

## Optimum Reversible Information Hiding Based on Adaptive Joint Processing

Zhijie Mao<sup>1,a</sup>, Yinfa Zhang<sup>1</sup>, Lin Zhou<sup>1</sup>, and Tinglong Du<sup>2</sup>

<sup>1</sup> Department of Information Transmission, Xi'an Communications Institute, Shaanxi, 710106, China

<sup>2</sup> Department of Information Security, Xi'an Communications Institute, Shaanxi, 710106, China

<sup>a</sup> 2657262006@qq.com

**Keywords:** Information Hiding, Stego-information, Integer Wavelet Transform (IWT), Assignment Algorithm, Peak Signal to Noise Ratio (PSNR).

**Abstract.** This paper presents a novel reversible information hiding method for digital images by a joint with integer wavelet transform and assignment algorithm. This scheme takes advantage of Gaussian-like distribution histogram for utilizing integer wavelet coefficients in frequency and assignment algorithm for best matching between the secret image and the original one. Experimental results show that original image and extracted marked image could have high visual quality and they are perceptually similar to their original versions. In addition, results show that this scheme outperforms peak signal to noise ratio (PSNR) than other methods.

### Introduction

The security of data problem, also known as the maximum weighted bipartite reversible processing problem, is a widely-studied problem applicable to many domains. Secure information means to hide the secret data into another data. The main targets of information security are to hide the secret data and avoid unauthorized attackers using the secret. The secure communication is main purpose of the security of data, in such a way that the stego-information (modified data which contains secret data) should not deviate much from original data (data not containing any secret information) and the observer could not be able to distinguish any sense between them with respecting to remain the real message invisible for the observer.

Several efficient data embedding methods have been proposed. They include set partitioning in hierarchical trees in [1], embedded block based coding with optimized truncation and set partitioning embedded block in [2,3]. These algorithms are efficient based on the discrete wavelet transform (DWT). However, the image coefficients decomposed by the DWT are floating-point numbers, which increases the computational complexity and is not well suited for efficient lossless coding application.

To solve the above problems, Daubechies and Sweldens presented the lifting scheme (LS) [4]. Based on the LS, a kind of new transforms called integer wavelet transforms (IWT) are proposed, which is a low complexity and efficient implementation of the DWT and can support the lossless data coding [5-8]. It is a basic modification of linear transforms, where each filter output is rounded to the nearest integer. IWT can be used to have a unified lossy and lossless codec. It is also of interest for hardware implementations, where the use of floating point is still a costly operation. In software implementations, many processors now offers multimedia instructions which can execute multiple integer operations in parallel, like the MMX instruction set in the Pentium processor [9]. The use of IWT is also a means to reduce the memory demands of the compression algorithm as integers are used instead of real numbers.

We present an information hiding method based on IWT joined with the use of assignment algorithm [10-13]. We hide secret image into the integer wavelet coefficients of the original image in order to provide higher data imperceptibility and increase the robustness of our steganography method. IWT avoids the floating point precision problems of the wavelet filter. Also, we also used an assignment algorithm to select the best embedding locations of the integer wavelet coefficients to increase the system security and stego-information can have high visual quality.

The remainder of this paper is organized as follows. IWT and the Hungarian's assignment algorithm are presented in Section II. The proposed method is detailed presented in Section III. Experimental results and performance evaluation are presented in Section IV. The conclusion is drawn in Section V.

## Integer Wavelet Transform and Hungarian Algorithm

### A. Integer Wavelet Transform

For the forward transform, typically the data is split into the even and odd samples have been replaced by low pass and high pass coefficients, respectively. The inverse transform is calculated by reversing the order of the lifting steps and flipping the signs. But reversible integer wavelet transforms can be constructed by rounding or truncating the output of the lifting step prior to adding. The lifting scheme is a spatial domain construction of biorthogonal wavelets developed by Sweldens [5]. Lifting allows a wavelet transform to be computed quickly through a series of individual lifting steps. Several reversible integer wavelet transforms based on the lifting scheme have been used extensively in the literature and are described in the remainder of this section. In each case, one dimensional signal  $\{x_l\}_{l \in \mathbb{Z}}$ , the lifting steps are described as follows.

$$\begin{cases} s_l^{(0)} = x_{2l} \\ d_l^{(0)} = x_{2l+1} \end{cases}, \begin{cases} d_l^{(1)} = d_l^{(0)} + \mathbf{a} (s_l^{(0)} + s_{l+1}^{(0)}) \\ s_l^{(1)} = s_l^{(0)} + \mathbf{b} (d_l^{(1)} + d_{l-1}^{(1)}) \end{cases} \quad (1)$$

$$\begin{cases} d_l^{(2)} = d_l^{(1)} + \mathbf{g} (s_l^{(1)} + s_{l+1}^{(1)}) \\ s_l^{(2)} = s_l^{(1)} + \mathbf{d} (d_l^{(2)} + d_{l-1}^{(2)}) \end{cases}, \begin{cases} s_l = \mathbf{z} s_l^{(2)} \\ d_l = d_l^{(2)} / \mathbf{z} \end{cases} \quad (2)$$

$$\mathbf{a} = -1.586134342, \mathbf{b} = -0.05298011854, \mathbf{g} = 0.8829110762, \mathbf{d} = 0.4435068522, \mathbf{z} = 1.149604398 \quad (3)$$

where  $s_l$  and  $d_l$  are generally referred to as lower frequency and detail coefficients, respectively.  $s_l^{(i)}, d_l^{(i)}$  ( $i = 0, 1, 2$ ) are mid-output.

According to integer wavelet theory [7], we construct integer wavelet transform based on the framework mentioned above. That is:

$$\begin{cases} s_l^{(0)} = x_{2l} \\ d_l^{(0)} = x_{2l+1} \end{cases}, \begin{cases} d_l^{(1)} = d_l^{(0)} + \mathbf{int}(\mathbf{a} (s_l^{(0)} + s_{l+1}^{(0)})) \\ s_l^{(1)} = s_l^{(0)} + \mathbf{int}(\mathbf{b} (d_l^{(1)} + d_{l-1}^{(1)})) \end{cases} \quad (4)$$

$$\begin{cases} d_l^{(2)} = d_l^{(1)} + \mathbf{int}(\mathbf{g} (s_l^{(1)} + s_{l+1}^{(1)})) \\ s_l^{(2)} = s_l^{(1)} + \mathbf{int}(\mathbf{d} (d_l^{(2)} + d_{l-1}^{(2)})) \end{cases}, \begin{cases} d_l^{(3)} = d_l^{(2)} + \mathbf{int}((\mathbf{z} - \mathbf{z}^2) s_l^{(2)}) \\ s_l^{(3)} = s_l^{(2)} + \mathbf{int}((-1/\mathbf{z}) d_l^{(3)}) \end{cases} \quad (5)$$

$$\begin{cases} d_l^{(4)} = d_l^{(3)} + \mathbf{int}((\mathbf{z} - 1) s_l^{(3)}) \\ s_l^{(4)} = s_l^{(3)} + d_l^{(4)} \end{cases}, \begin{cases} s_l = s_l^{(4)} \\ d_l = d_l^{(4)} \end{cases} \quad (6)$$

where  $\mathbf{int}$  means integer part of  $x$ . The values of parameters  $\mathbf{a}, \mathbf{b}, \mathbf{g}, \mathbf{d}, \mathbf{z}$  are given in formula (3). Equation (5) is an extra lifting step different from Equation (2). We adopt it here because it can achieve reversible transform according to [7] while Equation (2) cannot.

Wavelet transform decomposes an image into a set of band limited components which can be reassembled to reconstruct the original data without error. In general most of the image energy is concentrated at the lower frequency coefficient sets (approximation coefficients) and therefore embedding secret data in these coefficient sets may degrade the image significantly. Embedding in the low frequency coefficient sets, however, could increase robustness significantly.

On the other hand, the high frequency coefficient sets (diagonal detail coefficients) include the edges and textures of the image and the human eye is not generally sensitive to changes in such coefficient sets. This allows the secret image to be embedded without being perceived by the human eye. The agreement adopted by many wavelet-based image hiding methods, is to embed the secret image in the

middle frequency coefficient sets (horizontal detail coefficients and vertical detail coefficients) is better in perspective of imperceptibility and robustness.

Lifting schemes which we have used in this paper is one of many techniques that can be used to perform integer wavelet transform. The wavelet lifting scheme is a method for decomposing wavelet transform into a set of stages. An advantage of lifting schemes is that they do not require temporary storage in the calculation steps and have required less no of computation steps.

### B. Hungarian Algorithm

The Hungarian algorithm assumes the existence of a bipartite graph  $G = \{V, U, E\}$  as illustrated in Figure 1, where  $V$  and  $U$  are the sets of nodes in each partition of the graph, and  $E$  is the set of edges. The edge weights may be stored in a matrix  $C_{ost}$ . The method maintains feasible values for all the  $d_i$  and  $g_j$  from initialization through termination. An edge in the bipartite graph is called admissible when  $d_i + g_j \leq c_{ij}$ .

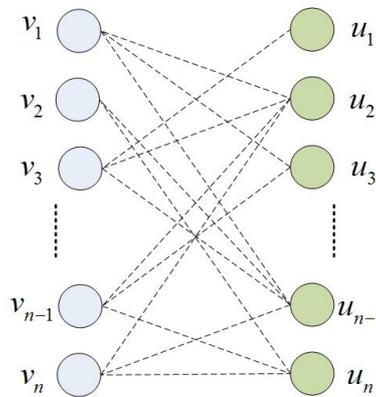


Fig.1 Bipartite graph showing matched and unmatched edges

Algorithm input:

- w** An assignment problem comprising a bipartite graph  $G = \{V, U, E\}$  (where  $|V| = |U| = n$ ) and an  $n \times n$  matrix of edge costs  $C_{ost}$ .
- w** An optimal solution to the above assignment problem, comprising a complete matching  $M$ , and the final values of all dual variables  $d_i$  and  $g_j$ .
- w** Each of which can be a row  $c_{i*}$ , a column  $c_{*j}$  or a single entry  $c_{ij}$  of the cost matrix  $C_{ost}$ .

Algorithm output:

- w** A new complete matching  $M$ , representing an optimal solution to the problem with the changed edge costs.

The hungarian algorithm steps are described as follows.

**Step.1** Begin with an empty matching  $M_0 = \emptyset$ . Assign feasible values to the dual variables  $d_i$  and  $g_j$  as follows:

$$\begin{aligned} \forall v_i \in V, d_i &= 0 \\ \forall u_j \in U, g_j &= \min_i (c_{ij}) \end{aligned} \quad (7)$$

**Step.2** Designate each exposed (unmatched) node in  $V$  as the root of a Hungarian tree.

**Step.3** Grow the Hungarian trees rooted at the exposed nodes in the equality subgraph. Designate the indices  $i$  of nodes  $v_i$  encountered in the Hungarian tree by the set  $I$ , and the indices  $j$  of nodes  $u_j$  encountered in the Hungarian tree by the set  $J$ . If an augmenting path is found, go to step 5. If not, and the Hungarian trees cannot be grown further, proceed to step 4.

**Step.4** Modify the dual variables  $d_i$  and  $g_j$  as follows to add new edges to the equality subgraph. Then go to step 3 to continue the search for an augmenting path.

$$\begin{aligned}
q &= \frac{1}{2} \min_{i \in I, j \in J} (c_{ij} - d_i - g_j) \\
d_i &\leftarrow \begin{cases} d_i + q, i \in I \\ d_i - q, i \notin I \end{cases} \\
g_j &\leftarrow \begin{cases} g_j + q, j \in J \\ g_j - q, j \notin J \end{cases}
\end{aligned} \tag{8}$$

**Step.5** Augment the current matching by flipping matched and unmatched edges along the selected augmenting path. That is,  $M_k$  (the new matching at stage  $k$ ) is given by  $(M_{k-1} - P) \cup (P - M_{k-1})$ , where  $M_{k-1}$  is the matching from the previous stage and  $P$  is the set of edges on the selected augmenting path.

**Step.6** Output the matching after the  $n^{\text{th}}$  stage:  $M = M_n$ .

### Adaptive Reversible Joint Processing

In the adaptive reversible joint processing method, the original and secret images are decomposed into 4 sub-images such as approximation coefficients (WC), horizontal detail coefficients (WH), vertical detail coefficients (WV) and diagonal detail coefficients (WD) using integer wavelet transform. These sub-images are divided into non-overlapping blocks. The blocks of approximation coefficients of original image are subtracted from approximation coefficients of secret image. The differences of these coefficients are called error blocks.

By applying assignment algorithm, matching and distribution could be optimized. Thus, by using Hungarian's assignment algorithm, we find the best matched blocks between resulted error blocks and the  $3 \times 3$  non-overlapping blocks that belong to WH sub-image of original image. We find best embedding locations of original image and then replace these error blocks with related matched blocks of original image.

In addition, in this scheme we have two secret keys that we have made them in two different ways. Therefore, we have partly increased the security. Also, in this method matching and distribution have been optimized. Figure 2 shows the block diagram of the adaptive reversible joint processing method, left: data embedding, right: data extraction.

#### A. Embedding Procedure

The steps of embedding procedure are as follows.

**Step.1** Using integer wavelet transform, decompose the original image  $C$  and the secret image  $S$  into nine sub-images  $C_{2 \times 2}$  and  $S_{2 \times 2}$ , respectively.

$$C_{2 \times 2} = \begin{bmatrix} CWC & CWH \\ CWV & CWD \end{bmatrix}, S_{2 \times 2} = \begin{bmatrix} SWC & SWH \\ SWV & SWD \end{bmatrix} \tag{9}$$

**Step.2** Each of  $SWC$ ,  $CWC$ , and  $CWH$  are partitioned into blocks of  $3 \times 3$  pixels and can be represented by:

$$\begin{aligned}
SWC_{3 \times 3} &= \{SS_i, 1 \leq i \leq 9\} \\
CWC_{3 \times 3} &= \{CC_j, 1 \leq j \leq 9\} \\
CWH_{3 \times 3} &= \{HH_k, 1 \leq k \leq 9\}
\end{aligned} \tag{10}$$

where  $SS_i$ ,  $CC_j$  and  $HH_k$  represent the  $i^{\text{th}}$  block in  $SWC$ , the  $j^{\text{th}}$  block in  $CWC$  and the  $k^{\text{th}}$  block in  $CWH$ , respectively.

**Step.3** For each block  $SS_i$  in  $SWC$ , the best matched block  $CC_j$  of minimum error in  $CWC$  is searched by using the root mean squared error (RMSE). Calculate the error block  $RMSE_{SC}$  between  $SS_i$  and  $CC_j$  as follows:

$$RMSE_{SC_i} = E\{SS_i - CC_j\} \quad (11)$$

The first secret key  $K_j$  consists of the addresses  $j$  of the best matched blocks in  $CWC$ .

**Step.4** After finding all of the error blocks in step3, then for each error block  $RMSE_{SC_i}$ , the best matched block  $HH_k$  in  $CWH$  is searched by Hungarian's algorithm. So, we first create  $3 \times 3$  matrix, called the cost matrix. In which each element represents the RMSE between each of  $RMSE_{SC_i}$  blocks and  $HH_k$  blocks. In fact, the minimal cost perfect matching is the set of  $HH_k$  blocks corresponding to these  $RMSE_{SC_i}$  blocks. In this way, we can find the best blocks of  $HH_k$  that have best matching with  $RMSE_{SC_i}$  blocks, the second secret key  $K_k$  consists of the addresses  $k$  of the best matched blocks in  $CWH$ . Therefore, now we have the best option for embedding. So, we replace these  $HH_k$  blocks with matched  $RMSE_{SC_i}$  blocks.

**Step.5** After embedding all of  $RMSE_{SC_i}$  blocks in step 4, apply the inverse IWT to the  $CWC$ ,  $CWV$ ,  $CWD$ , and the modified sub-image  $CWH$  to obtain the stego-data  $D$ .

## B. Extraction Procedure

The steps of secret image extraction procedure are as follows.

**Step.1** Decompose the stego-data  $D$  into four sub-images [ $DWC$ ,  $DWH$ ;  $DWV$ ,  $DWD$ ] using integer wavelet transform.

**Step.2** Extract the block  $CC_j$  from the sub-image  $DWC$  by using first secret key  $K_j$ . Use the second secret key  $K_k$  to extract the error block. The secret block  $SS_i$  can be obtained by:

$$SS_i = E\{CC_j - RMSE_{SC_i}\} \quad (12)$$

Repeat step 2 until all secret blocks are extracted and form the sub-image  $CWC$ .

**Step.3** Using detail coefficients from sender such as  $CWD$ ,  $CWV$ ,  $CWH$  and extracted  $CWC$  from above step, apply the inverse IWT to obtain the embedded secret image which is visually similar to the original data.

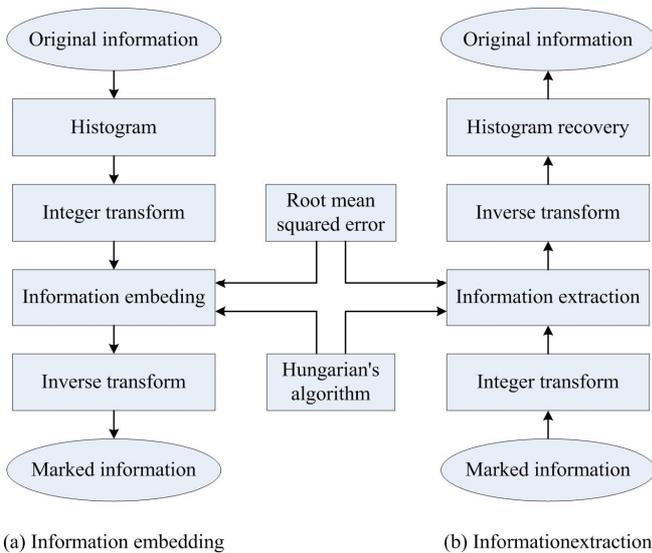


Fig.2 Block diagram of the presented method, Left: data of embedding, Right: data extraction

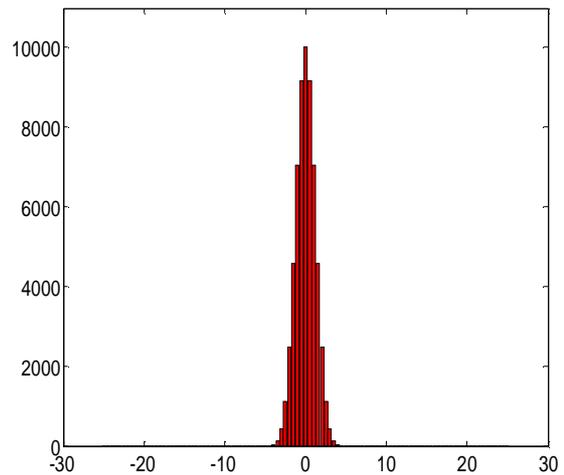


Fig.3 Histogram of one detail subband 512x512 grayscale image Lena

## Experimental Results

Experimental results of a wide range of natural images show that histogram of IWT detail subband has approximate shape of discrete Gaussian distribution function likewise. Moreover, study on human

visual system in digital wavelet transform domain indicates that modification on wavelet coefficients under detection threshold can't be detected by human eyes. Figure 3 shows histogram of a detail subband of  $512 \times 512$  grayscale image Lena. This work presented a particular property of wavelet detail coefficients of almost every natural textured image that they have a histogram corresponding to a Generalized Gaussian Density (GGD).



Fig. 4 Visual impact of the presented method in Lena,

(a) PSNR = 44.3dB, 0.121bpp (b) PSNR = 41.6dB, 0.306bpp

We applied the presented reversible information hiding algorithm to a grayscale level images of Lena of size  $512 \times 512$  shown in Figure 4. For an image of size of  $512 \times 512$ , a payload 1 bpp (bits per pixel) means that 262,144 (namely  $512 \times 512$ ) bits are embedded in the image. The results indicate that the adaptive reversible joint processing algorithm can hidden a large payload, while maintain the high peak signal-to-noise-ratio (PSNR) of the marked image versus the original image. In Figure 5, the comparison results between the difference expansion method [6] and our proposed method are shown. It is observed that our proposed method can obtain better visual quality in the same payload. More than 2dB improvement in PSNR has been achieved.

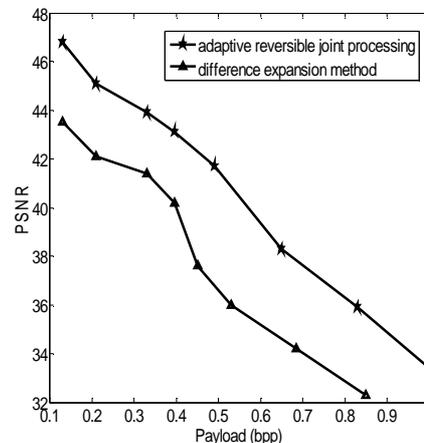


Fig.5 Comparison results on Lena

## Conclusions

This paper presents an adaptive reversible information hiding method based on integer wavelet transform and assignment algorithm. Experimental results and the comparison with the difference expansion method demonstrate that this joint processing method can obtain a better visual quality of the marked image at the same payload. It is expected that this reversible data hiding technique will be deployed for a wide range of applications in secure data system.

## Acknowledgement

The authors deeply thank several colleagues who helped them at different stages during the preparation of this paper. In particular, the authors thank the anonymous reviewers for their helpful comments and suggestions. The project supported in part by Natural Science Basic Research Plan in Shaanxi Province of China (Program No.2014JM2-6101, 2015JM6325).

## References

- [1] Said, W.A.Pearlman, New fast and efficient image codec based on set partitioning in hierarchical trees. IEEE Transaction on Circuit System Video Technology, Vol.6, pp.243-249, 1996.
- [2] D.Taubman, High performance scalable image compression with EBCOT. Proceeding of IEEE, IEEE International Conference on Image Processing, pp.24-28, 2013.

- [3] W.A.Pearlman,A.Islam,N.Nagaraj, and A.Said, Efficient, low-complexity image coding with a set-partitioning embedded block coder. IEEE Transaction on Circuit and Systems for Video Technology, Vol.14,pp.1219-1235,2014.
- [4] Daubechies, W.Sweldens, Factoring wavelet transforms into lifting steps. Journal of Fourier Analysis Application, Vol.4(3),pp.247-269,1998.
- [5] W.Sweldens, The lifting scheme: A custom-design construction of biorthogonal wavelets, Appl. Comput.Harmon. Anal., Vol.3(2), pp.186-200,1996.
- [6] S.Mallat, A theory of multiresolution signal decomposition: the wavelet representation. IEEE Transactions Pattern Analysis and Machine Intelligence, pp.674-693,2013.
- [7] R.Calderbank, I.Daubechies, W.Sweldens, and B. L.Yeo, Lossless image compression using integer to integer wavelet transforms, in International Conference on Image Processing (ICIP), Vol.(I).1997, pp.596-599,IEEE Press.
- [8] R.Calderbank, I.Daubechies, W.Sweldens, and B. L.Yeo, Wavelet transforms that map integers to integers, Appl. Comput. Harmon. Anal., Vol.5(3), pp.332-369,1998.
- [9] Intel-Corporation, Intel architecture MMX(TM) technology, programmer's reference manual, Tech. Rep.,Intel Corporation, March 2010.
- [10]M.Z.Spivey, W.B.Powll, The dynamic assignment problem. Transportation Science Vol38(4), pp.399-419,2014.
- [11]J.Munkres, Algorithms for the assignment and transportation problems. Journal of the Society for Industrial and Applied Mathematics Vol.5(1),pp.32–38,1957.
- [12]E.L.Lawler, Combinatorial Optimization: Networks and Matroids. Holt, Reinehart and Winston, New York,1976.
- [13]R.E.Burkard, C.E.Ela, Handbook of combinatorial optimization, Supplement Volume A.Kluwer Academic Publishers, ch. Linear assignment problems and extensions,pp.75-149,1999.