Data Hiding Using Difference Expansion Method

YASMEEN M.G, RAJALAKSHMI G

Final year M.E, Arunai Engineering College, Thiruvannamalai, Tamilnadu, India
Assistant Professor, Arunai Engineering College, Thiruvannamalai, Tamilnadu, India

Abstract—In inverse order of data hiding techniques, the values of original data are modified according to some particular rules and the original host content can be perfectly restored after extraction of the hidden data on another side. In this paper, the optimal rule of value modification under a payload-distortion criterion is found by using an iterative procedure, and a practical inverse order of data hiding scheme is proposed. The embedded secret data, as well as the auxiliary information used for content get back, are carried by the differences between the original pixel values and the corresponding values estimated from the neighbors. Here, the errors are modified according to the optimal value transfer rule. Also, the original image is divided into a number of pixel subsets and the auxiliary information of a subset is always embedded into the estimation errors in the next subset. A receiver can successfully pull out the embedded secret data and recover the original content in the subsets with an inverse order. This way, a good inverse order of data hiding performance is achieved.

Keywords: Distortion, payload, inverse order of data hiding.

1. INTRODUCTION

DATA hiding technique aims to embed some secret information into a carrier signal by altering the insignificant components for copyright protection or covert communication. In general cases, the data embedding operation will result in distortion in the host signal. However, such distortion, no matter how small it is and they are acceptable to some applications, e.g., military and medical images. In this method, to improve the additional secret messages, the reversibility of embedding methods have been proposed, and they can be simply classified into three types: lossless compression based methods, difference expansion methods, and histogram modification methods. The lossless compression based methods make use of statistical redundancy of the host media by performing lossless compression in order to create empty space to accommodate additional secret data. In the RS method, for example, an ordinary singular status is defined for each group of pixels according to flipping operation and discrimination function. The entry of RS status is the losslessly compressed to provide empty space for data embedding. Alternatively, the least significant digits of pixel values in the L-LSB of quantized DCT coefficients is in JPEG image can also be used to provide the required extra space. In the inverse order of data hiding techniques, as spare, replace can always be made available to accommodate secret data along the chosen item is compressible, but the capacities are low.

Copyright @ IJIRCCE www.ijircce.com 3578
A data-hider can also employ histogram modification mechanisms to realize inverse order of data hiding. In the host image is divided into blocks sized 4×4, 8×8, or 16×16, and gray values are mapped to a circle. After pseudo-randomly segmenting each block into two sub-regions, the histogram rotation of the two sub-regions on this circle is used to embed one bit in each block. On the receiving side, the host block can be recovered from a marked image in a reverse process. Payload of this method is low since each block can only carry one bit. Based on this method, a robust lossless data hiding scheme is proposed in which can be used for semi-fragile image authentication. A typical HM method is defined utilizing the zero and peak points of the histogram of an image and slightly modifies the pixel gray scale values to embed data into the image. In a binary tree structure is used to eliminate the requirement to communicate pairs of peak and zero points to the recipient, and a HM shifting technique is adopted to prevent overflow and underflow. The HM mechanism can be implemented in the difference between sub-sampled images and the prediction error of host pixels, and several good prediction approaches have been introduced to improve the performance of reversible data hiding. Although the original host can be perfectly recovered after data extraction, a data-hider always hopes to lower the distortion caused by data hiding or to maximize the embedded payload with a given distortion level, in other words, to achieve a good "payload-distortion" performance.

II. OPTIMAL VALUE TRANSFER

This section will introduce a value transfer matrix for illustrating the modification of cover values in reversible data hiding. Then, an iterative procedure is proposed to calculate the optimal value transfer matrix, which will be used to realize reversible data hiding with good payload-distortion performance.

In reversible data hiding methods using DE or HM mechanisms, the particular data available for accommodating the secret data, such as pixel differences or prediction errors, are first generated from host image, and then their values are changed according to some given rules, such as difference expansion or histogram modification, to perform the reversible data hiding. Here, we use transfer matrix to model the reversible data hiding in available data. Denote the histogram of the available data as \( H = \{ h_{-2}, h_{-1}, h_{0}, h_{1}, h_{2}, \ldots \} \), where \( h_k \) is the amount of available data with a value \( k \). We also denote the number of available data possessing an original value \( i \) and a new value \( j \) caused by data hiding as \( t_{i,j} \), and a transfer matrix made up of \( t_{i,j} \) as

\[
T = \begin{bmatrix}
  t_{M_1,M_1} & \cdots & t_{M_1,M_2} \\
  \vdots & \ddots & \vdots \\
  t_{M_2,M_1} & \cdots & t_{M_2,M_2}
\end{bmatrix},
\]

(1)

where \( M_1 \) and \( M_2 \) are the minimum and the maximum of the available cover data. Clearly,

\[
\sum_{j=-\infty}^{\infty} t_{i,j} = h_i, \quad (2)
\]

and

\[
t_{i,j} \geq 0. \quad (3)
\]

The new histogram after data hiding should be \( M_2 \).
In fact, the DE and HM reversible data hiding methods possess their corresponding transfer matrixes. For instance, in the typical difference expansion method, the difference between two adjacent pixels is doubled and the secret bit is embedded as the least significant bit of the new difference value,

\[ d = 2d + b. \]  

Here, \( d, d', \) and \( b \) are the original pixel-difference, the new difference value, and the secret bit. That means a difference with original value \( d \) will be changed as \( 2d/(2d+1) \) when the secret bit is 0/1. Since the probabilities of 0 and 1 in secret data are same, \( h_{2d}=h_{2d+1}=h_d/2 \), in other words, \( t_{d,2d}=t_{d,2d+1}=h_d/2 \).

With the typical histogram modification method in after finding a peak point and a zero point of the original histogram, the gray values between them are shifted towards the zeros point by 1, and the pixels with values at the peak point will be kept or shifted by 1 towards the zeros point according to the secret bits to be embedded. Denote \( p \) and \( z \) as the gray values corresponding to the peak and zero points of histogram, and suppose \( p<z \) without loss of generality. Thus, \( h_p=h_{p+1}=h_d/2 \) and \( h_x=h_{x-1} \) \( (p+2 \leq x \leq z) \), in other words, \( t_{p,p}=t_{p,p+1}=h_d/2 \) and \( t_{x-1,x}=h_{x-1} \) \( (p+2 \leq x \leq z) \). So, the transfer matrix is

\[
T = \begin{bmatrix}
    h_{p-1} & 0 & 0 & 0 & \cdots & 0 & 0 & \cdots \\
    \vdots & \ddots & \ddots & \ddots & \vdots & \ddots & \ddots & \ddots \\
    0 & \frac{h_p}{2} & \frac{h_p}{2} & 0 & \cdots & 0 & 0 & \cdots \\
    \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \\
    0 & 0 & 0 & 0 & \cdots & h_x & 0 & \cdots \\
    \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \\
    0 & 0 & 0 & 0 & \cdots & 0 & h_{x+1} & \cdots \\
\end{bmatrix}.
\]

The distortion caused by data hiding is

\[ M_2 = \sum_{i=M_1}^{+\infty} \sum_{j=-\infty}^{\infty} [t_{i,j} \cdot d(i,j)]. \]  

Here, is the energy of distortion when changing the original value \( i \) of an available datum to a new value \( j \). In DE method, the difference value is altered by modifying both the two pixels by \((j-i)/2\) when \((j-i)\) is even, or modifying the two pixels by \((j-i+1)/2\) and \((j-i-1)/2\) respectively when \((j-i)\) is odd. That means

\[
d(i,j) = \begin{cases} 
    \frac{(j-i)^2}{2}, & \text{if } (j-i) \text{ is even} \\
    \frac{((j-i)^2+1)}{2}, & \text{if } (j-i) \text{ is odd}
\end{cases}
\]

And, for histogram modification method in , the energy of distortion caused by changing an original pixel-value \( i \) to a new value \( j \) is

\[ d(i,j) = \frac{(j-i)^2}{2}. \]
By introducing the transfer matrix to model the modification of cover values, the difference expansion and histogram modification methods can be viewed as two special cases. For any transfer matrix, denote its rows

\[
\mathbf{t}_i^{(R)} = [\cdots \quad t_{i,-1} \quad t_{i,0} \quad t_{i,1} \quad \cdots], \quad (10)
\]

and its columns

\[
\mathbf{t}_j^{(C)} = [t_{M_0,j} \quad t_{M_1,j} \quad \cdots \quad t_{M_2,j}]^T. \quad (11)
\]

Considering the available data with original value \(i\), the maximal data amount carried by them is

\[
E\left(\mathbf{t}_i^{(R)}\right) = h_i \cdot H\left(\cdots \quad \frac{t_{i,-1}}{h_i} \quad \frac{t_{i,0}}{h_i} \quad \frac{t_{i,1}}{h_i} \quad \cdots\right), \quad (13)
\]

Where \(H\) is entropy function

\[
H\left(\cdots \quad \frac{t_{i,-1}}{h_i} \quad \frac{t_{i,0}}{h_i} \quad \frac{t_{i,1}}{h_i} \quad \cdots\right) = \sum_{j=-\infty}^{+\infty} \frac{t_{i,j}}{h_i} \cdot \log \frac{h_i}{t_{i,j}}. \quad (14)
\]

Furthermore, considering the available data with new value \(j\) after data hiding, since we need to recover their original values, the minimal amount of required data is

\[
E\left(\mathbf{t}_j^{(C)}\right) = h_j \cdot H\left(\frac{t_{M_0,j}}{h_j} \quad \frac{t_{M_1,j}}{h_j} \quad \cdots \quad \frac{t_{M_2,j}}{h_j}\right) \quad (15)
\]

Thus, the data amount of pure payload is

\[
P = \sum_{i=M_0}^{M_2} E\left(\mathbf{t}_i^{(R)}\right) - \sum_{j=-\infty}^{+\infty} E\left(\mathbf{t}_j^{(C)}\right). \quad (16)
\]

As mentioned above, a data-hider always hopes to achieve a good payload-distortion performance. In the following, we will find the optimal transfer matrix \(\mathbf{T}\) to maximize the function \(P\) when meeting the constraint conditions in (2) and (3) with a given distortion level. Define a Lagrange function,

\[
L = P - \sum_{i=M_0}^{M_2} \left(\lambda_i \cdot \sum_{j=-\infty}^{+\infty} t_{i,j}\right) - \lambda \sum_{i=M_0}^{M_2} \sum_{j=-\infty}^{+\infty} |t_{i,j} \cdot d(i,j)|. \quad (17)
\]

When meeting an extremum of \(P\), for any \(t_{i,j} > 0\), there must have
Note that all the elements in $T$ are non-negative. According to (17), if both $t_{i,j}$ and $t_{i,k}$ are positive, there is

$$
\frac{\log \left( \frac{h_{i}^{j}}{h_{i}^{k}} \right)}{d(i,k) - d(i,j)} = \lambda.
$$

(19)

Based on the necessary condition given in (18), we can employ the following iterative numerical method to calculate the optimal transfer matrix.

1. Initialize

$$
T = \begin{bmatrix}
    h_{M_{1}} & 0 & \cdots & 0 \\
    0 & h_{M_{i+1}} & \cdots & 0 \\
    \vdots & \vdots & \ddots & \vdots \\
    0 & 0 & \cdots & h_{M_{t}}
\end{bmatrix},
$$

(20)

and $D = 0$, $P = 0$

2. Calculate the new histogram $H'$ by (4).

3. For each $t_{i,j} > 0$ and each $k (k \neq j, h_{i}^{j} > h_{i}^{k})$, calculate

$$
\lambda(i,j,k) = \frac{\log \left( \frac{h_{i}^{j}}{h_{i}^{k}} \right)}{d(i,k) - d(i,j)}.
$$

(21)

According to (19), the values of $\lambda(i,j,k)$ should be same in an optimal transfer matrix. So, find the largest one among all calculated $\lambda(i,j,k)$, and denote the corresponding $i,j$ and $k$ as $i^*, j^*$ and $k^*$. Update the transfer matrix

$$
t_{i^*,j^*,k^*} = t_{i^*,j^*,k^*} + \Delta,
$$

(22)

Here, $\Delta$ is a given small positive value, and the purpose of the update operation is to decrease the largest $\lambda(i,j,k)$ for equalizing all of $\lambda(i,j,k)$.

4. Calculate the distortion level $D$ and the pure payload $P$ using (8) and (16). The current $T$ is just the optimal transfer matrix for the pure payload and the distortion level. Then, go to Step 2. Using the above-described procedure, the value of the computational complexity is higher. In practice, we should make a tradeoff between the precision and computational complexity.

III. REVERSIBLE DATA HIDING SCHEME

In the proposed scheme, the host hidden data, as well the auxiliary information used for content decryption, are carried by the differences between the host pixel-values and the
corresponding values estimated from the neighbors, and the estimation errors are modified according to the optimal value transfer matrix. The optimal value transfer matrix is produced for maximizing the amount of secret data, i.e., the pure payload, by the iterative procedure described in the previous section. That implies the size of auxiliary information does not affect the optimality of the transfer matrix. By dividing the pixels in host image into two sets and a number of subsets, the data embedding is orderly performed in the subsets, and then the auxiliary information of a subset is always generated and embedded into the estimation errors in the next subset. This way, a receiver can successfully extract the embedded secret data and recover the original content in the subsets with an inverse order.

A. Data Embedding

The data embedding procedure is sketched in Fig. 1. Denote the host pixels as $p_{u,v}$, where $u$ and $v$ are indices of row and column, and divide all pixels into two sets: Set A containing pixels with even $(u+v)$ and Set B containing other pixels with odd $(u+v)$. Fig. 2 shows the chessboard-like division. Clearly, the four neighbors of a pixel must belong to the different set. For each pixel, we may use four neighbors to estimate its value,

$$ p^{(E)}_{u,v} = w_{u-1,0} \cdot p_{u-1,v} + w_{1,0} \cdot p_{u+1,v} + w_{0,u-1} \cdot p_{u,v-1} + w_{0,u+1} \cdot p_{u,v+1} \quad (23) $$

two parts: data-embedding in estimation errors of Set A, and data-embedding in estimation errors of Set B. Before data embedding in estimation errors of Set A, we first find the optimal weights with the least square error

$$ \{w_{-1,0}, w_{1,0}, w_{0,-1}, w_{0,1}\} = \arg \min_{\{w_{-1,0}, w_{1,0}, w_{0,-1}, w_{0,1}\}} \sum_{p_{u,v} \in \text{Set A}} e_{u,v}^2. \quad (24) $$

Then, the actual estimation errors are calculated according to the optimal weights and rounded the below equation

Fig 1. Sketch of data embedding procedure
where $\omega_{-1,0}, \omega_{0,1}, \omega_{0,-1}$ and $\omega_{0,1}$ are the weights, and the estimation error is

$$
\varepsilon_{u,p} = \text{round}\left[p_{u,p} - \left(\omega_{-1,0}p_{u-1,p} + \omega_{1,0}p_{u+1,p} + \omega_{0,-1}p_{u,p-1} + \omega_{0,1}p_{u,p+1}\right)\right] \quad (25)
$$

That means the pixels in Set A/B are estimated by using the pixels in B/A. The data embedding procedure is made up of

\[ \text{Let the histogram of estimation errors be } G = \{\ldots, g_{-2}, g_{-1}, g_{0}, g_{1}, g_{2}, \ldots\}, \text{ and the number of estimation errors be } N, \text{ which equals half of the size of host image.} \]

\[ \text{Generally speaking, } g_k \text{ decreases with increasing } |k|. \text{ Then, find two values } M_1 \text{ and } M_2 \text{ satisfying} \]

$$
\frac{N}{4096}, \quad g_k \leq \frac{N}{4096}, \quad k < M_1, \quad (27)
$$

and,

$$
\frac{N}{4096}, \quad g_k < \frac{N}{4096}, \quad k > M_2. \quad (28)
$$

Discard the trivial parts of the histogram on the left of $M_1$ and on the right of $M_2$, and calculate a scaled histogram in central area

$$
\hat{h}_k = \text{round}\left(\frac{g_k}{N/2048}\right), \quad M_1 \leq k \leq M_2. \quad (29)
$$

Clearly, the scaled histogram on the left of $M_1$ and on the right of $M_2$ must be zeros, therefore will be ignored. For example, when a gray scale image Lena sized 512 $\times$ 512 was used as the host, the optimal estimation weights for Set A were $\omega_{-1,0} = 0.406, \omega_{0,-1} = 0.408, \omega_{0,1} = 0.094$ and $\omega_{0,1} = 0.093$. The histogram of estimation errors $G$. 

Fig. 3. Histogram of estimation errors for Set A in Lena.
Fig. 4. Scaled histogram generated from Fig. 3.

around the diagonal. Fig. 5 gives an example of optimal transfer matrix generated from the histogram in Fig. 4 by 4.0 × 10^4 iterations, in which the extreme white represents zero and the extreme black represents the maximal value in T. The computational complexity is proportional to the iteration number, and the generation of optimal transfer matrix can be finished in several seconds by a personal computer with 2.40 GHz CPU and 3.00 GB RAM.

B. Data Extraction and Content Recovery

Then, the receiver recovers the original content and extracts the hidden data in Subset N B -1 of Set B. Since the first part of AI N B -1 contains the labels of saturated pixels and the original values of the first type of saturated pixels, the first type of saturated pixels in Subset N B -1 can be localized and their original values can be recovered. For the second types of saturated pixels and the unsaturated pixels, after calculating the probability P(ē) in (36), the receiver can convert the second part of AI N B -1 into a sequence of original estimation error by arithmetic decoding. Thus, the original pixel values are recovered as

$$p = y' - e' + e_1$$

where P' and e' are the pixel value and estimation error in received image, and e is the original estimation error. Furthermore, with the original estimation errors e and the new estimation errors e’, after calculating the probability P N(ē) in (34), the receiver can also retrieve the embedded data by arithmetic decoding.

IV. EXPERIMENTAL RESULTS

Four images, Lena, Baboon, Plane and Lake, all sized 512 × 512, shown in the host images. Both Set A and Set B were divided into 16 subsets. Since the auxiliary information of a subset is generated after data embedding and embedded into the next subset, we should ensure the capacity of a subset is more than the data amount of auxiliary information of the previous subset. This way, a receiver can successfully extract the embedded secret data and recover the original content in the subsets with an inverse order. On the other hand, the optimal transfer mechanism implemented in every subset except the last one is used to achieve a good payload-distortion performance. For the last subset, a LSB replacement method is employed to embed the auxiliary information of the second last subset and C B for content recovery with an inverse order. So, we hope the size of the last subset is small. Considering the two aspects, we make the subset sizes identical and let N A = N B = 16. In this case, the last subset occupies only 1/32 of cover data and almost does not affect the payload-distortion per
V. CONCLUSION

In order to achieve a good payload-distortion performance of reversible data hiding, this work first finds the optimal value transfer matrix by maximizing a target function of pure payload with an iterative procedure, and then proposes a practical reversible data hiding scheme. The differences between the original pixel-values and the corresponding values estimated from the neighbors are used to carry the payload that is made up of the actual secret data to be embedded and the auxiliary information for original content recovery. According to the optimal value transfer matrix, the auxiliary information is generated and the estimation errors are modified. Also, the host image is divided into a number of subsets and the auxiliary information of a subset is always embedded into the estimation errors in another subset. This way, one can successfully extract the embedded secret data and recover the original content in the subsets with an inverse order. The payload-distortion performance of the proposed scheme is excellent. For the smooth host images, the proposed scheme significantly outperforms the previous reversible data hiding methods. The optimal transfer mechanism proposed in this work is independent from the generation of available cover values. In other words, the optimal transfer mechanism gives a new rule of value modification and can be used on various cover values. If a smarter prediction method is exploited to make the estimation errors closer to zero, a best performance can be reached, but the computation complexity due to the prediction will be higher. The combination of the optimal transfer mechanism and other kinds of available cover data deserves further investigation in the future.

REFERENCES