - \alpha + (1,1)) \tag{9}$$

which interpolates a given function f defined on Ω at the points of the set V, i.e.

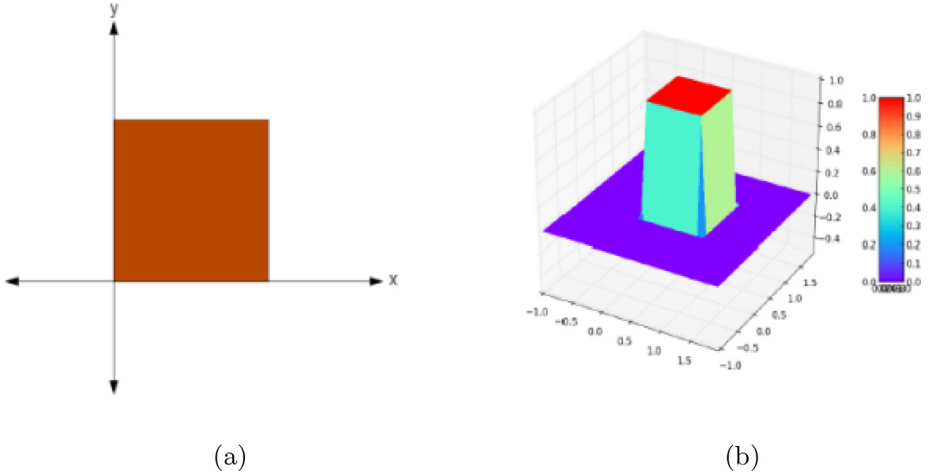
$$I_h(v_{ij}) = f(v_{ij}), \quad \text{for } i = 0, \cdots, p \text{ and } j = 0, \cdots, q.$$

Moreover, the interpolation error verifies $\|I_h - f\|_\infty \leqslant Kh^2$ where K is a constant and $\|.\|_\infty$ is infinity norm (see De Boor et al. (1993)).

Let $X := \{x_{ij} = \frac{v_{ij}+v_{i+1j}}{2}, i \neq p\}, Y := \{y_{ij} = \frac{v_{ij}+v_{ij+1}}{2}, j \neq q\}$ be the set of midpoints of horizontal and vertical edges respectively and let $Z := \{z_{ij} = \frac{v_{ij}+v_{i+1j+1}}{2}, i \neq p \text{ and } j \neq q\}$ be the set of the center of all squares in the uniform triangulation Δ_{pq}, as shown in Fig. 5.

By using the Eqs. (8) and (9), we obtain for $i = 0, \cdots, p$ and $j = 0, \cdots, q$:

$$\begin{cases} I_h(x_{ij}) = \frac{f(v_{ij})+f(v_{i+1j})}{2} \\ I_h(y_{ij}) = \frac{f(v_{ij})+f(v_{ij+1})}{2} \\ I_h(z_{ij}) = \frac{f(v_{ij})+f(v_{i+1j+1})}{2}. \end{cases} \tag{10}$$



(a) (b)

Fig. 3. (a): The support of $\mathbb{B}_1$, (b): The Haar box spline $\mathbb{B}_1$.

Please cite this article in press as: Benhfid, A., et al. Reversible steganographic method based on interpolation by bivariate linear box-spline on the three directional mesh. Journal of King Saud University – Computer and Information Sciences (2018), https://doi.org/10.1016/j.jksuci.2018.09.016

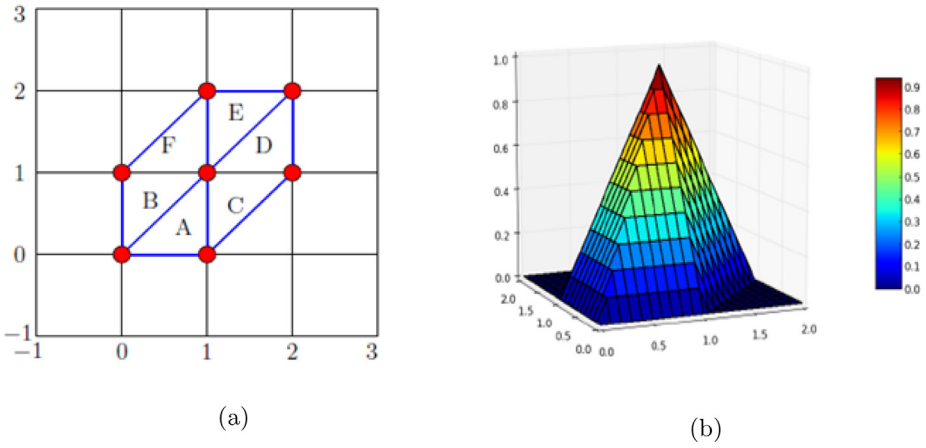


Fig. 4. (a): The support of $\mathbb{B}_2$, (b): The courant hat box spline $\mathbb{B}_2$.

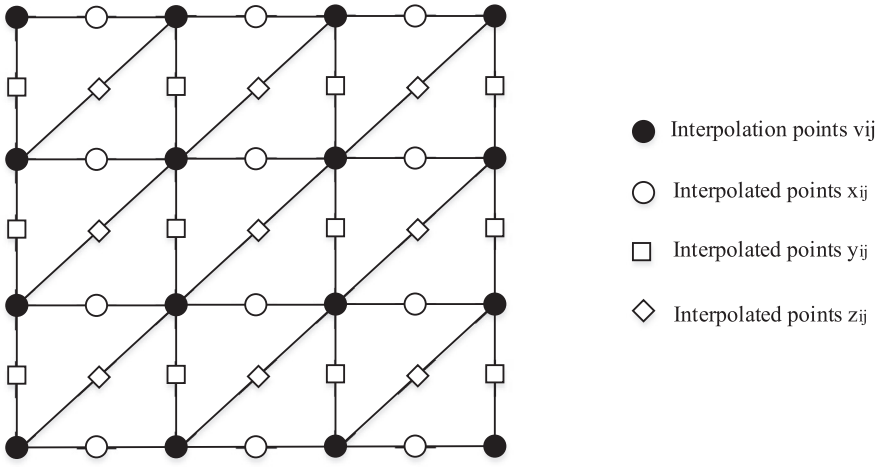


Fig. 5. Points and vertices pixels.

In our method, the cover image C represents the signal which we interpolate $C_{(i,j)} = f(v_{ij})$. By using the Eq. (8), the virtual predicted pixel $I_{(i,j)}$ is obtained by the following equation:

$$I_{(i,j)} = \begin{cases} \left\lfloor \frac{(O_{(i,j-1)}+O_{(i,j+1)})}{2} \right\rfloor & \text{if } i = 2p, j = 2q+1 \\ \left\lfloor \frac{(O_{(i-1,j)}+O_{(i+1,j)})}{2} \right\rfloor & \text{if } i = 2p+1, j = 2q \\ \left\lfloor \frac{(O_{(i-1,j-1)}+O_{(i+1,j+1)})}{2} \right\rfloor & \text{otherwise.} \end{cases} \quad (11)$$

3.2. The dissimulation using OPAP Method

The objective of applying (OPAP) is to minimize the error between the original image O and the stego image S. To dissimulate data, we calculate the error of interpolation as in CRS which was defined in the Eq. (5). Let $L_k(i,j) = [log_2(|E_k(i,j)|)]$be the number of successive bits of the secret message to be embedded by substitution into the interpolated pixel $I_{i,j}$ obtained by the linear box-spline on the directional mesh. When a message of size $L_k(i,j)$ bits is hidden by substitution into the interpolated pixel $I_{i,j}$, the message resides in the $L_k(i,j)$ least significant bits of the obtained pixel which we name $S^{(1)}_{i,j}$. Thus, the idea is to modify the bits of $S^{(1)}_{i,j}$ that do not carry the message (weights above $L_k(i,j)$) in order to get close to the original pixel $O_{i,j}$. This can be achieved by adding $\pm 2^{L_k(i,j)}$ to $S^{(1)}_{i,j}$; we obtain two new pixels which we name $S^{(2)}_{i,j}$ and $S^{(3)}_{i,j}$, they are calculated as follows: $S^{(2)}_{i,j} = S^{(1)}_{i,j} + 2^{L_k(i,j)}$ and $S^{(3)}_{i,j} = S^{(1)}_{i,j} - 2^{L_k(i,j)}$. The corresponding stego pixel $S_{i,j}$ is determined as the closest one to $O_{i,j}$ among $S^{(1)}_{i,j}, S^{(2)}_{i,j}$ and $S^{(3)}_{i,j}$:

$$S_{i,j} = S^{(r)}_{i,j} \quad \text{with} \quad r = \underset{k=1,2,3}{\operatorname{argmin}}(|O_{i,j} - S^{(k)}_{i,j}|)$$

Following the example shown in Fig. 6, the original pixel is $O_{0,1} = 56$, we hide the message $msg = 00111$ of size $L_1(0,1) = 5$ bits into the interpolated pixel $I_{0,1} = 97$ by substituting the 5 *LSB*s. We obtain $S^{(1)}_{0,1} = 103$; we find $S^{(2)}_{0,1} = S^{1}_{0,1} + 2^5 = 135$ and $S^{(3)}_{0,1} = S^{1}_{0,1} - 2^5 = 71$. Since 71 is the closest value to $O_{0,1}$ among 135, 103 and 71, then the stego pixel $S_{0,1} = S^{(3)}_{0,1} = 71$.This procedure allows us to reduce the difference from $103 - 56 = 47$ to $71 - 56 = 15$.

3.3. Hiding message using MAE method

The Message Adaptive Error is a method based on the error between the original image and the interpolation resultant image. The message is not substituted int the *LSB*s of the pixel $I_{i,j}$ interpolated by the method described in the Section 3.1; but it is added to $I_{i,j}$ as a decimal value *Msg*. In the extraction, *Msg* is the difference between the stego pixel $S_{i,j}$ and the interpolated pixel $I_{i,j}$. Since

Please cite this article in press as: Benhfid, A., et al. Reversible steganographic method based on interpolation by bivariate linear box-spline on the three directional mesh. Journal of King Saud University – Computer and Information Sciences (2018), https://doi.org/10.1016/j.jksuci.2018.09.016

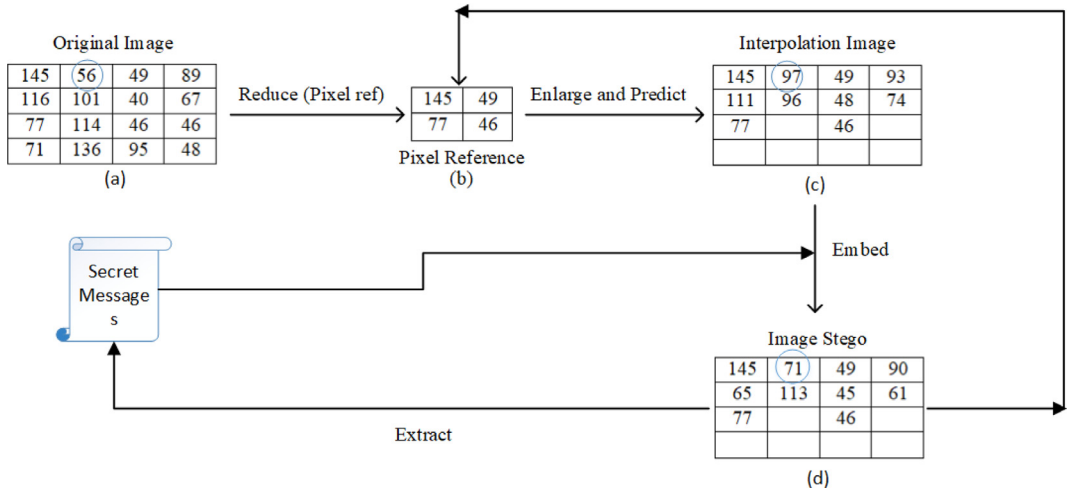


Fig. 6. Reversible scheme with OPAP method using numerical values.

the sign of this difference is irrelevant, then we have two possibilities, we can add Msg or subtract it from $I_{i,j}$:

$$S_{i,j} = I_{i,j} \pm Msg.$$

To choose the convenient sign, we calculate both $S_{i,j}^{(1)} = I_{i,j} + Msg$ and $S_{i,j}^{(2)} = I_{i,j} - Msg$, then we choose the closest one to the original pixel $O_{i,j}$:

$$S_{i,j} = \begin{cases} S_{i,j}^{(1)} = I_{i,j} + Msg & if \quad |O_{i,j} - S_{i,j}^{(1)}| < |O_{i,j} - S_{i,j}^{(2)}| \\ S_{i,j}^{(2)} = I_{i,j} - Msg & \text{otherwise.} \end{cases}$$

Fig. 7 shows the same example used in the previous section; the value of the original pixel is $O_{0,1} = 56$. We suppose that we hide the 5 bits of the message vector "00111" in the pixel $I_{0,1} = 97$ predicted by the interpolation method. The decimal value of these 5 bits is $Msg = 7$. Then, we find $S_{0,1}^{(2)} = 97 - 7 = 90$ and $S_{0,1}^{(1)} = 97 + 7 = 104$. The differences are $|O_{0,1} - S_{0,1}^{(1)}| = 48$ and $|O_{0,1} - S_{0,1}^{(2)}| = 34$. Since $34 < 48$, we choose then $S_{0,1} = S_{0,1}^{(2)} = 90$.

4. Experiment results

In this section, we use the standard images shown in Fig. 8. They are 512×512 8-bit gray-scale images which are usually used in tests. We apply the methods explained in the previous sections to achieve the test and comparison based on the imperceptibility and the capacity of embedding.

The capacity of embedding refers to the maximal quantity of information that can be hidden without generating perceptible artefacts on the cover image. It is expressed by the number of bits that can be hidden in the image or the number of bits that can be hidden in one pixel (bit per pixel bpp).

The PSNR informs about the imperceptibility of the steganographic scheme. When it is beyond 30 dB, the human eye can not distinguish between the cover and stego images. This metric is calculated as follows:

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right) \text{dB},$$

where

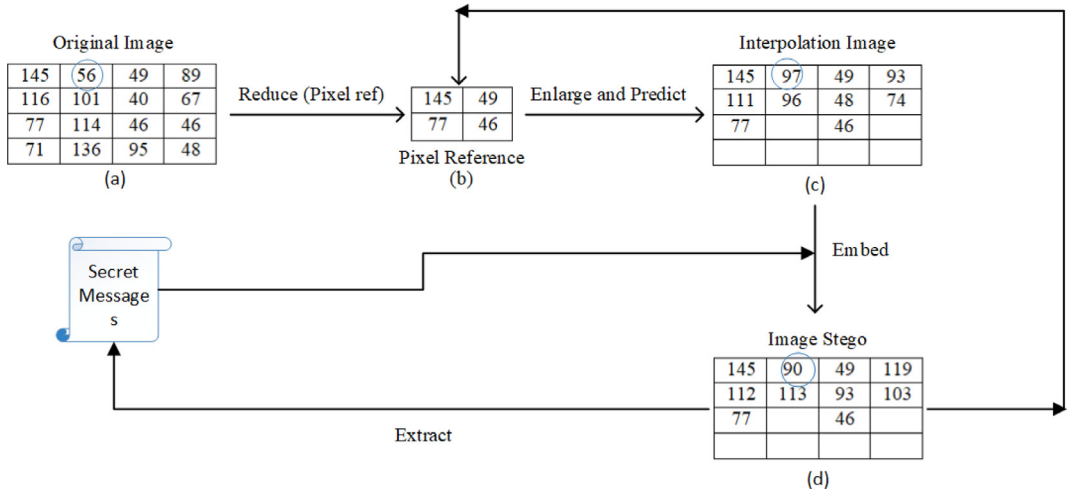
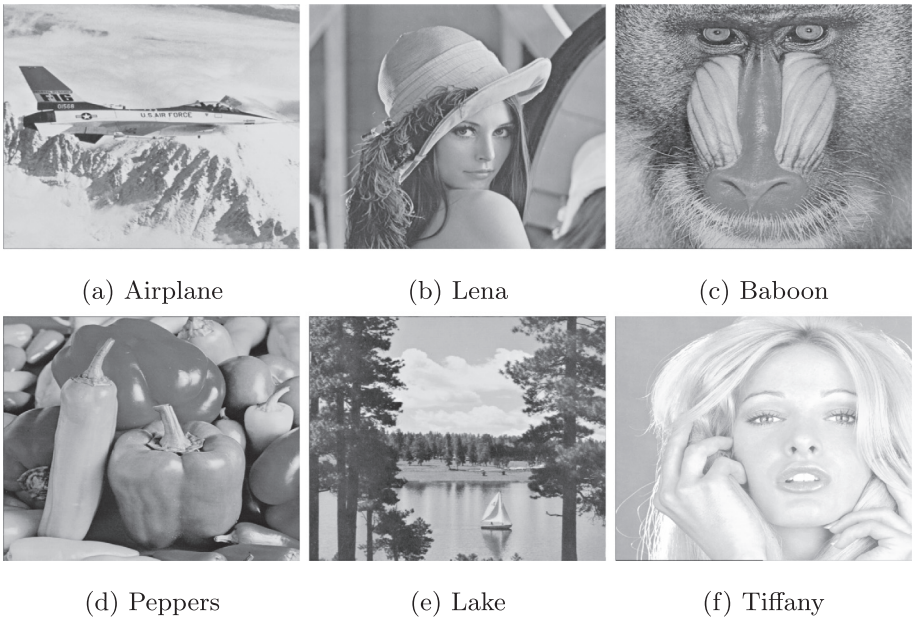


Fig. 7. Reversible scheme with MAE method using numerical values.

Please cite this article in press as: Benhfid, A., et al. Reversible steganographic method based on interpolation by bivariate linear box-spline on the three directional mesh. Journal of King Saud University – Computer and Information Sciences (2018), https://doi.org/10.1016/j.jksuci.2018.09.016



(a) Airplane (b) Lena (c) Baboon

(d) Peppers (e) Lake (f) Tiffany

Fig. 8. Six 512 × 512 grayscale testing images.

$$MSE = \frac{1}{512^2}\sum_{i=1}^{512}\sum_{j=1}^{512}(C_{i,j} - S_{i,j})^2.$$

We use also the Image Fidelity (*IF*) to evaluate the imperceptibility. The IF has to be very close 1; because the difference $1 - IF$ measures the ratio of the error energy to the image energy. It is calculated as follows:

$$IF = 1 - \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(S_{i,j} - C_{i,j})^2}{\sum_{i=1}^{M}\sum_{j=1}^{N}C_{i,j}^2}.$$

To estimate the similarity of the cover and stego image, we use the metrics Normalized Correlation Coefficient (*NCC*) and the *Q*-index. These two parameters take values between −1 and 1. The closest they are to 1, the more similar are the images. When they are close to 0, the images are said uncorrelated. When it is close to −1, they are said opposite.

$$NCC = \frac{\theta_{cs}}{\theta_c\theta_s}, \quad Q = 4\frac{\theta_{cs}}{(\theta_c^2 + \theta_s^2)}\frac{\eta_c\eta_s}{(\eta_c^2 + \eta_s^2)}. \tag{12}$$

The parameters η_c and η_s are the mean values of the cover and stego images respectively, and θ_c, θ_s and θ_{cs} are given by the following expressions

$$\theta_c = \sqrt{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(C_{i,j} - \eta_c)^2}, \theta_s = \sqrt{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(S_{i,j} - \eta_s)^2},$$

$$\theta_{cs} = \sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(C_{i,j} - \eta_c)(S_{i,j} - \eta_s).$$

To evaluate our work, we perform a comparison to the NMI, INP and CRS methods. Tables 1 and 2 show the values of the capacity and the metrics of the imperceptibility obtained by using the NMI (Jung and Yoo, 2009), INP (Lee and Huang, 2012), CRS (Tang et al., 2014) and the proposed methods with OPAP and MAE. We used the images Lena, Mandrill, Airplane, Peppers, Lake and Tiffany, they

Table 1
The comparison of capacity (bpp) and PSNR between NMI, INP, CRS and proposed method based on (OPAP) and (MAE).

Image	Metric	NMI (Jung and Yoo, 2009)	INP (Lee and Huang, 2012)	CRS (Tang et al., 2014)	Proposed	
					OPAP	MAE
Lena	PSNR	34.8457	35.936	38.2489	40.3762	40.2854
	Capacity	0.75875	1.2698	1.7617	1.8109	1.8109
Mandrill	PSNR	27.0762	27.5971	28.5853	29.7128	30.7378
	Capacity	1.6232	2.3201	2.8916	2.9432	2.9432
Airplane	PSNR	33.0183	33.659	38.2641	41.6837	41.3954
	Capacity	0.68324	1.1232	1.5856	1.637	1.637
Peppers	PSNR	34.377	35.3741	36.3833	38.7154	38.6007
	Capacity	0.74458	1.2716	1.782	1.8373	1.8373
Lake	PSNR	32.5011	32.5902	33.6581	35.6969	36.3886
	Capacity	1.0373	1.6381	2.168	2.2234	2.2234
Tiffany	PSNR	34.5023	35.4419	38.2357	39.5246	40.1976
	Capacity	0.63644	1.0877	1.5759	1.6367	1.6367

Please cite this article in press as: Benhfid, A., et al. Reversible steganographic method based on interpolation by bivariate linear box-spline on the three directional mesh. Journal of King Saud University – Computer and Information Sciences (2018), https://doi.org/10.1016/j.jksuci.2018.09.016

Table 2
The comparison of the IF, NCC and Q-index between NMI, INP, CRS and proposed method based on (OPAP) and (MAE).

Image	Metric	NMI (Jung and Yoo, 2009)	INP (Lee and Huang, 2012)	CRS (Tang et al., 2014)	Proposed	
					OPAP	MAE
Lena	IF	0.99881	0.99908	0.99946	0.99967	0.99966
	NCC	0.99545	0.99644	0.99796	0.99873	0.99869
	Q-index	0.99543	0.99644	0.99794	0.99873	0.99869
Mandrill	IF	0.9931	0.99381	0.99504	0.99619	0.99699
	NCC	0.96386	0.96803	0.9749	0.98053	0.9843
	Q-index	0.96371	0.96801	0.97484	0.9805	0.98428
Airplane	IF	0.99881	0.99888	0.99953	0.99977	0.9998
	NCC	0.99061	0.99117	0.99633	0.99821	0.9984
	Q-index	0.9906	0.99116	0.99633	0.99821	0.9984
Peppers	IF	0.99767	0.99758	0.9981	0.99897	0.99916
	NCC	0.99307	0.99281	0.99442	0.99696	0.9975
	Q-index	0.99305	0.9928	0.9944	0.99695	0.9975
Lake	IF	0.99744	0.99728	0.99782	0.99867	0.99898
	NCC	0.99408	0.99374	0.99504	0.99695	0.99764
	Q-index	0.99408	0.99373	0.99501	0.99694	0.99764
Tiffany	IF	0.99942	0.99949	0.99972	0.99982	0.99985
	NCC	0.98465	0.98672	0.99281	0.99527	0.99595
	Q-index	0.98464	0.9867	0.9928	0.99527	0.99595

have different degree of texture which is an important criterion in the interpolation based stegnography.

Results in Tables 1 and 2 indicate that the proposed methods provide the larger capacity; and at the same time, they have the highest imperceptibility. We proposed to interpolate by the average of the neighbouring pixels horizontally, vertically and diagonally to minimize the error between the interpolated and the original pixels; this gives a better image quality. Furthermore, by using the OPAP or the MAE, the stego pixel is the closest possible to the original one. Hence, the obtained PSNR by the proposed methods are the highest. The values of IF, NCC and Q-index in Table 2 obtained by the proposed methods are closer to their optimal value 1 than the three other methods. For the capacity, we adopted the same methodology used in CRS to calculate the error of interpolation. However, what made the difference with CRS in the obtained capacity is the interpolation technique we utilized; it allowed us to surpass the capacity of CRS; because the interpolation in CRS is concentrated on the minimum pixel of the four reference pixels; whereas in the proposed method, the interpolation is the average in the three directions.

Fig. 9 shows the evolution of the PSNR as we increase the size of the secret message from 0.1 bpp to 1 bpp for the six test images shown before in Fig. 8. As can be seen in Fig. 9, the proposed work using OPAP and MAE offers better trade-off between the PSNR and the capacity of hiding.

To evaluate the security of the proposed steganographic scheme, we use the statistical attack χ^2 (Westfeld and Pfitzmann, 1999). It is based on the idea that at the end of the dissimulation process, the sum of the frequencies of each pair of pixels $(2i, 2i+1)$ in the histogram remains unchanged; and the frequency of $2i$ and $2i+1$ tends to the average of their initial values. Let v_{2i} and v_{2i+1} be the frequencies of $2i$ and $2i+1$ in the histogram respectively. Their average is $\eta_i = \frac{v_{2i}+v_{2i+1}}{2}$. The χ^2_n statistic with n degree of freedom is then calculated as follows:

$$\chi^2_n = \sum_{i=0}^{n+1} \frac{(v_{2i} - \eta_i)^2}{\eta_i}.$$

The degree of freedom is the number of pairs $(2i, 2i+1)$ having a sum of frequencies greater than 4, i.e.

$$n = card\{(2i, 2i+1); 0 \leqslant i \leqslant 127; v_{2i} + v_{2i+1} > 4\}.$$

Then, the probability that the attacked image hides a secret data is computed as follows:

$$p = 1 - \frac{1}{2^{\frac{n}{2}}\Gamma\left(\frac{n}{2}\right)} \int_0^{\chi^2_n} e^{-\frac{t}{2}} t^{\frac{n}{2}-1} dt,$$

while Γ is the Gamma function defined for every positive x by

$$\Gamma(x) = \int_0^{+\infty} t^{x-1} e^{-t} dt.$$

Table 3 shows the PSNR and χ^2 values of the same six images for the proposed methods. To measure the contribution of the OPAP and MAE, we use only the LSB substitution which is the simplest way of insertion; we hide data by substituting the LSBs of the interpolated pixels. Results are shown in the column LSB for both PSNR and χ^2 test. Obviously, the PSNR of the LSB substitution is the lowest. This shows the effectiveness of the proposed MAE and OPAP; they search for the closest pixel possible to the original pixel that can hide data. We obtain an amelioration of the PSNR with 3 dB.

The χ^2 results in Table 3 indicate a very low rate of detectability; the proposed work is not detected by this attack. The changes of the histogram are not predictable by χ^2.

In Table 4, the proposed work is compared to schemes developed in Ou et al. (2012), Pei et al. (2013), Wang et al. (2013) and Hu and Li (2015). The comparison is done on the images Lena, Mandrill and Airplane. As can be seen, the proposed methods OPAP and MAE outperform the other methods in the PSNR and the capacity at the same time.

The proposed work surpasses the work developed by Ou et al. (2012) in both PSNR and the capacity for the images Lena and Airplane. The difference in PSNR is 5 and 7 dB respectively, the capacity we obtain is respectively 1.6 times and 1.3 times greater. For the image Mandrill, while the PSNR of the proposed work is smaller by 9 dB, the capacity is almost 6 times greater. The PSNR obtained by Wang et al. (2013) is constant for the three images with a significant variation of the capacity of hiding. It is higher than our PSNR with 8 dB but our capacity is more than 6 times greater than theirs. In comparison to Pei et al. (2013), we obtained a comparable capacity for Lena and Airplane but a remarkably greater PSNR. For Mandrill, the proposed work gives better PSNR

Please cite this article in press as: Benhfid, A., et al. Reversible steganographic method based on interpolation by bivariate linear box-spline on the three directional mesh. Journal of King Saud University – Computer and Information Sciences (2018), https://doi.org/10.1016/j.jksuci.2018.09.016

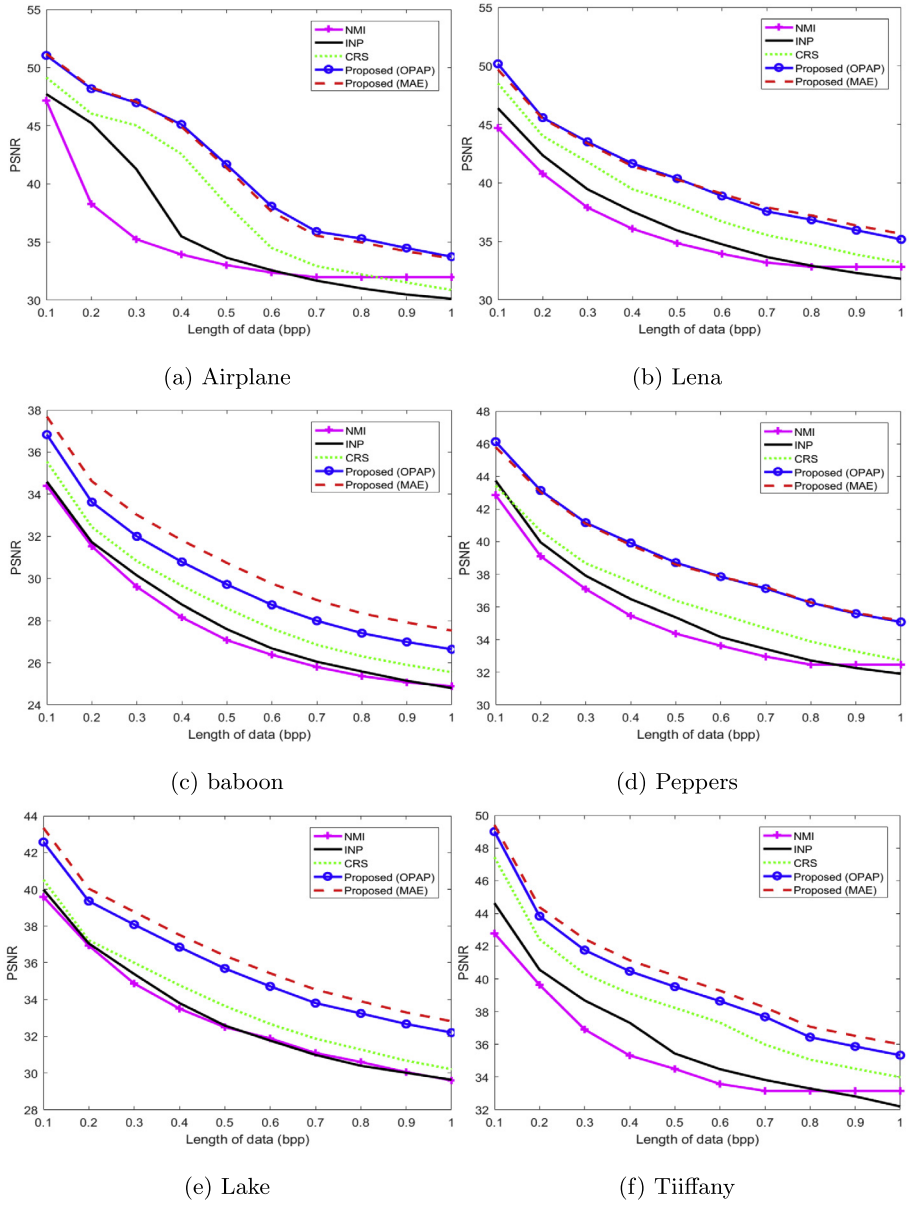


Fig. 9. Comparison of all interpolation methods with the two proposed methods over six standard testing images.

Table 3
χ^2 results on six usual images after using OPAP and MAE.

Metric	PSNR			χ^2 (Westfeld and Pfitzmann, 1999)		
Image	LSB	MAE	OPAP	LSB	MAE	OPAP
Lena	37.2916	40.2854	40.3762	4.1481e−10	1.3890e−08	6.5503e−15
Mandrill	27.2397	30.7378	29.7128	0.5239	0.8667	2.2922e−04
Airplane	38.6339	41.3954	41.6837	0	0	0
Peppers	35.5388	38.6007	38.7154	6.0263e−13	1.9386e−11	0
Lake	32.7401	36.3886	35.6969	4.8950e−13	0	0
Tiiffany	36.7134	40.1976	39.5246	0	0	0

and remarkably better capacity. In Hu and Li (2015), while the capacity increases with only 0.2 bpp from Lena and Airplane to Mandrill, the PSNR decreases with 4 dB. The capacity provided by the proposed work increases significantly for images with a lot of texture as can be seen in comparison between Lena and Mandrill, the capacity grows by 61%. Results in this table indicate that the proposed work gives better compromise between the PSNR and the capacity of hiding than the other works. We obtain around 40 dB in PSNR for almost 2 bpp capacity and 30 dB for almost 3 bpp.

Please cite this article in press as: Benhfid, A., et al. Reversible steganographic method based on interpolation by bivariate linear box-spline on the three directional mesh. Journal of King Saud University – Computer and Information Sciences (2018), https://doi.org/10.1016/j.jksuci.2018.09.016

Table 4
Comparison of our proposed work with four reversible data hiding methods basing on image quality and capacity.

Methods	Metric	Lena	Mandrill	Airplane
Ou et al. (2012)	PSNR	35.3729	38.9982	34.1648
	Capacity (bpp)	1.0954	0.5321	1.2242
Wang et al. (2013)	PSNR	48.6747	48.9441	48.7547
	Capacity (bpp)	0.2716	0.0952	0.3332
Pei et al. (2013)	PSNR	26.8483	21.4183	26.7403
	Capacity (bpp)	1.8388	1.2496	1.8108
Hu and Li (2015)	PSNR	34.6967	30.1452	34.2991
	Capacity (bpp)	1.6945	1.8483	1.6636
Proposed (OPAP)	PSNR	40.3762	29.7128	41.6837
	Capacity (bpp)	1.8109	2.9432	1.637
Proposed (MAE)	PSNR	40.2854	30.7378	41.3954
	Capacity (bpp)	1.8109	2.9432	1.637

5. Conclusion

In this paper, we introduced new data hiding methods that allowed us to increase the capacity while keeping the imperceptibility at a good level. Depending on the image's complexity, theadopted interpolation technique and the method utilized to calculate the interpolation error enabled us to obtain a good capacity. Results show that the capacity and PSNR of the proposed methods whether using OPAP or MAE are higher than NMI, INP and CRS algorithms. In addition, the χ^2 test results prove the undetectability of the proposed algorithm. Therefore, these substantial performance improvements demonstrate the effectiveness of the proposed scheme. In comparison to wavelet transform based steganographic schemes, the wavelets forbid to dissimulate data in the bloc of the approximation; this subtracts quarter of the image size from the capacity. However, the imperceptibility is good. The proposed work has better capacity but lower imperceptibility than wavelet based schemes. In our future works, we will focus on strengthening the robustness of our work and study its resistance to attacks trying to destroy the information hidden inside the stego image.

References

Bender, D.W., Gruhl, N.M., Lu, A., 1996. Techniques for data hiding. IBM Syst. J. 35, 313–316.
Chan, C.K., Chen, L.M., 2004. Hiding data in images by simple LSB substitution. Pattern Recognit. 37, 469–474.
Chui, C.K., 1988. Multivariate Splines. Soc. for Indust. & Appl, Math, Philadelphia.
De Boor, C., Hllig, K., Riemenschneider, S., 1983. Bivariate cardinal interpolation by splines on a three-direction mesh. Illinois J. Math. 29 (4), 533–566.
De Boor, C., Hllig, K., Riemenschneider, S., 1993. Box Splines. Springer-Verlag, New York, Berlin.
Fridrich, J., Goljan, M., Du, R., 2001. Reliable detection of LSB steganography in grayscale and color images. In: Smith, Y., (Ed.), Proc, of the ACM Workshop on Multimedia and Security, Ottawa, Canada, October 5, pp. 27–30.
Hu, J., Li, T., 2015. Reversible steganography using extended image interpolation technique. Comput. Electr. Eng. 26, 447–455.
Hu, J., Li, T., 2015. Reversible steganography using extended image interpolation technique. Comput. Electr. Eng. 46.
Jung, K., Yoo, K., 2009. Data hiding method using image interpolation. Comput. Standards Interfaces 31, 465–470.
Lee, C.F., Huang, Y.L., 2012. An efficient image interpolation increasing payload in reversible data hiding. Expert Syst. Appl. 39, 6712–6719.
Liao, X., Wena, Q., Zhang, J., 2011. A steganographic method for digital images with four-pixel differencing and modified LSB substitution. Proc. Inst. Elect. Eng., Vis. J. Vis. Commun. Image R. 22, 1–8.
Lin, I.C., Lin, Y.B., Wang, C.M., 2009. Hiding data in spatial domain images with distortion tolerance. Comput. Stand. Inter. 31, 458–464.
Ou, B., Zhao, Y., Ni, R., 2012. Reversible watermarking using optional prediction error histogram modification. Neurocomputing 93, 67–76.
Pei, Q., Wang, X., Li, Y., Li, H., 2013. Adaptive reversible watermarking with improved embedding capacity. J. Syst. Softw. 86, 2841–2848.
Tang, M.W., Hu, J., Song, W., 2014. A high-capacity image steganography using multi-layer embedding. Optik 125, 3972–3976.
Unser, M., 1999. Splines: a perfect fit for signal and image processing. IEEE Signal Processing Mag. 16 (6), 22–38.
Wang, R.Z., Lin, C.F., Lin, J.C., 2001. Image hiding by optimal LSB substitution and genetic algorithm. Pattern Recognit. 34, 671–683.
Wang, X.T., Chang, C.C., Nguyen, T.S., Li, M.C., 2013. Reversible data hiding for high quality images exploiting interpolation and direction order mechanism. Digital Signal Process. 23, 569–577.
Westfeld, A., Pfitzmann, A., 1999. Attacks on Steganographic Systems. Lecture Notes in Computer Science in International Workshop on Information Hiding. 1768, 61–76.
Wu, D.C., Tsai, W.H., 2003. A steganographic method for images by pixel-value differencing. Pattern Recognit. Lett. 24, 1613–1626.
Wu, H.C., Wu, N.I., Tsai, C.S., Hwang, M.S., 2005. Image steganographic scheme based on pixel-value differencing and LSB replacement methods. Proc. Inst. Elect. Eng., Vis. Images Signal Process. 152, 611–615.

Please cite this article in press as: Benhfid, A., et al. Reversible steganographic method based on interpolation by bivariate linear box-spline on the three directional mesh. Journal of King Saud University – Computer and Information Sciences (2018), https://doi.org/10.1016/j.jksuci.2018.09.016