An Image Steganography Algorithm Based on PSO and IWT for Underwater Acoustic Communication

WENJIN WANG and QINGZHONG LI

1School of Management Science and Engineering, Shandong University of Finance and Economics, Jinan 250014, China
2College of Engineering, Ocean University of China, Qingdao 266100, China

Corresponding author: Wenjin Wang (shuzidianlu@126.com)

This work was supported in part by the National Key Research and Development Program under Grant 2017YFC1405202.

ABSTRACT

To achieve fast and secure information steganography in underwater acoustic channel scenarios, this paper proposes a PSO (Particle Swarm Optimization) and IWT (integer wavelet transform) based image steganography algorithm for underwater acoustic communication. Firstly, the underwater image to be embedded is interleaved and packed to generate the secret information code-stream to improve the detection and recovery performance of transmission errors. Secondly, the cover image is divided into non-overlapping blocks and IWT is applied to each block, which can save PSO search space and improve the optimal solution performance. Thirdly, the embedding position matrix of the high frequency sub-band coefficients is chaotic scrambled, and PSO is used to select the optimal key to obtain the optimal matching position for the secret information to produce the best stego-image quality. Finally, transmission error detection and recovery measures are applied to the extracted secret information to improve the reconstruction quality in underwater acoustic channel scenarios. Experimental results show that the proposed algorithm outperforms existing approaches in terms of information embedding capacity and steganographic visual quality, meeting the requirements of safety and real-time performance of underwater communication. Moreover, it also has the ability of error detection and recovery for harsh underwater acoustic channel.

INDEX TERMS

Image steganography, integer wavelet transform, particle swarm optimization, underwater acoustic communication.

I. INTRODUCTION

Underwater acoustic channel is the only channel for wireless transmission of underwater information and is characterized by a narrow bandwidth and high bit error rate. Image information is one of the main pieces of information used by underwater robots for deep-sea close observation operations. However, how to transmit the observed image information to the surface workstation quickly and covertly through the hydro-acoustic channel is one of the obstacles for deep sea observation of underwater robots.

Digital image steganography embeds information into the cover image, thereby increasing the covert and secure level of communication. Image steganography methods can be divided into two main categories: spatial domain-based image steganography methods and transform domain-based image steganography methods.

In spatial domain-based image steganography methods, secret information is embedded directly into the pixel values of the cover image. Spatial domain data hiding methods are mainly classified into LSB (Least Significant Bit) substitution based methods, PVD (Pixel Value Difference) methods, QIM (Quantized Index Modulation) based methods and LSB matching based methods. Among this class of steganography methods, LSB replacement is the most commonly used method. In this method, in order to hide the secret information in the cover image, the least significant bit of the pixel value of the cover image is directly replaced with the secret...
information bit, thus generating a stego image, and repre-
representative studies in this regard are as follows. Reference [1]
plied an ant colony optimization algorithm to construct an
optimal LSB substitution matrix, which effectively improved
the quality of stego images. Reference [2] proposes a genetic
algorithm to hide important information in the rightmost k
LSBs of the cover image, which has the disadvantage of being
computationally intensive. The PVD-based approach identi-
ifies the bits to be embedded in the cover image by computing
the differences between consecutive pixels. Reference [3]
divides the cover image into non-overlapping blocks of two
consecutive pixels and uses the difference between the two
pixel gray scale values as features to cluster the blocks into
many categories based on smoothness and contrast attributes,
allowing different amounts of information to be embedded
into different categories based on smoothness or contrast.
This method is more covert than the simple least signifi-
cant bit replacement method. A pixel pair LSB matching
method based on double steganography and with reversibility
is proposed in [4]. Although this type of method has less
computational effort, the quality of the stego image degrades
severely when the amount of embedded secret information
increases, and the security is poor, meaning that it is not
resistant to steganalysis attacks. Based on amplifying channel
modification probabilities [5] presented a channel-dependent
payload partition approach among RGB channels taking into
account inter-channel correlations. Reference [6] designed
payload distribution strategies based on image texture com-
plexity and distortion distribution. The proposed distribution
strategy can achieve better security performance. Reference
[7] uses channel attention mechanisms based on generative
adversarial networks to embed secret messages in spatial
domain. Moreover [8] suggests an adaptive steganography
algorithm that employs syndrome trellis codes to maintain a
high-dimensional statistical model of the image, thus signifi-
cantly improving the performance of steganography-resistant
analysis of stego images.

In transform domain-based image steganography methods,
secret information is embedded in the transform coefficients
of the cover image. The transform domain based informa-
tion hiding method overcomes the disadvantages of poor
steganography and security that exist in spatial domain tech-
niques. Commonly used transform domain methods include
DFT (Discrete Fourier Transform) based methods, DCT (Dis-
crete Cosine Transform) based methods, DWT (Discrete
Wavelet Transform) based methods, IWT (Integer Wavelet
Transform) based methods, and so forth. Currently, DWT
based image steganography algorithms are commonly used.
Representative studies based on DWT methods are as follows.
Reference [9] extracts the maximum tolerable variability of
each DWT coefficient based on HVS (Human Visual Sys-
tem) and selects the coefficients with the maximum tolerable
variability for secret information embedding. The embedding
capacity of this method is low and there is a certain degree
of distortion. Reference [10] processes the lowest bits of
DWT neighbouring coefficients with XOR logic functions
and employs a genetic algorithm to select among the XOR
results so that the resulting stego image has minimal variation
with respect to the cover image. This method has a small
amount of embedding and a large time expense. Reference
[11] proposes an embedding algorithm based on a diamond
encoding (DE) scheme in the wavelet domain, which per-
forms embedding in the LL sub-band with low embedding
amount. As the output of a DWT transformation is a floating
point number, and as truncation is required during the data
embedding process, data extraction is often accompanied by
errors. Therefore, IWT solves this problem by mapping an
integer data set to another integer data set. Representative
studies in this area are listed below. Reference [12] applies the
PVD method to embed data in pairs in wavelet coefficients,
which has a lower steganographic quality than the PVD-
based spatial domain method and lacks security testing of the
algorithm. Reference [13] used a steganographic embedding
method based on edge recognition and heterogeneous encod-
ing with low embedding capacity. Reference [14] classifies
edge coefficients based on MSB to determine the amount
of embeddable secret information, and this approach lacks
security detection. Reference [15] utilizes the PSO (Particle
Swarm Optimization) method to find the optimal substi-
tution matrix for secret information, which lacks attention
to the location of the message embedding and is poorly
secured. Reference [16] utilizes a genetic algorithm to select
high frequency coefficients suitable for embedding secret
information and determine the order of embedding so that
the generated stego images have the highest PSNR (Peak
Signal to Noise Ratio). Compared with existing methods,
this method can produce higher quality stego images and is
secure against steganalysis attacks. However, the method is
less real-time, with an embedding time of 20 minutes for a
512 × 512 grayscale image when embedding 192K bits.

In short, the transform domain steganography method has
better performance than the spatial domain method. Among
the transform domain methods, the IWT (Integer Wavelet
Transform) based image steganography algorithm has the
best prospect of application. However, the current IWT-based
image steganography algorithm still has the following three
problems. At first, the embedding capacity of secret infor-
mation is low as well as the poor visual quality of stego
images. Secondly, the bit error rate of the underwater acoustic
channel is high, while the current algorithm does not have
the transmission error detection and recovery capabilities.
Finally, underwater acoustic communication systems are gen-
ernally embedded computer systems with limited computing
power, while current image steganography algorithms are too
computationally complex to meet the requirements of real-
time computation and transmission of underwater acoustic
channels.

To overcome the above problems, this paper proposes an
image steganography algorithm for underwater acoustic
communication based on integer wavelet transform (IWT) and
particle swarm optimization (PSO). Firstly, the underwater
secret image to be embedded is generated using interleaved
packing method to generate the secret information code stream to improve the transmission error detection and recovery capability. Next, the cover image is chunked and IWT is performed. Subsequently, the embedding position matrix of high-frequency sub-band coefficients is chaotically disordered and PSO is used to select the optimal key and obtain the optimal matching position of the secret information to produce the best quality stego image. In the process of secret information extraction, transmission error detection and recovery measures are used to ensure a good reconstruction of the underwater secret images. Finally, the proposed algorithm is tested and validated using standard test images.

II. GENERAL FRAMEWORK OF THE ALGORITHM
The overall block diagram of the algorithm is shown in Fig. 1 and consists of four modules. The functions of each module are described below.

A. UNDERWATER SECRET IMAGE INTERWEAVING AND PACKAGING PROCESS
The process performs a first order integer wavelet transform on the input secret underwater image, followed by a rational segmentation, interleaving and packing to transform it into a secret information code stream.

B. SECRET INFORMATION EMBEDDING PROCESS
The cover image is first divided into non-overlapping sub-blocks and an integer wavelet transform is applied to each sub-block separately. Then, for each sub-band of that sub-block, a particle swarm optimization algorithm is used to find the optimal embedding position matrix, obtaining the key and performing the data embedding. After the data embedding is completed in a sub-block, a inverse wavelet transform is performed on it and placed in the corresponding block in the stego image. After all sub-blocks have completed embedding, the stego image is generated.

C. SECRET INFORMATION EXTRACTION
After transmission over the hydro-acoustic channel, the receiver receives a stego image disturbed by transmission errors, and then the stego image is extracted for secret information. The stego image is first divided into non-overlapping sub-blocks and the inverse wavelet transform is applied to the sub-blocks. By using a raster scan sequence, the scrambled secret information code stream is extracted from the high frequency sub-band coefficients. The key is used to calculate the embedding position matrix and the scrambled secret information code stream is converted into the original secret information code stream. Finally, the original secret information of all sub-blocks is combined to reconstruct the embedding data disturbed by transmission errors.

D. TRANSMISSION ERROR DETECTION AND RECOVERY
After reconstructing the embedded data disturbed by transmission errors, the receiver detects packet loss errors and takes different transmission error recovery measures for low-frequency and high-frequency data, outputting the error-fixed underwater image.

The specific implementation of each module is described below.

III. UNDERWATER SECRET IMAGE INTERWEAVING AND PACKAGING PROCESS
In order to effectively prevent the spread of channel errors and facilitate the recovery of erroneous data, the underwater secret image data to be embedded must be reasonably segmented, interleaved and packed. Firstly, a first order integer wavelet transform is applied to the underwater images, specifying that the data in each packet consists of the following four components: the low frequency sub-band LL coefficients, the high frequency sub-bands LH, HL, and HH coefficients. The segmentation and interleaving strategies for each of these parts are specified below.

Fig. 2 shows the interleaved packetisation of the underwater image high and low frequency data from underwater secret images.
serial number of the packet to which the data belongs at that location. Scan the coefficients sequentially and split it into K packets, see Fig.2 for an illustration of the splitting of the top left sub-band. The initial scanning position of the LL sub-band is shifted to the right by 1, 2 and 3 × 1 columns to obtain the segmented packet form for all coefficients in the HL, LH and HH sub-bands respectively. As can be seen from the above split packing process, the packing method in this paper divides adjacent low-frequency coefficients into different packets, which can facilitate the interpolation recovery of errors. In addition, each low-frequency coefficient and its corresponding high-frequency coefficients in three directions are distributed in four different packets. When a certain low-frequency coefficient is lost, it can be reconstructed approximately by using the method described below, guided by the high-frequency coefficients in other packets. When the high frequency coefficients in one direction are lost, the high frequency coefficients in the other two directions are still present in the other two packets, thus greatly reducing the extent of damage to image quality from errors.

![FIGURE 3. Contents of the data package.](image)

The data composition of each packet is shown in Fig.3. Data to be embedded includes the low frequency sub-band data and the high frequency sub-band data of the underwater image, all of which are stored first with \( Num \) being the fixed-length encoding of the packet number. Since the number of coefficients in each packet is determined, it is sufficient to store the fixed-length code for each coefficient directly after assigning a separate sign bit to the high-frequency coefficients, without recording their number of coding bits. The advantage of using fixed-length coding is that it effectively prevents the spread of error codes and facilitates the recovery of errors in important low-frequency coefficients.

After the underwater image has been pre-processed, it is converted into a secret information code stream, which allows the following secret information embedding process to be carried out.

### IV. INFORMATION EMBEDDING PROCESS

For images of size Height × Width, the HH sub-band is sufficient to embed the data if the data length is less than \(((\text{Height} \times \text{Width})/4)\). Otherwise, the rest of the data must be distributed among the other sub-bands (HL and LH). The algorithm first divides the cover image into non-overlapping sub-blocks and performs an integer wavelet transform on each sub-block separately. Then, for each sub-band of the sub-block, a particle swarm optimization algorithm is used to find the optimal embedding location matrix and perform data embedding. After the data embedding is completed in a sub-block, a reverse wavelet transform is applied to it and placed in the corresponding block in the stego image.

The following section describes the implementation details of the three steps of integer wavelet transform of the \( m \)-th sub-block, obtaining the optimal embedding location matrix using the particle swarm optimization algorithm and data embedding, assuming that the HH sub-band space is sufficient for embedding the data.

#### A. INTEGER WAVELET TRANSFORM

In order to solve the problem of loss of secret information due to truncation of floating point values caused by the use of DWT, this paper adopts the integer wavelet transform scheme. The integer wavelet transform is performed employs a lifting scheme that has simple truncation and does not affect reversibility [17]. The Daub5/3 wavelet lifting transform is a reversible integer transform. Only one prediction and update process is needed to complete the transform. It has excellent feature of completely reconstructing the original signal, so it is often used in lossless image compression encoding. The intermediate data of the wavelet transform are integers, thus avoiding the problem of loss of secret information due to truncation of floating point values.

Its forward transformation formula is:

\[
\begin{align*}
d_{i+1,l} & = s_{i,2l+1} - \frac{s_{i,2l} + s_{i,2l+2}}{2} + 0.5 \\
s_{i+1,l} & = s_{i,2l} + \frac{d_{i+1,l-1} + d_{i+1,l}}{4} + 0.5
\end{align*}
\]  \tag{1}

The corresponding inversion equation is:

\[
\begin{align*}
s_{i,2l} & = s_{i+1,l} - \frac{d_{i+1,l-1} + d_{i+1,l}}{4} + 0.5 \\
d_{i,2l+1} & = d_{i+1,l} - \frac{s_{i,2l} + s_{i,2l+2}}{4} + 0.5
\end{align*}
\]  \tag{2}

The advantages of the Daub 5/3 wavelet are as follows. Firstly, it is a fast computation, as the calculation of the forward and backward transforms can be achieved by integer addition and shifting alone. Secondly, the memory requirements are low, as the coefficients of the wavelet transform can be stored in short data (2 bytes). All these features facilitate its implementation in hardware.

#### B. PSO-BASED EMBEDDING POSITION MATRIX SELECTION

1) DESCRIPTION OF THE PSO ALGORITHM

The Particle Swarm Optimization (PSO) algorithm was proposed by Kennedy and Eberhart [18]. It is a Swarm Intelligence-based optimization method that simulates the behaviour of a flock of birds foraging for food, where the birds collaborate collectively to achieve the optimal purpose of the flock. The advantages of PSO are its simplicity, ease of implementation and deep intelligence background, which makes it suitable for both scientific research and engineering applications, without many parameters to be adjusted.
2) PARAMETER SETTING FOR THE ALGORITHM
Suppose that there are \( N \) particles in \( d \)-dimensional space. The position of particle \( i \) is \( X_i = (x_{i1}, x_{i2}, \ldots, x_{id}) \). The velocity of particle \( i \) is \( V_i = (v_{i1}, v_{i2}, \ldots, v_{id}) \). Then the particle velocity and position update equations are as follows.

\[
V_i(t + 1) = w \times V_i(t) + c_1 \times r_1 \times (pbest_i - X_i(t)) + c_2 \times r_2 \times (gbest - X_i) \tag{3}
\]

\[
X_i(t + 1) = X_i(t + 1) + V_i(t + 1) \tag{4}
\]

\( pbest_i \) denotes the individual pole position of particle \( i \). \( gbest \) denotes the global pole position of the population. \( c_1 \) and \( c_2 \) are learning factors that regulate the maximum step size of learning. \( r_1 \) and \( r_2 \) are two random numbers that take values in the range \((0,1)\) to increase the search randomness. \( w \) is an inertia factor that regulates the search range of the space.

3) PROCESS OF THE ALGORITHM
The processes of the PSO algorithm are as follows.

Step 1: Initialization
The population is initialized to find the initial position and velocity of each particle in a random way.

Step 2: Evaluation
The fitness value of the particle is calculated from the fitness function.

Step 2.1: Find the Pbest
Find the optimal solution \( pbest_i \) for each particle so far in the search process.

Step 2.2: Find the Gbest
Find the best global solution \( gbest \) for all particles searched so far.

Step 3: Update the Velocity
The velocity and position of each particle is updated according to (3) and (4).

Step 4: Iteration
Go back to Step 2 and continue until a satisfactory result is obtained or the termination condition is satisfied.

The inertia factor of particle swarm optimization algorithms usually takes a fixed value, which tends to cause the algorithm to fall into a local optimum solution during the search. To address this problem, this paper introduces the concept of linearly decreasing inertia weights when the PSO method is used to find the optimal embedding position matrix in the next section.

4) FINDING THE OPTIMAL EMBEDDING POSITION MATRIX USING PSO
In this section, the formation of the embedding location matrix will be discussed through the PSO algorithm. The algorithm consists of five distinct steps. A detailed description of these steps is given below.

Step 1: Initialization
Assume that the total number of particles in a population is \( N \). According to the definition of the key in Step 2, the dimension of each particle is 2, representing keys \( k \) and \( n \). The random generation interval of the initial position of each particle depends on the range of values of \( k \) and \( n \). The random generation interval of the initial velocity takes 10-20\% of the size of the position interval. The individual extreme point of the particle is set to \( pbest_i = X_i \). The global extreme point of the population is set to \( gbest = 0 \).

The inertia factor \( w \) reflects the ability of a particle to inherit previous velocities. Experience shows that a larger inertia weight is beneficial for global search, while a smaller inertia weight is more favorable for local search. In order to better balance the global search capability of the algorithm with the local search ability, a linearly decreasing inertia weight is used in this paper, with the following equation:

\[
w(k) = (w_{start} - w_{end}) \times (T_{max} - k)/T_{max} + w_{end} \tag{5}
\]

where \( w_{start} \) is the initial inertia weight, \( w_{end} \) is the inertia weight at the maximum number of iterations; \( k \) is the current number of iterations, and \( T_{max} \) is the maximum number of iterations. In general the algorithm performs best at \( w_{start} = 0.9 \) and \( w_{end} = 0.4 \). Thus, the inertia weight decreases from 0.9 to 0.4 as the iterations progress, and the larger inertia weight at the beginning of the iteration keeps the algorithm with a strong global search capability. The smaller inertia weights at the end of the iteration allow the algorithm to perform a more accurate local search.

Step 2: Fitness function evaluation
The less modification to the cover image during the information steganography process, the better the quality of the final stego image generated. Therefore, our target is to minimize the difference between the embedded information bits and the lowest significant bits of the cover image, that is, to maximize the number of matching bits. The embedding position matrix of each sub-block of high frequency sub-band coefficients corresponds to a different value of matching bits and therefore produces a different stego image. Hence, in order to evaluate the fitness function, we first generate the embedding position matrix for the high-frequency sub-band coefficients of each sub-block.

The original position matrix of the sub-block high frequency sub-band coefficients is operated by position displacement to obtain the embedded position matrix. The spatial position permutation algorithm used in this paper is an extended formulation of the Baker transform of a two-dimensional chaotic mapping, and (6) gives the transformation formula with the mapping interval \( A : U \rightarrow U, U \subset [0, l] \times [0, l] \).

\[
\begin{bmatrix}
X_{n+1} \\
Y_{n+1}
\end{bmatrix} = \begin{bmatrix}
1 & 1 \\
k & k + 1
\end{bmatrix} \begin{bmatrix}
X_n \\
Y_n
\end{bmatrix} (mod l) \tag{6}
\]

where \( k, n \) are parameters that can be used as keys, and \( k \in [1, l] \). \( l \) denotes the dimensions of the sub-block high frequency coefficient sub-bands. \( n \) is the number of iterations, with different values of \( n \) for different coordinates. The coefficient coordinates \( X, Y \in [0, 1, 2, \ldots, l - 1] \) can be viewed as a tight branch set \( V_n \) of the space \( U \) on a two-dimensional plane. After a number of iterations, the distribution of points
in the tight branch set $V_n$ is chaotically disordered to the whole $U$ space, that is, the coefficient coordinates are distributed to the whole plane.

In this paper, the fitness function is defined as the total number of bits of the secret information that match the lowest significant bits of the high frequency coefficients after the embedding position matrix has been permuted.

Step3: Find $p_{best}$ and $g_{best}$

If the fitness function value calculated at the current position of particle $i$ is higher than the previous one, $p_{best}$ is updated with the new position. In addition, if the fitness function value is globally higher, $g_{best}$ is updated to the current position. Otherwise, $p_{best}$ and $g_{best}$ do not undergo any change.

Step4: Update process

Update the position and velocity of each particle with (3) and (4). However, applying these formulas may produce a floating point value. Therefore, this paper performs a whole rounding operation for the particle positions and velocities after each update.

Step5: Stopping criteria

The algorithm satisfies the stopping condition if the number of iterations reaches its maximum permissible value. Thus, we obtain $g_{best}$, which corresponds to the keys $k$ and $n$, and by performing the calculation in (6) we obtain the optimal embedding position matrix of the secret information.

The secret information is scrambled by the optimal embedding position matrix, so that the total number of bits matching the lowest significant bits of the wavelet high frequency coefficients is maximized, resulting in a stego image with optimal quality.

C. EMBEDDING PROCESS

Embedding is the process of hiding secret information into a cover image. In this paper, the coefficients of the integer wavelet transform are used to embed the secret information. The secret information is embedded into the lowest significant bits of the wavelet high frequency coefficients, while the embedding position matrix is used to minimize the pixel difference between the cover image and the stego image.

The embedding process is divided into four steps.

Step1: Access the secret message code stream generated in Section III.

Step2: The secret information code stream is converted to a scrambled secret information code stream according to the optimal embedding position matrix obtained in Section B.

Step3: Embedding of the scrambled secret information code stream into the lowest significant bit of each coefficient in the HH sub-band using the wavelet coefficients generated in Section A. The embedding sequence in the sub-band is a raster scan.

Step4: Applying IIWT to wavelet sub-band coefficients to convert the image from transform domain to spatial domain.

With the above embedding process, the stego image of the $m$-th image sub-block is obtained. The sender has to put the best keys of all sub-blocks in an array and send it to the receiver.

V. SECRET INFORMATION EXTRACTION AND TRANSMISSION ERROR DETECTION RECOVERY

A. SECRET INFORMATION EXTRACTION PROCESS

Once transmitted through the hydro-acoustic channel, the stego image is accepted at the receiver end, which is disturbed by transmission errors, and the stego image is extracted for secret information. The extraction process of the method at the receiver end is divided into the following five steps.

Step1: Divides the stego image into non-overlapping sub-blocks.

Step2: Transformation of sub-blocks from spatial domain to transform domain by integer wavelet transform.

Step3: From the high frequency sub-band coefficients, the lowest significant bits are extracted to form a scrambled secret information code stream. The extraction sequence is a raster scan sequence, the same as the embedding sequence.

Step4: The key is employed to calculate the embedding position matrix, which converts the scrambled secret information stream into the original secret information stream.

Step5: By combining the original secret information of all the sub-blocks, the embedded data code stream that was disturbed by transmission errors is reconstructed.

B. TRANSMISSION ERROR DETECTION AND RECOVERY PROCESS

After reconstructing the embedded information that has been disturbed by transmission errors, the receiver must perform error detection and recovery. Errors in underwater acoustic channel transmissions include packet loss errors, as well as burst errors and random bit errors that occur in the packet. Packet loss errors cause the greatest loss of data, so the following lists transmission error detection and recovery measures for packet loss errors. Packet loss errors can be detected by observing whether the sequence number $Num$ of adjacent packets is consecutive. Different error masking measures are required for low frequency data and high frequency data, which are described below.

A commonly used error recovery for low frequency coefficients is the eight neighbourhood averaging algorithm. This algorithm takes into account the smoothness of the image, but is less effective in recovering the edge part of the image. In this paper, the error recovery method of neighbourhood-weighted averaging [19] is used, which can better solve the above problems. When the low frequency coefficient $c_{x,y}$ is lost, it can be estimated using its eight neighbourhood coefficients according to (7). Where $L_h$, $L_v$, and $L_d$ represent the average of the neighbourhood coefficients in the horizontal, vertical, and diagonal directions respectively; $a_1$ to $a_8$ represent the states of the eight low-frequency coefficients in the eight neighbour-hoods of $c_{x,y}$. A value of 1 indicates that the coefficient is error-free; a value of 0 indicates that
the coefficient is error-prone and unavailable.

\[ c_{x,y} = h_{wt}L_h + v_{wt}L_v + d_{wt}L_d \]

\[ L_h = \frac{a_1c_{x-1,y} + a_2c_{x+1,y}}{a_1 + a_2} \]

\[ L_v = \frac{a_3c_{x,y-1} + a_4c_{x,y+1}}{a_3 + a_4} \]

\[ L_d = \frac{(a_5c_{x-1,y-1} + a_6c_{x+1,y-1} + a_7c_{x-1,y+1} + a_8c_{x+1,y+1})}{a_5 + a_6 + a_7 + a} \]  

(7)

\[ h_{wt}, v_{wt} \text{ and } d_{wt} \] are the weights of the horizontal, vertical and diagonal directional neighbourhood coefficients respectively, such that the absolute values of \( c_{x,y} \) corresponding to the horizontal, vertical and diagonal directional HF coefficients are \( h, v, d \). Then the weights of each directional neighbourhood coefficient are defined as follows.

\[ h_{wt} = \frac{h + 1}{h + v + d + 3} \]  

(8)

\[ v_{wt} = \frac{v + 1}{h + v + d + 3} \]  

(9)

\[ d_{wt} = \frac{d + 1}{h + v + d + 3} \]  

(10)

It can be seen that the magnitude of the weights in each direction is proportional to the absolute value of the lost coefficients corresponding to the high frequency coefficients.

Due to the poor correlation between the HF coefficients, various error masking methods have yielded little result despite extensive interpolation operations [20]. Therefore, this paper takes the measure of directly filling in zero for the high-frequency coefficients with errors detected.

VI. EXPERIMENTAL RESULTS AND ANALYSIS

A. EXPERIMENTAL ENVIRONMENT

This paper evaluates the performance of the algorithm in four aspects: stego image quality, security, transmission error detection and recovery performance and algorithm running time. The proposed method is implemented in Visual C++. The performance of the steganographic scheme in this paper is evaluated using eight different standard gray-scale images as cover images. The resolution of all these images is 512 × 512, which is very popular in the research community [21]. Two units bit and bpp are used to represent the length of the data. If \( L \) bits are embedded into an image of size \( H \times W \), the length of data is expressed using the unit bpp, calculated as \( (L/(H \times W)) \).

B. EVALUATION OF EMBEDDING CAPACITY AND STEGO IMAGE QUALITY

Invisibility of noise in stego image is the simplest and most basic requirement for any steganography method. Fig. 4 shows the stego images obtained by the proposed method by embedding three data streams in Baboon images of lengths 0.25 bpp, 0.5 bpp and 0.75 bpp respectively. Visually, the stego images with different embedding capacities are visually indistinguishable from the cover image, and thus the proposed method satisfies visual invisibility. However, satisfying this requirement alone is not sufficient and the quality of the stego images should be evaluated more accurately using quantitative criteria. For steganography, one of the most effective quality metrics is Peak Signal to Noise Ratio (PSNR), which measures the similarity between the cover image and the stego image [22]. High PSNR values mean that the difference between the stego image and the cover image is smaller and the hidden secret information is less visible. In addition to PSNR, the Structural Similarity Index Measure (SSIM) is also used to evaluate the quality of the stego images generated by the method in this paper [23].

The maximum embedding capacity of the method is 0.75 bpp, so for a 512 × 512 image, the method can embed data with a maximum length of 196608 bits in the image. To investigate the effect of embedding data length on stego image quality, data of different lengths from 16384 bits to 196000 bits have been embedded in eight standard test images and the PSNR and SSIM of the stego images have been measured and the results are shown in Table 1. Results show that stego image quality is directly related to the length of the data embedded in them.

The performance of the DWT-based methods [6], [7] and the IWT-based method [12] has been compared with the method in this paper. The comparison is performed at an embedding level of 0.5 bpp and the values of the two parameters PSNR and SSIM for the test images are shown in Table 2. The results show that the algorithm in this paper outperforms the other three methods in terms of both PSNR and SSIM.

FIGURE 4. Results for cover images and stego images with different embedding lengths. (a) Cover image; (b) Stego image, embedding rate 0.25bpp; (c) Stego image, embedding rate 0.5bpp; (d) Stego image, embedding rate 0.75bpp.
TABLE 1. PSNR and SSIM of stego images with different embedding data lengths.

|   | L=16384bits | L=65536bits | L=131072bits | L=196608bits |
|---|-------------|-------------|--------------|--------------|
| Lena | PSNR | 65.01 | 56.5312 | 0.9999 | 52.78 | 0.9999 | 50.68 | 0.9999 |
| Baboon | PSNR | 63.61 | 56.4440 | 0.9999 | 52.84 | 0.9999 | 51.04 | 0.9998 |
| Peppers | PSNR | 62.79 | 56.7416 | 0.9999 | 52.76 | 0.9999 | 50.56 | 0.9999 |
| Couple | SSIM | 0.9999 | 56.44 | 0.9999 | 52.84 | 0.9999 | 50.90 | 0.9998 |
| Boat | SSIM | 0.9999 | 56.51 | 0.9999 | 52.81 | 0.9999 | 50.87 | 0.9999 |
| Jet | SSIM | 0.9999 | 56.58 | 0.9999 | 52.78 | 0.9999 | 50.85 | 0.9999 |
| Splash | SSIM | 0.9999 | 57.13 | 0.9999 | 52.80 | 0.9999 | 50.71 | 0.9999 |
| Goldhill | SSIM | 0.9999 | 56.41 | 0.9999 | 52.82 | 0.9999 | 50.89 | 0.9998 |

TABLE 2. Image steganography results comparison.

|   | This paper | [16] | [10] | [11] |
|---|------------|------|------|------|
| Image | PSNR | SSIM | PSNR | SSIM | PSNR | SSIM | PSNR | SSIM |
| Lena | 52.78 | 0.9999 | 52.53 | 0.9977 | 51.48 | 0.9971 | 49.11 | 0.9970 |
| Baboon | 52.84 | 0.9999 | 52.14 | 0.9990 | 51.47 | 0.9988 | 49.11 | 0.9970 |
| Peppers | 52.76 | 0.9999 | 52.41 | 0.9972 | 51.48 | 0.9970 | 49.11 | 0.9868 |
| Jet | 52.78 | 0.9999 | 52.76 | 0.9980 | 51.47 | 0.9968 | 49.14 | 0.9767 |
| Splash | 52.80 | 0.9999 | 52.77 | 0.9966 | 51.49 | 0.9964 | 49.12 | 0.9977 |

C. SECURITY ANALYSIS
Steganographic methods generate stego images by modifying the cover image. The steganalysis attack utilizes these changes to discover the presence of hidden information. As the amount of these changes increases, the likelihood of the hidden data being discovered increases, which means that the steganographic method fails. Therefore, security testing of steganographic methods is of great importance in practice. In the following, RS attacks are used to test the security of the proposed method.

RS steganalysis is a technique used to estimate the security of steganographic methods. In this technique, the pixels of a stego image are divided into three groups: the regular group ($R_m$ or $R_{-m}$), the singular group ($S_m$ or $S_{-m}$) and the anomaly group, by using the $m$-mask and the $f$-function. If the two relations $R_m \cong R_{-m}$ and $S_m \cong S_{-m}$ hold for a stego image, it means that the steganalysis method failed to discover the data in that image and therefore the steganography method is secure against this attack. RS steganalysis is tested on three images, Lena, Baboon and Pepper, with different embedding data amounts, and the results are shown in Fig.5. These three figures show that the proposed method is resistant to RS attacks at different embedding levels and that such attacks cannot detect the data embedded by the method.

D. TRANSMISSION ERROR DETECTION AND RECOVERY PERFORMANCE TESTS
In this paper, the underwater secret image data is embedded in a cover image using the proposed error-resistant steganography algorithm. The obtained stego image is transmitted in the hydro-acoustic channel and the information is extracted to reconstruct the image under the interference of hydro-acoustic channel errors and the experimental results are shown in Fig.6. In this paper, the most serious consequence of packet loss error in hydro-acoustic channel transmission is selected for testing.

From the results, it can be seen that the quality of the extracted underwater images after error recovery is acceptable when the stego images are disturbed by various channel errors. In particular, when the packet loss rate is as high as 20%, the PSNR of the reconstructed images of Uw1 and Uw2 can reach 36.32dB and 37.24dB respectively. Moreover, the
### TABLE 3. Running time of the algorithm.

| Embedding | 0.25bpp | 0.5bpp | 0.75bpp |
|-----------|---------|--------|---------|
| Extraction| 142s    | 248s   | 355s    |
|           | 1.183s  | 1.774s | 2.366s  |

Overall image quality is completely acceptable in terms of visual aspect.

At a packet loss rate of 10% or more, the reconstructed PSNRs of the other four underwater images are above 34dB, and the reconstructed images have good visual quality.

### E. COMPUTATION TIME TESTS

For embedded video surveillance systems installed on unmanned vessels or buoys, the computation time of the steganography algorithm is an important performance indicator. Table 3 shows the computation times of this method at three different embedding levels. A normal portable laptop specifications used in this test are as follows: Processor: Intel (R) Core (TM) i7-4510U CPU @ 2GHZ; Main memory: 8GB; Video card chip: Intel GMA HD 4400. Because underwater robots generally use embedded systems, their computing power is comparable to normal laptops.

The results in Table 3 show that the processing speed of the algorithm is suitable for the real-time requirements of underwater robotic acoustic communication.

### VII. CONCLUSION

This paper proposes an image steganography algorithm based on PSO and IWT for underwater acoustic communication. This algorithm adopts interleaving packing measures for the pending embedded data, which improves the transmission error detection and recovery capability of the underwater image. The cover image is chunked before the integer wavelet transform, which not only saves the search space of PSO, but also improves the search performance of the algorithm. The optimal chaotic scrambled matrix is selected by PSO, which obtains the optimal matching position of the secret information and produces the best quality stego image. The secret information is reprocessed using transmission error detection and recovery measures to improve the reconstruction quality of underwater images. Experimental results show that the algorithm achieves better visual quality of stego images with the same information embedding capacity, enables fast and secure underwater image information hiding, and solves the problem of noise interference in the harsh underwater environment that exists in underwater acoustic communication.

### REFERENCES

[1] C.-S. Hsu and S.-F. Tu, “Finding optimal LSB substitution using ant colony optimization algorithm,” in Proc. 2nd Int. Conf. Commun. Softw. Netw., 2010, pp. 293–297.

[2] R.-Z. Wang, C.-F. Lin, and J.-C. Lin, “Image hiding by optimal LSB substitution and genetic algorithm,” Pattern Recognit., vol. 34, no. 3, pp. 671–683, 2001.
[3] D.-C. Wu and W.-H. Tsai, “A steganographic method for images by pixel-value differencing,” Pattern Recognit. Lett., vol. 24, nos. 9–10, pp. 1613–1626, Jun. 2003.

[4] A. Sahu and G. Swain, “Dual stego-imaging based reversible data hiding using improved LSB matching,” Int. J. IntelI. Eng. Syst., vol. 12, no. 5, pp. 63–73, Oct. 2019.

[5] X. Liao, Y. Yu, B. Li, Z. Li, and Z. Qin, “A new payload partition strategy in color image steganography,” IEEE Trans. Circuits Syst. Video Technol., vol. 30, no. 3, pp. 685–696, Mar. 2020.

[6] X. Liao, J. Yin, M. Chen, and Z. Qin, “Adaptive payload distribution in multiple images steganography based on image texture features,” IEEE Trans. Dependable Secure Comput., vol. 19, no. 2, pp. 897–911, Apr. 2022.

[7] J. Tao, X. Liao, J. Liu, Y. Cao, and H. Jiang, “Channel attention image steganography with generative adversarial networks,” IEEE Trans. Netw. Sci. Eng., vol. 9, no. 2, pp. 888–903, Mar. 2022.

[8] T. Fillier, J. Judas, and J. Fridrich, “Minimizing additive distortion in steganography using syndrome-trellis codes,” IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 920–935, Sep. 2011.

[9] M. Fakhredanesh, M. Rahmati, and R. Safabakhsh, “Steganography in discrete wavelet transform based on human visual system and cover model,” Multimedia Tools Appl., vol. 78, no. 13, pp. 18475–18502, Jul. 2019.

[10] V. Sabeti and M. Amerehei, “Secure and imperceptible image steganography in discrete wavelet transform using the XOR logical function and genetic algorithm,” ISeCure, vol. 14, no. 2, pp. 167–179, 2022.

[11] S. Atawneh, A. Almomani, H. Al Bazar, P. Sumari, and B. Gupta, “Secure and imperceptible digital image steganographic algorithm based on diamond encoding in DWT domain,” Multimedia Tools Appl., vol. 76, no. 18, pp. 18451–18472, Sep. 2017.

[12] A. K. Galve and M. S. Joshi, “An image steganography method hiding secret data into coefficients of integer wavelet transform using pixel value differencing approach,” Math. Problems Eng., vol. 2015, pp. 1–11, 2015.

[13] H. Al-Dmour and A. Al-Ani, “A steganography embedding method based on edge identification and XOR coding,” Exp. Syst. Appl., vol. 46, pp. 293–306, Mar. 2016.

[14] A. Miri and K. Faez, “An image steganography method based on integer wavelet transform,” Multimedia Tools Appl., vol. 77, no. 11, pp. 13133–13144, Jun. 2018.

[15] P. K. Muhuri, Z. Ashraf, and S. Goel, “A novel image steganographic method based on integer wavelet transformation and particle swarm optimization,” Appl. Soft Comput., vol. 92, Jul. 2020, Art. no. 106257.

[16] V. Sabeti, M. Sobhani, and S. M. H. Hasheminejad, “An adaptive image steganography method based on integer wavelet transform using genetic algorithm,” Comput. Electr. Eng., vol. 99, Apr. 2022, Art. no. 107809.

[17] C. Lin, B. Zhang, and Y. F. Zheng, “Packed integer wavelet transform constructed by lifting scheme,” IEEE Trans. Circuits Syst. Video Technol., vol. 10, no. 8, pp. 1496–1501, Dec. 2000.

[18] J. Kennedy and R. Eberhart, “Particle swarm optimization,” in Proc. IEEE ICNN, vol. 4, Nov./Dec. 1995, pp. 1942–1948.