



Hog based high capacity and blind image steganography technique with tamper detection and content authentication

Iffat Rehman Ansari¹  · Mohd Ayyub Khan²  · Ekram Khan² 

Received: 8 October 2025 / Accepted: 13 December 2025
© Bharati Vidyapeeth's Institute of Computer Applications and Management 2025

Abstract

This paper proposes a Histogram of Oriented Gradients (HOG) based high capacity and blind image steganography technique with tamper detection and content authentication capabilities to verify the integrity and authenticity of the secret and confidential data. In this approach, an HOG feature vector is computed for each block of the cover image to determine the dominant gradient direction. The gradient magnitude corresponding to the dominant gradient direction is thresholded to generate Blocks of Interest (BOIs), and the message bits are embedded in the BOIs according to the dominant gradient direction. The simulation results demonstrate that the proposed technique improves the payload by up to 27.2% and raises the Peak Signal-to-Noise Ratio (PSNR) value by up to 3.4 dB compared to other state-of-the-art methods. By adjusting the values of the embedding parameters, the proposed scheme provides a good balance between capacity and image quality. Authentication analysis confirms that the proposed method exhibits high fragility to various attacks, with the Number of Blocks Tampered (NBT) reaching up to 75.7%, highlighting its effectiveness in tamper detection and content authentication. Additionally, the proposed technique is computationally efficient with reduced embedding and extraction times compared to the state-of-the-art approaches.

Keywords Secure Communication · Histogram of Oriented Gradients (HOG) · Dominant Gradient Direction · Blocks of Interest (BOIs) · Payload · Imperceptibility · Tamper detection · Content authentication

1 Introduction

In today's digital world, information security has become a significant concern due to readily and easily accessible communication networks and information processing tools [1–4]. The two fundamental pillars of information security systems that enable secure data transmission are information encryption and information hiding [5–7]. Information

encryption, also known as cryptography, scrambles a message into an unreadable format, while information hiding conceals the existence of the message to make it invisible. Information hiding can be further classified into watermarking and steganography. Watermarking is widely used for copyright protection of digital media by embedding a watermark logo into it [8, 9], whereas Steganography embeds a secret message in digital media in such a way that makes the message undetectable to typical users of public networks. Among various digital media, digital images are one of the most commonly used media for concealing secret messages, a process referred to as image steganography [10–12].

Image steganography schemes can be broadly classified into spatial and frequency domain methods. Spatial domain methods hide the secret data by directly altering the pixel values of the cover image, while frequency domain methods hide the secret data by modifying the transform coefficients of the cover image. Spatial domain methods are fast, simple, computationally less complex, and cost-effective, whereas transform domain methods require significant processing time to perform forward and inverse transformations [13].

✉ Iffat Rehman Ansari
iransari.uwp@amu.ac.in

Mohd Ayyub Khan
mayyubkhan@zhcet.ac.in

Ekram Khan
ekhan.el@amu.ac.in

¹ Electronics Engineering Section, University Women's Polytechnic, Aligarh Muslim University, Aligarh 202002, India

² Department of Electronics Engineering, Aligarh Muslim University, Aligarh 202002, India

The major challenge in image steganography is to achieve a high payload while maintaining high imperceptibility. Generally, there is a trade-off between payload and imperceptibility; that is, to achieve a high payload, more pixels or transform coefficients need to be altered, which in turn decreases imperceptibility [14]. Another critical issue is to secure secret and confidential data from automated detection systems, as they can more easily trace and identify the hidden data compared to the human visual system (HVS). The simpler the concealing algorithm, the more easily it can be identified, and the larger the payload, the more detectable the hidden data will be [15, 16].

To address these issues, a blind image steganography technique is proposed that exploits HOG features to compute and identify edge regions in terms of Blocks of Interest (BOIs), and then embed more data along the dominant edge direction of these BOIs to enhance the payload while maintaining imperceptibility. Furthermore, the proposed embedding algorithm is designed to embed data in different pixels of BOIs using three distinct edge directions — horizontal, vertical, and diagonal, providing enhanced security compared to methods that embed data using only one direction. Additionally, there is a non-uniform distribution of message bits, embedding more message bits in pixels along the dominant gradient direction of BOIs than in other pixels of the BOIs. Hence, it would be challenging for automated detection systems to trace and detect the concealed sequence of secret data. The simulation results demonstrate that the proposed technique achieves a high payload with improved imperceptibility, shorter embedding and extraction times, indicating its computational efficiency compared to state-of-the-art methods. Moreover, the overhead bits employed in the proposed method serve a dual purpose. In addition to identifying the BOI category, the overhead bits also quantify the tampered blocks, thereby facilitating reliable tamper detection and authentication to verify the integrity and authenticity of the secret confidential data. Along with data security, tamper detection, and content authentication are equally crucial in several critical applications, as the secret and confidential data is unreliable without verification and authentication. Our proposed data hiding algorithm also provides a solution to this problem.

The main **contributions** of this paper are as follows:

- Design and implementation of an HOG feature-based image steganographic technique to achieve high payload with better imperceptibility.
- Leveraging HOG features to embed more message bits in the pixels of BOIs along the dominating gradient direction. The directional embedding strategy improves both payload and security while ensuring good imperceptibility.

- Offers users the flexibility to balance payload and imperceptibility through adjustment of the embedding parameters.
- Facilitates blind message extraction process, tamper detection, and content authentication.
- Payload, imperceptibility, authentication, and complexity analyses are performed to assess the effectiveness of the proposed method compared to the state-of-the-art methods.

The remainder of the paper is structured as follows. The systematic literature review is described in Sect. 2. Section 3 presents the proposed steganographic method in detail. The simulation results, payload, imperceptibility, authentication, and timing analyses are reported and explained in Sect. 4. Finally, the proposed method is concluded in Sect. 5.

2 Literature review

Several image steganographic techniques based on spatial and frequency domain methods have been explored and studied.

One of the most common and simple steganography techniques in the spatial domain proposed by Chan et al. [17] is using the LSB substitution method, in which the message is embedded directly in the LSBs of the selected pixels. The method employs an optimal pixel adjustment process (OPAP) to enhance the quality of the stego image, but it can be easily detected and manipulated due to the uniform and sequential distribution of message bits across all pixels. The authors in [18] proposed a data hiding technique based on Pixel Value Differencing (PVD), which enhances security by utilizing a non-uniform distribution of message bits. It embeds a larger number of message bits in regions where large pixel differences exist. This may cause greater distortion in complex regions and result in a degradation of image quality. Another data hiding method, based on PVD and modified Exploiting Modification Direction (EMD) in [19], offers a satisfactory payload and better image quality; however, this approach requires significantly longer execution time. Sahu et al. [20] proposed a steganographic scheme based on Overlapped PVD (OPVD) to further improve the payload. The scheme yields a large payload and reduced execution time. However, the low Peak Signal-to-Noise Ratio (PSNR) values result in increased distortion and degraded image quality. The data hiding technique proposed by Xuan et al. [21] in the transform domain embeds data into the middle bit planes of the Integer Wavelet Transform (IWT) coefficients in the middle frequency (MF) and high frequency (HF) subbands. Consequently, the payload is improved at the cost of image quality. However, there is

still a need to improve the payload and imperceptibility further. Another data hiding approach, employing block partitioning and IWT, is presented in [22] to achieve a high payload. The wavelet transform is applied to both the cover image and the secret message to achieve perfect embedding and high security. The authors claim that the scheme has several parameters that can control the amount of embedding, depending on the requirements, and provides users with the flexibility to increase the payload according to their needs. Chakraborty et al. [23] introduced an LSB-based predictive edge adaptive image steganography. The method enhances imperceptibility and security by embedding secret data only in edge regions of the image. The simulation results demonstrate that the scheme offers low payload and is non-blind. Another data hiding technique in the spatial domain, proposed by Parah et al. [24], generates good stego images and embeds a satisfactory amount of payload. But the scheme may result in increased computational complexity due to the use of interpolation. Moreover, it is required to further improve the payload. The data hiding method based on image resizing and pixel permutation in [25] provides improved image quality, as evidenced by high PSNR values. However, this technique requires further improvements to enhance the payload. [16] proposed a data hiding technique based on hybrid edge detection to maximize the edges suitable for proper data embedding. The method improves both payload and imperceptibility. Although the formula for the Bit Error Rate (BER) is mentioned in the paper, the accuracy of the extracted data is not evaluated in terms of BER for different attacks. Similarly, an image steganography technique based on HOG in [26] employed PVD and LSB methods for data embedding. The results indicate that it provides a reasonably high payload with good image quality. However, while computing HOG for the stego image, the gradient values and, therefore, edges may differ from those of the cover image. This leads to the extraction of erroneous message bits. Furthermore, the scheme does not incorporate a strategy to detect an attack required for data authentication, and it also requires more execution time. A reversible data hiding scheme [2] utilizes the enhanced neighbour mean interpolation (ENMI) method to expand the blocks. The original pixels of the cover image are retained at the corners of each expanded block to maintain reversibility, and the other pixels are used to carry 4-bit secret data and a 1-bit authentication code. As a large number of authentication bits is embedded for authentication purposes, it reduces the amount of secret data embedded in different pixels. The results also demonstrate that the fragility of the scheme is somewhat towards the weaker side in some cases. Another steganography technique, based on a combination of chaos functions and image blocking [3], embeds randomly selected data bits in the pixels of randomly selected blocks

to preserve the confidentiality of sensitive data in the Internet of Things (IOT), and it overcomes the key disclosure problem as the block centers generate the initial key of the chaos function. However, it does not support tamper detection and content authentication. The Dual Image Reversible data hiding techniques [27, 28] are based on Coordinate Vector, Coordinate Vector Directions, and Triangular Order Coding (TOC). These schemes offer a good payload while ensuring better imperceptibility and security; however, they are not capable of detecting tamper caused by various malicious attacks.

The contributions and limitations of the existing state-of-the-art techniques discussed above are summarized in Table 1.

Our proposed HOG based high capacity and blind image steganography technique with tamper detection and content authentication aims to overcome these limitations. The simulation results and different analyses highlight the effectiveness of the proposed approach.

3 Proposed steganographic technique

Our proposed technique involves two main processes — the data embedding process and the data extraction process.

3.1 Data embedding process

The block diagram of the proposed data embedding process is shown in Fig. 1. Here, the cover image is preprocessed prior to embedding, and it can be explained in detail as follows:

3.1.1 Computing HOG feature vector of the cover image

Histogram of Oriented Gradients (HOG) [29, 30] serves as a popular feature descriptor that captures the structural or shape-related characteristics of an object by extracting feature vectors for each block of the cover image based on pixel's gradient magnitudes and directions. The HOG feature vector of the cover image can be computed as follows:

1. The gradients in the x and y directions for each pixel of the cover image are computed using Eq. (1):

$$G_x = C * F_x, \quad G_y = C * F_y \quad (1)$$

where the gradient filters F_x and F_y in the x and y directions, respectively, are given in Eq. (2):

$$F_x = [-1 \quad 0 \quad 1], \quad F_y = [-1 \quad 0 \quad 1]^T \quad (2)$$

Table 1 Work done in various steganographic Techniques

References	Approach/ Technique	Contributions and Limitations
[17]	Data hiding using simple LSB substitution method	Simple to design and easy to implement, but it lacks security and is easily detectable. Exploits OPAP to improve the image quality at a cost of computational complexity.
[18]	Image Steganography using PVD	Enhances security by utilizing adaptive embedding and preserving smooth regions. Embedding more bits in textured regions causes a larger change in pixel values, which may distort and degrade the visual quality of the stego image.
[19]	Steganographic scheme based on PVD and modified EMD	Integrating PVD with EMD enhances security and reduces detectability compared to standard PVD. However, combining PVD with EMD makes the technique computationally more complex.
[20]	Image Steganographic Technique using OPVD	Overlapped PVD significantly enhances the payload and reduces the computational time, but results in low imperceptibility.
[21]	Distortionless Data Hiding Technique based on IWT	Embeds data into the middle bit planes of the coefficients of IWT in the MF and HF subbands. However, there is still a need to further improve the payload and imperceptibility.
[22]	High Payload and Secure Steganography method based on Block Partitioning and IWT	Achieves a fairly good payload as well as imperceptibility. The complexity may be increased as the wavelet transform is applied to both the cover image and the secret message before embedding.
[23]	Predictive edge adaptive LSB Image steganography	Improves security and imperceptibility. Offers low payload as the data is embedded only in edge regions, and the non-blind nature of the scheme limits its feasibility in real-world scenarios.
[24]	Reversible and high capacity data hiding technique for E-healthcare applications	Supports tamper detection and content authentication. Offers a sufficient amount of payload with better imperceptibility. There may be an increase in computational complexity due to the use of interpolation, and further improvements are required to enhance the payload.
[25]	Reversible Steganographic Technique based on image resizing and pixel permutation	Upscales the original image by using simple arithmetic operations to meet the reversibility criterion, and performs embedding using a permutation table. Offers a sufficient payload and improves imperceptibility, but still requires further work to enhance the payload.
[16]	Hiding Data in medical images for e-healthcare applications	Use of Hybrid edge detection, consisting of Canny and Perwitt edge detectors, enhances the payload by maximizing the detected edges while maintaining good imperceptibility. The simulation results are not provided for the security and fragility/robustness analyses.
[26]	Adaptive Image Steganographic Scheme based on HOG and PVD-LSB methods	Exploits HOG to find the dominant edge direction and embeds data using PVD and LSB substitution methods. The scheme achieves a fairly high payload while maintaining better imperceptibility. However, it may extract incorrect message bits when an edge mismatch occurs. The scheme does not employ any tamper detection method, thereby limiting its applications in ensuring the integrity and authenticity of secret data.
[2]	Efficient Data Hiding Strategy with Tamper Detection for Medical Images	Conceals a satisfactory amount of payload while ensuring good imperceptibility. The fragility analysis shows weaker results in some cases, and the authentication bits result in the reduction of the payload.
[3]	Privacy-preserving in the IOT based on steganography and chaotic functions	Effectively conceals the information in the cover image while ensuring a better quality of the images. However, if the data becomes corrupted during transmission, the initial key changes, resulting in the reconstruction of erroneous data bits. The scheme lacks verification of the integrity and authenticity of the confidential data, and without verification, the data is untrustworthy in today's digital world.
[27, 28]	Dual Image Reversible Data Hiding based on Coordinate Vector Directions, Dual Image Reversible Data Hiding Scheme based on Coordinate Vector and TOC	These techniques provide a fair amount of payload while maintaining better imperceptibility and security. However, these techniques do not support any tamper detection strategy. Consequently, the integrity and authenticity of the data cannot be verified.

2. The gradient magnitude and gradient angle of each pixel are calculated by Eq. (3):

$$G_M = \sqrt{(G_x^2 + G_y^2)}, \quad G_\theta = \tan^{-1} \left(\frac{G_y}{G_x} \right) \quad (3)$$

3. The gradient angles of the cover image's pixels, ranging from 0° to 180°, are divided into several orientation bins, and the cell and block sizes are defined.

4. The gradient magnitudes of the cover image's pixels with respect to the bins within a cell are accumulated to generate cell histograms.
5. The cell histograms are concatenated to generate block histograms, and then the magnitudes of the HOG blocks are normalized. 6. Finally, the normalized blocks are concatenated to generate an HOG feature vector of the cover image.

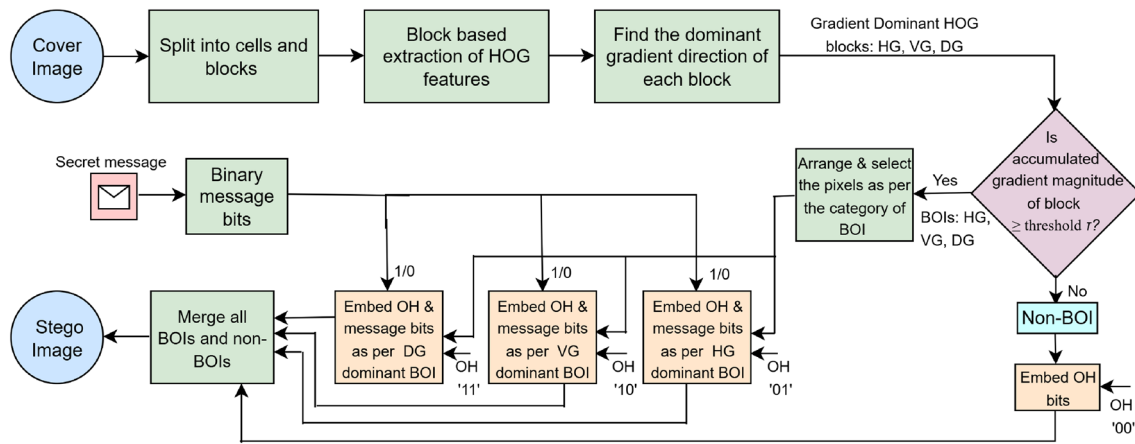


Fig. 1 Block diagram of the Proposed Data Embedding Process

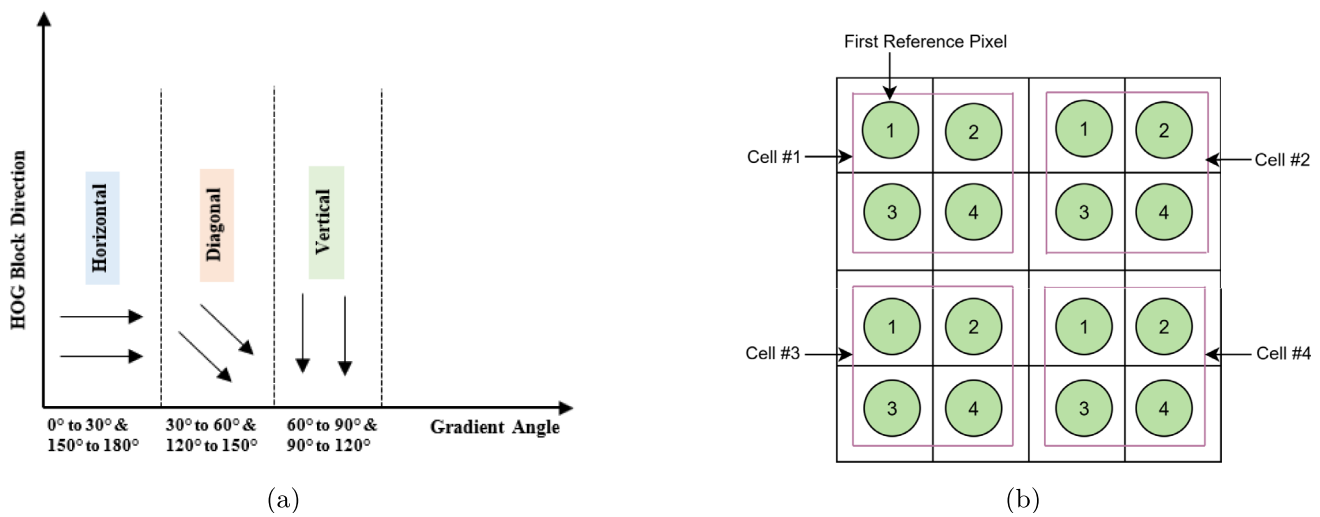


Fig. 2 (a). Direction of HOG blocks w.r.t. Gradient angles (b). Structure of a typical (4×4) HOG block

3.1.2 Finding dominant gradient direction of HOG blocks

The three directions of HOG blocks with respect to the gradient angles are shown in Fig. 2 (a). In the proposed method, the gradient angle (0° to 30°) corresponds to bin1, (30° to 60°) corresponds to bin2, (60° to 90°) to bin3, (90° to 120°) corresponds to bin4, (120° to 150°) to bin5, and (150° to 180°) corresponds to bin6. As a result, bin1 and bin6 determine the horizontal direction, bin2 and bin5 correspond to the diagonal direction, and bin3 and bin4 determine the vertical direction. To compute the dominant gradient direction of each HOG block, the magnitudes of cell histograms with respect to their gradient directions are summed, and the gradient direction corresponding to the highest accumulated magnitude is the dominant gradient direction of an HOG block. Consequently, three types of HOG blocks are obtained, namely, horizontal gradient (HG) dominant HOG blocks, vertical gradient (VG) dominant HOG blocks, and diagonal gradient (DG) dominant HOG blocks.

The structure of an HOG block, having a cell size of (2×2) and a block size of (4×4) , is shown in Fig. 2 (b). Each HOG block comprises 4 cells, and each cell consists of 4 pixels. Thus, there are a total of 16 pixels in each HOG block of the cover image. The reference pixel of the first cell (top left pixel) of each block is assumed to be the *first reference pixel*.

3.1.3 Generation of non-BOIs and BOIs

To generate BOIs, the highest magnitude corresponding to the dominant gradient direction of an HOG block is compared with the threshold value τ . If the magnitude is greater than or equal to τ , then the block is referred to as BOI, and if it is not, then the block is non-BOI. So, the three different categories of BOIs corresponding to the three different types of HOG blocks are generated — HG dominant BOIs, VG dominant BOIs, and DG dominant BOIs.

3.1.4 Embedding in non-BOIs and BOIs

The data embedding for non-BOIs and different categories of BOIs can be explained as follows:

Non-BOIs: Only two overhead bits '00' are embedded in the first reference pixel (top left pixel) of each non-BOI, and no message bits are embedded.

HG Dominant BOIs: Fig. 3 (a) shows the arrangement of 16 pixels (or 4 cells) for the HG dominant BOIs. Among 16 pixels, P_1 , P_3 , P_5 , and P_7 shown in red are selected as reference pixels of each cell. P_2 , P_4 , P_6 , and P_8 shown in green denote the pixels dominating along the horizontal gradient direction in each cell, while the pixels P_9 to P_{16} shown in black are the remaining pixels. Initially, the two overhead bits '01' are embedded in the first reference pixel P_1 of each HG dominant BOI. Then, the $(k+1)$ message bits are embedded in all the reference pixels and in the pixels dominating along the horizontal gradient direction, while the k message bits are embedded in the remaining pixels of the block.

VG Dominant BOIs: Similarly, for the VG dominant BOIs shown in Fig. 3 (b), $(k+1)$ message bits are embedded in all the reference pixels shown in red colour and in the pixels dominating along the vertical gradient direction shown in green colour, while the k message bits are embedded in the remaining pixels (shown in black colour) of the block.

DG Dominant BOIs: In the same way, for the DG dominant BOIs shown in Fig. 3 (c), $(k+1)$ message bits are embedded in all the reference pixels shown in red colour and in the pixels dominating along the diagonal gradient direction shown in green colour, while the k message bits are embedded in the remaining pixels of the block.

After embedding overhead and message bits into all blocks of the cover image, including both BOIs and non-BOIs, all the blocks are merged to generate a stego image.

The proposed data embedding process is summarized in Algorithm 1.

Input: Load Cover Image C of size $(M \times N)$, and Secret message.

- 1: Initialize the values of the embedding parameters τ and k .
- 2: Divide the cover image into cells of dimensions (2×2) and blocks of dimensions (4×4) .
- 3: Extract the HOG feature vectors of the cover image on a block-by-block basis, as explained in section 3.1.1.
- 4: Compute the dominant gradient direction of each HOG block, as explained in section 3.1.2.
- 5: Generate the non-BOIs and different categories of BOIs as explained in section 3.1.3.
- 6: Embed only two overhead bits in the first reference pixel P_1 of all non-BOIs and two overhead bits followed by message bits in all BOIs, as explained in section 3.1.4.
- 7: Embed message at a rate of $(k+1)$ bits in all the reference pixels and in the pixels along the dominant gradient direction, while k bits in the remaining pixels of all BOIs, as explained in section 3.1.4.
- 8: Merge all non-BOIs and BOIs to generate the stego image.

Output: Stego Image S of size $(M \times N)$.

Algorithm 1 Algorithm of the Proposed Data Embedding Process

3.2 Blind data extraction

The proposed technique is a blind image steganography technique, as the message at the receiver can be recovered without requiring access to the cover image [31, 32]. Figure 4 shows the block diagram of the data extraction process. To retrieve the message, the two overhead bits from each block of the stego image are extracted, as shown in Fig. 4. Then, based on the BOI category, the location of the message bits can be determined. The data extraction process is summarized in Algorithm 2.

Fig. 3 Data Embedding (a). HG dominant BOIs (b). VG dominant BOIs (c). DG dominant BOIs

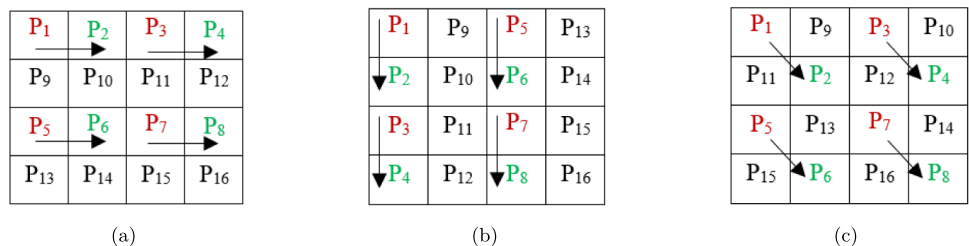
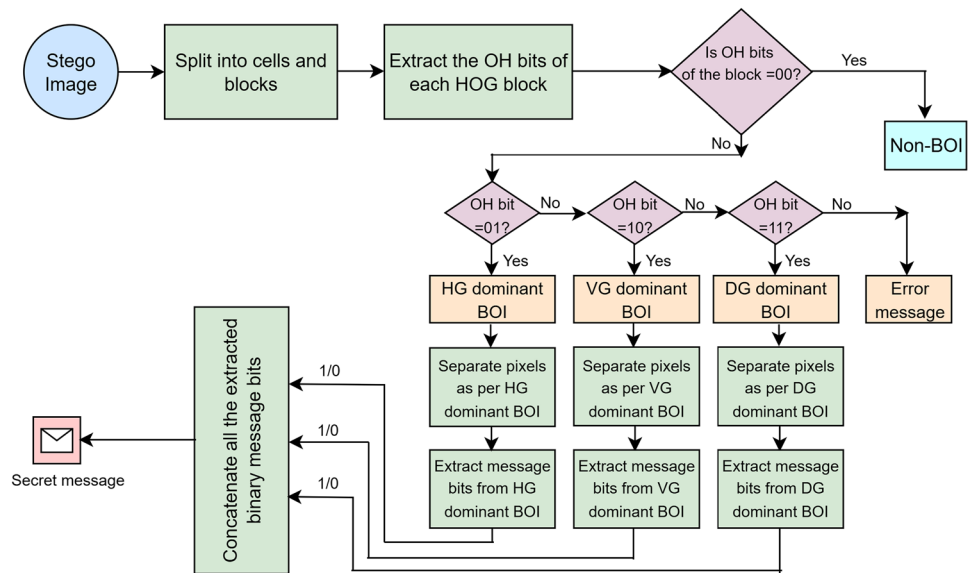


Fig. 4 Block diagram of the Data Extraction process

Cover Images (general)					
	Lena	Baboon	Peppers	Boat	Airplane
Cover Images (medical)					
	Foetus Scan	Brain MRI	Chest X-ray	Facial X-ray	Brain CT Scan

Fig. 5 General and medical cover images

Input: Stego Image S of size $(M \times N)$, values of the embedding parameters, τ and k .

- 1: Divide the stego image into cells of size (2×2) and blocks of size (4×4) .
- 2: Extract the overhead bits from the first two LSBs of the first reference pixel P_1 to determine the type of the block (non-BOI or BOI).
- 3: Separate the reference pixels, the pixels along the dominant gradient direction, and the remaining pixels based on the BOI category.
- 4: Extract the message bits from $(k + 1)$ LSBs of all the reference pixels and the pixels along the dominant gradient direction, while k LSBs of the remaining pixels.
- 5: Repeat steps 2 to 4 for all the blocks of the stego image to recover the full payload.
- 6: Concatenate the extracted message bits to reconstruct the secret message.

Output: Secret message.

Algorithm 2 Algorithm of Blind Data Extraction

4 Simulation results and analyses

The implementation and testing of the proposed scheme have been carried out using the MATLAB R2019b platform. The test images of size (512×512) , retrieved from databases [33, 34], are shown in Fig. 5. The secret message is randomly generated. In this section, various metrics are employed to perform different types of analyses and assess the performance of the proposed technique. These **metrics** are given and discussed below.

Let n_{BI} represent the number of BOIs, τ is the threshold value, and k denotes the number of LSBs replaced with message bits. The two embedding parameters τ and k are jointly defined as an embedding parameter vector $X = [\tau, k]$, and the payload and PSNR are both functions of the vector X .

The **Payload** is also referred to as **Embedding Capacity (EC)**, which denotes the total number of bits embedded, N_T , and for an image at a given τ and k , it can be defined in Eq. (4) as:

$$EC = N_T = (N_m + N_{OH}) \quad (4)$$

where N_m denotes the number of message bits that depends upon vector X , N_{OH} represents the number of overhead bits that is twice of n_{BI} , which in turn depends upon τ .

The EC can also be represented in terms of bits per pixel (bpp), as the ratio of the total number of bits embedded to the total number of cover image pixels, and it is given by Eq. (5) [35]:

$$EC = \frac{N_T}{(M \times N)} \quad (5)$$

The visual quality of the stego image is assessed in terms of PSNR, or Structural Similarity Index Measure (SSIM) [24]. The **PSNR** is defined in Eq. (6) as:

$$PSNR \text{ (dB)} = 10 \log_{10} \frac{(255)^2}{MSE} \quad (6)$$

where **Mean Squared Error (MSE)** is defined in Eq. (7):

$$MSE = \frac{1}{(M \times N)} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} [C(i, j) - S(i, j)]^2 \quad (7)$$

where $(M \times N)$ represents the cover and the stego image's dimensions, $C(i, j)$ and $S(i, j)$ denote the cover and the stego image's pixel intensities, respectively, in the i^{th} column and j^{th} row.

The quality metric **SSIM** is given in Eq. (8) as:

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + C_1) (2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1) (\sigma_x^2 + \sigma_y^2 + C_2)} \quad (8)$$

where $\mu_x, \mu_y, \sigma_x, \sigma_y$, and σ_{xy} represent the means, standard deviations, and cross-covariance for images x and y . c_1 and c_2 are the constants for the luminance and contrast terms and are defined in Eq. (9) as:

$$c_1 = (0.01 \times 255)^2 = 6.5, \quad c_2 = (0.03 \times 255)^2 = 58.5 \quad (9)$$

The performance of the proposed method is evaluated by computing **BER** and **Normalized Cross-Correlation (NCC)** [36] under no attack and under various attack scenarios. The NCC between the cover and the stego images is given by Eq. (10):

$$NCC = \frac{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} [C(i, j)S(i, j)]}{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} [C(i, j)]^2} \quad (10)$$

The bit error rate is calculated between embedded and extracted bits, and it is defined by Eq. (11):

$$BER \text{ (\%)} = \frac{1}{n} \left[\sum_{i=0}^{n-1} d(i) \oplus d^*(i) \right] \times 100 \quad (11)$$

where n represents the total number of bits embedded, d and d^* are the original and extracted bits, respectively.

In addition to computing NCC and BER, the **Number of Blocks Tampered (NBT)** is also determined to evaluate the performance of the proposed method. NBT is calculated by comparing the extracted overhead bits with those of the

embedded overhead bits, and it quantifies the blocks affected by tampering. Therefore, the overhead bits in the proposed method can also be utilized as authentication bits to verify and validate the integrity and authenticity of the secret and confidential data. As NBT represents the number of blocks received in error, it can detect any tampering under diverse attack scenarios to verify the integrity and authenticity of the secret message.

In the following sections, the payload, perceptual quality, authentication, and time complexity are analyzed to evaluate the performance of the proposed technique.

4.1 Payload and Imperceptibility Analysis

The payload and imperceptibility for different test images at the embedding parameter vectors $X = [0.1, 1]$ and $X = [0.1, 2]$, and block size of (2×2) cells or (4×4) pixels are presented in Table 2. The payload includes overhead and message bits.

Fig. 6 (a) compares the proposed method's EC with that of the Lin et al. method [2] at a PSNR of about 45 dB for various test images. The average EC of the proposed method is 416,734 bits, whereas that of [2] is 327,680 bits. Hence, the proposed method's EC is higher by 89,054 bits than [2], indicating that the payload of our technique is enhanced by 27.2% compared to the methods under comparison. Similarly, the graph in Fig. 6 (b) compares the proposed method's PSNR with that of [2] at an EC of 327,680 bits for various test images, which shows that our method achieves higher PSNR for various images compared to [2], and the average PSNR value of the proposed method is 3.4 dB higher than that of [2].

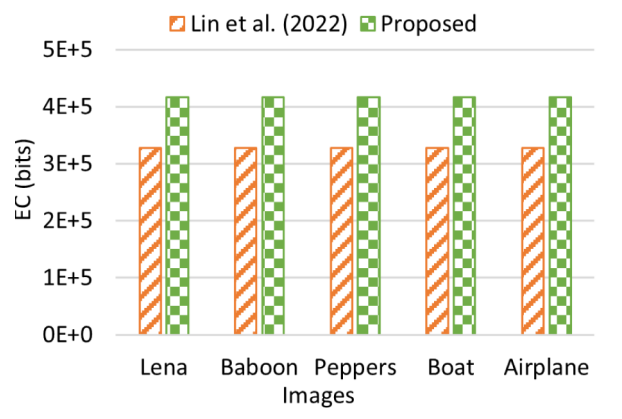
A new performance metric is designed for comparison, taking into account both payload and imperceptibility together. It is defined in Eq. (12):

$$ECPSNR = \frac{(EC \times PSNR)}{(M \times N)} \quad (12)$$

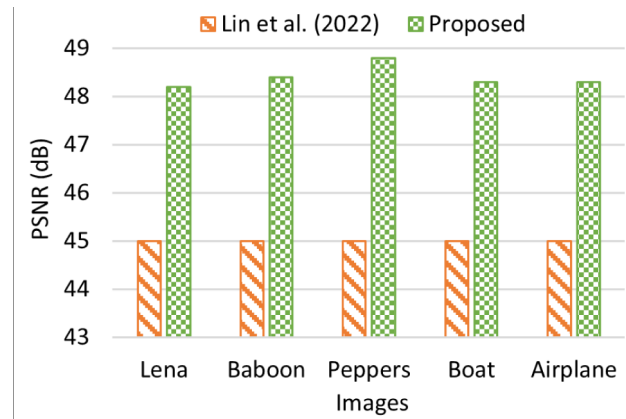
The average ECPSNR of the proposed method and the existing state-of-the-art methods are tabulated and compared in Table 3. As shown in Table 3, the proposed method's average ECPSNR is high compared to the methods under comparison because the message bits are embedded in blocks with a large gradient, while small-gradient blocks are not used for embedding the message. Concealing more message bits in dominant gradient directions results in high EC and improved imperceptibility. As a result, the high EC of the proposed method, coupled with the good imperceptibility, outperforms the state-of-the-art approaches.

Table 2 Payload and Imperceptibility

Cover Images (512 × 512)	Number of BOIs	$(\tau=0.1, k=1)$			$(\tau=0.1, k=2)$		
		Payload (bits)	PSNR (dB)	SSIM	Payload (bits)	PSNR (dB)	SSIM
Lena	16,384	425,984	43.12	0.9864	688,128	36.87	0.8893
Baboon	16,384	425,984	43.24	0.9845	688,128	36.97	0.8924
Peppers	16,370	425,648	43.99	0.9855	687,568	36.94	0.8953
Boat	16,384	425,984	43.28	0.9847	688,128	36.17	0.8927
Airplane	16,384	425,984	43.15	0.9848	688,128	36.96	0.8948
Foetus Scan	16,375	425,768	44.06	0.9865	687,768	37.03	0.8965
Brain MRI	16,360	425,408	43.99	0.9894	687,168	36.98	0.8919
Chest X-ray	16,382	425,936	43.98	0.9888	688,048	37.09	0.8988
Facial X-ray	16,380	425,888	44.08	0.9876	687,968	37.58	0.8996
Brain CT Scan	16,365	425,528	43.99	0.9858	687,368	36.95	0.8949



(a)



(b)

Fig. 6 Performance comparison with Lin et al. method (a). Capacity comparison (b). PSNR comparison.**Table 3** Capacity and PSNR comparison with existing schemes

Scheme	Lena		Baboon		Average ECPSNR
	EC (bits)	PSNR (dB)	EC (bits)	PSNR (dB)	
[2]	327,680	45.41	327,680	45.41	56.76
[3]	393,216	45.89	393,216	45.86	68.81
[16]	218,680	36.83	238,026	30.43	29.18
[18]	409,752	41.71	417,168	39.14	63.74
[19]	402,485	41.46	413,472	38.88	62.49
[21]	85,507	36.64	14,916	32.76	6.905
[22]	400,000	40.54	400,000	38.07	59.97
[24]	196,608	46.36	196,608	46.37	34.77
[25]	262,144	44.16	262,144	44.15	44.16
[26]	390,654	41.59	393,204	41.68	62.25
[27]	393,216	44.04	393,216	44.04	66.06
[28]	—	—	393,216	46.46	69.69
Proposed	425,984	43.12	425,984	43.24	70.17

4.2 Authentication analysis

The authentication analysis evaluates the fragility of the proposed technique in terms of performance metrics, including NCC, NBT, and BER, which in turn verifies and validates the integrity and authenticity of the confidential data.

Table 4 demonstrates that when the stego images are not subjected to any attack, NCC approximately approaches unity, indicating that the stego images are almost identical to the cover images. A zero NBT indicates that all blocks have been received without any errors, and it signifies that stego images have not been tampered, altered, or degraded. A zero BER coupled with zero NBT indicates that the extracted and embedded message bits are exactly the same, confirming perfect data recovery and ensuring both content integrity and authentication.

The fragility of the proposed approach is tested in the presence of various attack scenarios for different test images, and the NCC, NBT, and BER values obtained under the influence of these attacks are presented in Table 5 for

Table 4 Stego images and performance metrics under no attacks

Stego Images						
NCC	0.9991	0.9990	0.9995	0.9996	0.9996	0.9995
NBT	0	0	0	0	0	0
BER (%)	0	0	0	0	0	0

Table 5 Stego images and performance metrics under various attacks

Attacked Images				
	S&P noise ($d=0.1$)	AWGN ($\text{var}=0.02$)	LPF (3×3)	MF (3×3)
NCC	0.7078	0.8819	0.8804	0.8978
NBT	1361	12234	12400	11642
BER (%)	7.01	50.01	50.06	44.70
Attacked Images				
	Sharpening	Histogram Equalization	Rotation	JPEG Compression
NCC	0.8940	0.8911	0.4567	0.8982
NBT	12265	11857	12359	12348
BER (%)	49.94	50.16	50.12	49.74

the standard image Lena only. The low NCC and high BER values reflect that the proposed scheme is highly fragile. Furthermore, the high NBT and BER values represent that the proposed method can effectively detect tamper caused by different types of attacks. These values also indicate that the stego images have been tampered, the integrity of the content has been compromised, and the data is no longer authentic. Thus, our method is capable of detecting the tamper and authenticating the content for all attacks applied to stego images.

The performance metrics summarized in Table 5 show that the NBT varies from 8.3% to 75.7%, and the BER of the recovered message varies from 7.01% to 50.16%, respectively, when the stego images are exposed to various image processing and geometrical attacks. The high NBT of 75.7% and high BER of 50.16% of the proposed method, compared to 52.2% NBT and 29.8% BER of the Lin et al. method [2], indicate that the proposed method is highly fragile and can detect tamper even for slight alterations in the stego image. Therefore, the proposed method has a higher tamper detection capability than [2], and hence can detect tamper more accurately, effectively verify, and validate the integrity and authenticity of secret and confidential data.

4.3 Timing analysis

The proposed method's average embedding and extraction times at an embedding parameter vector $X = [0.1, 1]$ have been computed and compared with those of state-of-the-art techniques in Table 6.

Table 6 demonstrates that the proposed method achieves lower embedding and extraction times than the methods under comparison, indicating its computational efficiency.

5 Conclusion and future scope

In this paper, an HOG based blind image steganography technique with high Capacity and tamper detection & content authentication capabilities is proposed. Firstly, the HOG feature vector for each block of the cover image is computed. Then, the dominant gradient direction of each HOG block is determined, and the BOIs are selected by thresholding the gradient magnitude corresponding to the dominant gradient direction. Consequently, the three categories of BOIs are obtained, and the message embedding in the BOIs is performed at a rate of $(k + 1)$ bits in the pixels along the dominant gradient direction, while k bits in the remaining pixels. The payload, perceptual quality, authentication, and time complexity analyses have been performed, and the simulation results show that our proposed method provides improvements of up to 27.2% in payload and up to 3.4 dB in PSNR compared to state-of-the-art methods. The proposed method was also tested for various types of attacks. Authentication analysis confirms that the proposed method exhibits high fragility to almost all attacks, as the NBT reaches up to 75.7% and the BER reaches up to 50%. Therefore, our method provides better tamper detection performance compared to state-of-the-art methods, resulting in more accurate tamper detection and content authentication against all types of attacks. Furthermore, the proposed scheme offers low computational complexity, resulting in improvements of up to 0.7 s in embedding time and 0.2 s in extraction time, respectively. Thus, the proposed scheme is well-suited for secure and confidential communication applications.

For future work, the proposed scheme may be extended and tested on color images to further increase the payload while maximizing imperceptibility. The secret message can be scrambled using efficient encryption techniques to provide double layer security. The proposed steganography technique can be integrated with deep learning to automatically learn and extract features for embedding, thereby

Table 6 Computational Time comparison

Scheme	Embedding	Extraction
	time (secs)	time (secs)
[16]	3.0	—
[18]	2.3	1.4
[19]	3.5	2.1
[20]	2.9	2.0
[26]	2.5	2.0
Proposed	1.6	1.2

providing an automated system with reduced human intervention. Moreover, the steganography technique can be developed in the frequency domain, such as exploiting the dual-tree complex wavelet transform (DTCWT) to increase security and payload, as it provides more subbands or wavelet coefficients for embedding message bits.

Acknowledgements We thank the anonymous reviewer for his valuable suggestions, which significantly improved the clarity of this article.

Declarations

Conflict of interest The authors have no Conflict of interest to declare that are relevant to the content of this article.

References

- Nisha C, Monoth T (2024) A novel approach for the enhancement of payload capacity in pixel value differencing image steganography schemes. *Int J Inf Technol* 16(8):4779–4786
- Lin C-C, Chang C-C, Kao W-J, Chang J-F (2022) Efficient electronic patient information hiding scheme with tamper detection function for medical images. *IEEE Access* 10:18470–18485
- Rostam HE, Motameni H, Enayatifar R (2022) Privacy-preserving in the internet of things based on steganography and chaotic functions. *Optik* 258:168864
- Geetha R, Geetha S (2020) Efficient high capacity technique to embed epr information and to detect tampering in medical images. *J Medical Eng Technol* 44:55–68
- Kumar SN, Kannadhasan S, Miriam LRJ, Fred AL, Haridhas AK, Jane C (2024) Tchebichef moments and bat optimization algorithm-based information hiding and authentication of medical gray level images. *Int J Inf Technol* 16:207–219
- Roselinkiruba R, Sharmila TS (2023) Dynamic optimal pixel block selection data hiding approach using bit plane and image encryption. *Int J Inf Technol* 15(7):3441–3448
- Roselinkiruba R, Sharmila TS (2021) Performance evaluation of encryption algorithm using fruit fly optimization improved hybridized seeker and pvd algorithm. *Int J Inf Technol* 13(5):1797–1803
- Tavakoli A, Honjani Z, Sajedi H (2023) Convolutional neural network-based image watermarking using discrete wavelet transform. *Int J Inf Technol* 15:2021–2029
- Kumar N, Soni M (2025) Randomized salt lsb: a novel approach to steganography with improved concealment and robustness. *International Journal of Information Technology*, 1–14
- Panigrahi R, Padhy N (2025) An effective steganographic technique for hiding the image data using the lsb technique. *Cyber Secur Appl* 3:100069
- Xiang T, Hu J, Sun J (2015) Outsourcing chaotic selective image encryption to the cloud with steganography. *Digital Signal Proc* 43:28–37
- Ansari IR, Hurrah NN, Khan MA, Khan E (2024) Analyzing the effect of psychovisual thresholding of dct coefficients for improved robustness of a blind watermarking technique. In: 2024 3rd Edition of IEEE Delhi Section Flagship Conference (DEL-CON), pp. 1–7. IEEE
- Ansari IR, Hurrah NN, Khan MA, Khan E (2023) High capacity and reversible steganographic technique with authentication capability. In: *International Conference on Computer Vision and Image Processing*, pp. 337–349. Springer
- Parah SA, Sheikh JA, Akhoun JA, Loan NA, Bhat GM (2018) Information hiding in edges: a high capacity information hiding technique using hybrid edge detection. *Multimed Tools and Appl* 77(1):185–207
- Atta R, Ghanbari M, IEEE LF (2021) A high payload data hiding scheme based on dual tree complex wavelet transform. *Optik* 226:165786
- Loan NA, Parah SA, Sheikh JA, Akhoun JA, Bhat GM (2017) Hiding electronic patient record (epr) in medical images: a high capacity and computationally efficient technique for e-healthcare applications. *J Biomed Inform* 73:125–136
- Chan C-K, Cheng L-M (2004) Hiding data in images by simple lsb substitution. *Pattern Recogn* 37:469–474
- Wu D-C, Tsai W-H (2003) A steganographic method for images by pixel-value differencing. *Pattern Recogn Lett* 24:1613–1626
- Shen S-Y, Huang L-H (2015) A data hiding scheme using pixel value differencing and improving exploiting modification directions. *Comput Secur* 48:131–141
- Sahu AK, Swain G (2018) Pixel overlapping image steganography using pvd and modulus function. *3D Research* 9(3):40
- Xuan G, Zhu J, Chen J, Shi YQ, Ni Z, Su W (2002) Distortionless data hiding based on integer wavelet transform. *Electron Lett* 38:1646–1648
- Seyyedi SA, Ivanov NN (2014) High payload and secure steganography method based on block partitioning and integer wavelet transform. *Int J Secur Its Appl* 8:183–194
- Chakraborty S, Jalal AS, Bhatnagar C (2017) Lsb based non blind predictive edge adaptive image steganography. *Multimed Tools and Appl* 76:7973–7987
- Parah SA, Ahad F, Sheikh JA, Loan NA, Bhat GM (2017) A new reversible and high capacity data hiding technique for e-healthcare applications. *Multimed Tools and Appl* 76:3943–3975
- Loan NA, Hurrah NN, Parah SA, Sheikh JA (2017) High capacity reversible stenographic technique based on image resizing and pixel permutation. In: 2017 Fourth International Conference on Image Information Processing (ICIIP), pp. 1–6 (2017). IEEE
- Hameed MA, Hassaballah M, Aly S, Awad AI (2019) An adaptive image steganography method based on histogram of oriented gradient and pvd-lsb techniques. *IEEE Access* 7:185189–185204
- Lee CF, Chan KC (2023) Dual image reversible data hiding based on coordinate vector directions via communication networking. In: *Proceedings of the 2023 8th International Conference on Cloud Computing and Internet of Things*, pp. 10–16
- Lee C-F, Chan K-C (2024) A novel dual image reversible data hiding scheme based on vector coordinate with triangular order coding. *IEEE Access* 12:90794–90814
- Dalal N, Triggs B (2005) Histograms of oriented gradients for human detection. In: 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05) 1:886–893
- Basa B (2015) Implementation of hog edge detection algorithm on fpga's. *Procedia Soc Behav Sci* 174:1567–1575

31. Mohammed AO, Hussein HI, Mstafa RJ, Abdulazeez AM (2023) A blind and robust color image watermarking scheme based on dct and dwt domains. *Multimed Tools and Appl* 82(21):32855–32881
32. Wang Z, Byrnes O, Wang H, Sun R, Ma C, Chen H, Wu Q, Xue M (2023) Data hiding with deep learning: a survey unifying digital watermarking and steganography. *IEEE Trans on Comput Social Syst* 10:2985–2999
33. USC-SIPI Image Database from University of South California. (1977). <https://sipi.usc.edu/database/>
34. OPENi medical image database from National Laboratory of Medicine (2022). <https://openi.nlm.nih.gov/>
35. Atta R, Ghanbari M (2018) A high payload steganography mechanism based on wavelet packet transformation and neutrosophic set. *J Vis Commun Image Represent* 53:42–54
36. Parah SA, Ahad F, Sheikh JA, Bhat GM (2017) Hiding clinical information in medical images: a new high capacity and reversible data hiding technique. *J Biomed Inform* 66:214–230

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.