Reversible Data Hiding Scheme Survey Paper

Anjaney Pachori
(4th Semester M.tech): Instrumentation and Control
Shri Shankaracharya Engineering College
Junwani Bhilai

Navdeep Khare
(Asst Prof): Instrumentation and Control
Shri Shankaracharya Engineering College
Junwani Bhilai

Abstract— *We have witnessed recently the development of a fast growing body of research focused on reversible data hiding scheme with various approaches with an aim to recover complete text and image. It is the aim of this paper to survey the significant advances made in reversible data hiding scheme and the different methods followed by the researchers.*

Keywords—Data Hiding; Histogram; Scheme; Image

I. Introduction

IN RECENT YEARS, MANY SCHOLARS HAVE PAID GREAT ATTENTION TO THE RESEARCH OF MULTIMEDIA INFORMATION SECURITY, ESPECIALLY FOR DIGITAL IMAGES IN MILITARY AND MEDICAL APPLICATIONS. AS AN EFFECTIVE TECHNIQUE THAT EMBEDS INFORMATION INTO IMAGES FOR COPYRIGHT PROTECTION, IMAGE HIDING SCHEMES HAS BEEN WIDELY STUDIED. DATA HIDING IS AN ART AND SCIENCE OF DATA SMUGGLING THAT COMMUNICATES INFORMATION BY CONCEALING SECRET MESSAGES THROUGH INNOCUOUS COVER MEDIA SUCH AS IMAGES, AUDIO SIGNALS, VIDEOS, DOCUMENTS AND SO ON. THE DATA HIDING PROTECTS MULTIMEDIA CONTENTS BY CONCEALMENT OF SECRET MESSAGE FROM EAVESDROPPERS UNTIL THE SECRET MESSAGE IS EXTRACTED

II. Technique

Data hiding is a technique that embeds secret data into a cover image and has a tiny impact on the image, which can be evaluated by hiding capacity and image quality. Data hiding can be divided into two categories, i.e., irreversible and reversible. Reversible data hiding (RDH) refers to embed data into cover image imperceptibility, in receiver side, not only the secret data but also cover image can be restored without any distortion. However, in irreversible data hiding schemes, cover image cannot be recovered completely.

Currently, most of reversible data hiding schemes were studied to embed the data into cover image in an imperceptible way. That is to say, the embedded data for image tagging or labeling is invisible. The existing, invisible and reversible data hiding schemes are usually based on three mechanisms, i.e., lossless compression difference expansion (DE) and histogram shifting (HS).

III. Data hiding schemes

There are many existing reversible data hiding schemes, and mainly can be classified into several categories depending on the embedding region, i.e., the spatial domain, the frequency domain compression domain, and file structure and so on. In spatial domain, Tian proposed a novel, reversible data hiding method using difference expansion (DE). However, the size of uncompressed location map is even larger than that of the secret data for many images, and thus the hiding capacity could not be controlled to some extent. After that, many improved DE methods aimed at reducing the length of the location map were presented. Kim et al. proposed a DE-based method by using the quasi-Laplace distribution of the difference values and generated a simplified location map. Ni et al. presented a reversible, histogram-based data hiding approach, which utilized the histogram of the cover image for embedding, and the changes of the pixels in the cover image were increased or decreased by 1 at most, i.e., the quality of the stego image was good. A reversible data hiding technique based on histogram modification of pixel differences was presented in. Data hiding methods based on prediction is also a worthy approach and many researchers are working in that area. Yang et al. proposed an interleaving-prediction method that utilized the correlation between adjacent pixels to generate the prediction errors used for embedding; the quality of the stego image was good for the histogram-shifting method, and it was used in the embedding process. After that, Hsu et al. proposed a data hiding scheme based on the block prediction and histogram-shifting approach and the performance was improved .Dragoi and Coltuc presented a reversible watermarking method combined local prediction and difference expansion. In the scheme, a local least squares (LS) prediction method provided a more precise prediction, and additional information was not needed for predictor restoration. Pixel-value-ordering (PVO) and prediction-error expansion (PEE) methods were introduced in. Wu et al. proposed a reversible data hiding, which employed the prediction-error of prediction error (PPE) of a pixel to embed the secret data. The scheme achieved a good payload-distortion performance by using a good predictor and pixel selection approach.

In frequency domain, Xuan et al. proposed reversible data hiding using integer wavelet transform (IWT) and companding technique, which solved the problem of overflow/underflow after the inverse IWT .Chan et al. proposed a Haar digital wavelet transform (HDWT)-based reversible data hiding method, which embedded the secret data and compressed extra payload in the n least significant bits of integer part of the high frequency. A similar data Multimed Tools Applhiding method with Chan et al.'s was presented in, and it had proved good performance.

Lin proposed a reversible data hiding method, embedding secret data by exploiting the histogram-shifting method based on DCT coefficients, however, the problem of overflow/underflow was not solved in the proposed scheme. A two-dimensional difference expansion (2D–DE) scheme with a characteristics-based threshold was presented in. In the scheme, a threshold, which based on the standard deviation, was used to adjust the hiding capacity, meantime, the visual quality was enhanced. Mao et al. presented a distortion oriented, minimized, reversible data hiding method. In Mao et al.'s scheme, a cascading trellis coding algorithm was proposed, and also, the proposed scheme was employed in discrete wavelet transform (DWT) domain. Although a lot of research work has been done to demonstrate the good performance of the existing schemes in the frequency domain, many problems still exist, such as the tradeoff between hiding capacity and the quality of the stego image.

In compression domain, Fridrich proposed a lossless data hiding method for JPEG images. However, the hiding capacity was limited and the distortion of the method was large. A reversible hiding scheme that concealed secret data in the block of quantized discrete cosine transformation (DCT) coefficients of JPEG images was presented in. Qian proposed a loss data embedding approach into JPEG bit stream by Huffman code mapping, which increased the embedding capacity and preserved the image quality. Huang et al. presented a new Histogram Shifting (HS)-based reversible data hiding scheme in JPEG images, in the scheme, there was a good balance between the hiding capacity and visual quality, meanwhile, the storage size was well preserved. Some RDH schemes are based on file structure, for instance, Luo et al. presented a reversible data hiding method based on inter-view local texture analysis. By analyzing the texture similarity of matched pixels, a more accurate prediction was achieved. A reversible data hiding algorithm using texture synthesis was proposed in.

Here are some reversible data hiding scheme discussed in detail:-

A reversible data hiding scheme based on the Haar discrete wavelet transform (DWT) and interleaving-prediction method-

First, a one-level Haar discrete wavelet transform (DWT) is implemented to the cover image, and four sub-bands, LL , HL , LH and HH, are obtained. Sub-bands HL,LH and HH are chosen for embedding. After that, the wavelet coefficients of the chosen sub-bands are zig-zag scanned and two adjacent coefficients are used for prediction. The secret data is embedded in the prediction errors, which is the difference between the original value and the predicted value of the wavelet coefficients.

1.1 Framework of the proposed scheme-

The main idea of our proposed scheme is to embed secret data into wavelet coefficients using interleaving-prediction and histogram-shifting techniques after a zig-zag scan of the chosen wavelet sub-bands, which can be obtained by applying the Haar DWT to the cover image. The framework of the data hiding scheme is shown in following Figure. For the data embedding procedure, first, we modify the histogram of the cover image in case of overflow/underflow caused by the inverse Haar DWT after the embedding secret data; the modified information is recorded as a part of the overhead.

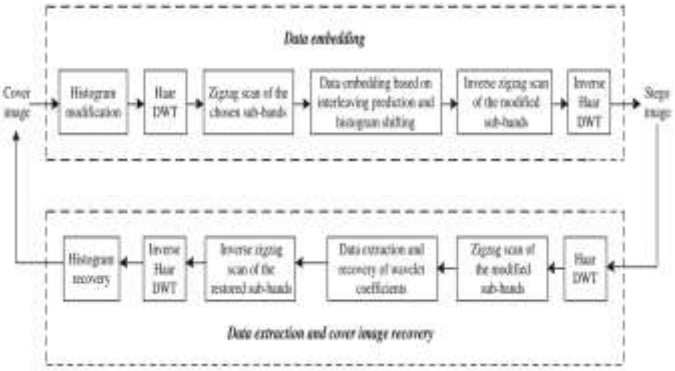
Data embedding
Cover image
Histogram modification
Haar DWT
Zigzag scan of the chosen sub-bands
Data embedding based on interleaving prediction and histogram shifting
Inverse zigzag scan of the modified sub-bands
Inverse Haar DWT
Stego image
Histogram recovery
Inverse Haar DWT
Inverse zigzag scan of the restored sub-bands
Data extraction and recovery of wavelet coefficients
Zigzag scan of the modified sub-bands
Haar DWT
Data extraction and cover image recovery

Fig. 1. Framework of the data hiding scheme

Actually, there is very small or even no overflow/underflow for many images. After that, one-level HDWT is applied to the cover image and the suitable wavelet sub-bands are chosen to embed secret data using interleaving-prediction and histogram-shifting methods after zig-zag scan of the chosen sub-bands. For the data extraction and cover image recovery procedure, one-level Haar DWT is applied to the stego image, and the secret data and overhead information are extracted from the modified wavelet sub-bands. In this way, we can restore the modified wavelet coefficients, i.e., wavelet sub-bands. And thus, the cover image is restored by using inverse Haar DWT and histogram recovery.

1.2 Histogram modification

After embedding secret data and overhead information into the wavelet sub-bands, overflow/underflow may occur when the modified wavelet sub-bands in the frequency domain are transformed to the image in spatial domain. That is to say, the pixels may be greater than 255 or less than 0, especially those pixels closer to 0 or 255.

In the paper, we use the histogram modification method to control overflow/ underflow, and an adaptive T is used in the approach. T is an empirical value, which varies from different images. The grayscale values of pixels between 0 and T are incremented by T, and the grayscale values of pixels between 255 - T and 255 are decreased by T to ensure that no overflow/underflow occurs. In addition, there is a location map to record the shifting information, and the location map is embedded as a part of the overhead information

1.3 Data embedding

In this section, we propose our data hiding scheme based on the interleaving prediction and histogram-shifting Techniques. The definition of a zig-zag scan is presented first, and, then, we clarify the embedding algorithm; last, an example of the embedding algorithm is described.

1.3.1 Zig-Zag scan

Zig-zag scan is a matrix scan approach that scans the matrix values from the top-left to the bottom-right with Z-shaped arrangement and changes the two-dimensional (2D) matrix into a one-dimensional (1D) vector. Here, we use the zig-zag scan for the chosen wavelet sub-bands to achieve more accurate prediction, which depends on the correlation between the diagonal elements.

1.3.2 Embedding algorithm

Assume that the size of cover image C is m × n and that the secret data $S = \{si|si = \{0, 1\}, i \in Z\}$ is a binary sequence. After histogram modification and one-level Haar DWT, the cover image is decomposed into the frequency domain, and four sub-bands, i.e., LL, HL, LH and HH, are obtained. And each size of the four wavelet sub-bands is m/2 × n/2. Since the LL sub-band represents the approximation information of the cover image, tiny changes may cause great impact on the cover image. We choose the HL, LH and HH sub-bands in our scheme to embed the secret data.

3.4 Data extraction and cover image recovery

In this section, we deal with the stego image to extract the embedded secret data and overhead information; after that, we restore the cover image. Note that the direction of the interleaving-prediction is opposite from the data embedding procedure, i.e., in the data extraction procedure, we use wavelet coefficients in odd columns to

predict coefficients in even columns first, and then wavelet coefficients in even columns to predict coefficients in odd columns.

Dual image based reversible data hiding scheme using (7,4) hamming code

In this Technique, a new dual-image based reversible data hiding scheme is proposed through (7,4) Hamming code (RDHHC) using shared secret key. A block of seven pixels are collected from cover image and copied into two arrays then it is adjusted redundant Least Significant Bits (LSBs) using odd parity such that any error creation is encountered at the sender end and recovered at the receiver end. Before data embedding, we first complement the bit at shared secret position. After that, secret message bit is embedded by error creation caused by tamper in any suitable position except secret position and that error is detected as well as corrected at the receiver end using Hamming error correcting code. One shared secret position κ and one shared secret key ξ help to perform data embedding, data extraction and recovery of the original image. The secret data and original cover image are successfully recovered at the receiver end from dual stego image. Finally, we compare our scheme with other state-of-the-art methods and obtain reasonably better performance in terms of PSNR.

1 Proposed RDH scheme using (7, 4) hamming code (RDHHC)

We introduce a dual-image based reversible data hiding scheme using (7, 4) Hamming code. The schematic diagram of data embedding process is depicted in Fig. 1. The diagram of secret data extraction and cover image reconstruction process is shown in Fig. 2. The corresponding pseudo code for data embedding and data extraction are given in Algorithm 1 and Algorithm 2 respectively. In the following, we first describe data embedding technique. Then, we describe the data extraction and cover image recovery technique.

1.1 Data embedding process

We first collect 7 consecutive pixels from the cover image. We collect LSBs of those pixels and copy it into two arrays M and A. Then we adjust redundant bits of both arrays separately using odd parity check. The redundant bits r1, r2 and r3 of M array are adjusted based on the number of 1s present in the bit positions which are mentioned in index 1 of Fig. 1. For example, the r1 bit is set to 1 if the number of 1 present in the bit positions at 3, 5 and 7 of M

array are even. The redundant bits r1 and r2, r3, r4 of A array are also adjusted and updated in the bit positions at 3, 5, 6 and 7 of A array depending on the number of 1 presents in the bit position mention in index 2

1.2 Data extraction and cover image recovery process

To extract the secret data, we first apply the secret key ξ = (ξ0ξ2 . . . ξl)2 to rearrange 7 pixels as a block. If ξi = 1 then selected block from SM is stored in SMi and block from SA is in SAi; otherwise, block from SM is stored in SAi and block from SA is in SMi.Now, we collect LSBs of seven consecutive pixels from both the stego images SMi and SAi.

We then complement the bit at the shared secret position κ of the SMi. After that, we apply the Hamming error correcting code to find out the error position (ω). Next, we extract the secret data bit from the ω position and complement the bit at that position. The redundant bits of SMi stego image are considered as per index 1 in Fig. 3. The error position of SMi is the data embedding position which is used as the secret position for SAi image. We complement the bit at the secret position in SAi then we find out the error using Hamming error correcting code. The redundant bits in index 2 of Fig. 3 are consider for SAi image.Now, the secret position κ is updated for the next block using the formula κi+1 = ((κi ×ω) mod 7)+ 1, where ω is the data embedding position of SAi (here it is 3 in Fig. 3) and κ0 is the shared secret key. After extracting the secret message bits from dual stego images, we complement all the corresponding data embedding positions, which will generate hamming adjusted cover image. There are few particular special cases may happen when no error will be found. In that situation, we will first check the LSB values and follow the condition given below.

For all the cases, we need not to complement the bit at ω-th location after extraction. If SMi=0 and find no error then extract D = 0 and set ω =1 For all other cases, if error find at the position of κ that means when ω is equal to κ then

data extraction process will be stopped. It is possible when no data bit is embedded means Multimed Tools Appl

no error has been created by sender then if receiver try to extract secret data after error creation at the secret position κ then obviously κ position will be the only error creation position which is equal with the data embedding position ω. This is the condition to find the end of secret message. As a result, we can send any arbitrary length of secret data using this scheme. Finally, we can reconstruct the original cover image from both the Hamming adjusted dual stego image. We collect the bits from the bit positions at 3, 5, 6 and 7 of SMi and bits from the bit positions at 1, 2 and 4 of SAi. After that, we rearrange all the collected bits to construct the original cover image. The algorithm for data extraction and cover image reconstruction is described in Algorithm 2. The time complexity of data extraction algorithm is also O(mn) for cover image of size (m × n).

Authenticable reversible data hiding scheme with less distortion in dual stego-images

1.1 EMD (Exploiting Modification Directions)-based data hiding method

Zhang and Wang proposed the exploiting modification directions (EMD) method, where the n secret bits are embedded in the (2n + 1) –ary notational system [19]. Assume that each group is segmented into L bits and the decimal value of embedding secret bits is represented by K digits in a sub-group (p(0, 0), p(0, 1), … , p(0, n - 1)), L = ⌊K x log2(2n + 1)⌋ can be obtained and the difference value s = d - F is calculated. In here, the modulus function F as a weighted sum modulo (2n + 1) is calculated for a secret digit d.

$$F = F(p_1, p_2, \ldots, p_n) = \left[\sum_{i=1}^{n} (p_i \times i)\right] mod\ (2n+1)$$

The EMD embedding procedure is considered for three cases as follows.

& Case 1: The value does not modify for F = d.

& Case 2: The value of pn is increased by 1for F ≠ d and s ≤ n.

& Case 3: The value of p2n + 1 - s is decreased by 1 for F ≠ d and s > n.

The secret digit d is extracted from the sub-group of stego-image, (p01; p02; …; p0n).

$$d = F\left(p_1', p_2', \ldots, p_n'\right) = \left[\sum_{i=1}^{n} \left(p_i' x\, i\right)\right] mod(2n+1)$$

In many previous works based on the EMD method which does not utilize the concept of dual images, the secret data can be extracted but the cover image cannot be recovered. The important advantage using dual stego-images is that the EMD-based methods can be also reversible data hiding by using dual stego-images. In the next section, previous reversible data hiding methods based on dual images are reviewed.

2.2 Dual image-based reversible data hiding methods

Chang et al. proposed a reversible data hiding method based on the EMD in dual images [1].

The modulus function M is modified to increase embedding capacity.

$$M = M(p_1, p_2) = (2\,x\,p_1 + p_2)\ mod\ 5$$

3 Research methods

The proposed method is based on horizontal and vertical directions to keep the reversibility, and difference values of neighboring pixels are used to maintain a good image quality.

3.1 Embedding algorithm

First, two stego-images S1 = {c1(1, 1), c1(1, 2), … , c1(w, h)} and S2 = {c2(1, 1), c2(1, 2), … ,c2(w, h)} are generated from the cover image C = {c(1, 1), c(1, 2), … , c(w, h)}, where w and h are the width and height of image respectively. The number of secret bits k to be embedded is taken and converted into secret digits d = d1d2 for corresponding two pixel pairs (c(i, j) , c(i, j + 1)). The modulus function M is defined as eq. (3).

$$M = M\left(c_{(i,j)}, c_{(i,j+1)}\right) = \left(2\,x\,c_{(i,j)} + c_{(i,j+1)}\right)\ mod\ 5$$

A new pixel pair can be calculated by the modulus function from the cover pixel pair (c(i, j) , c(i, j + 1)). Two pixel pairs can be obtained from and in horizontal direction, and in vertical direction respectively.

New two pixel pairs are finally selected for corresponding pixel pairs, where two smaller values of G are pivoted.

To provide the data integrity, two pixel pairs, and are modified as follows. First, four pixel values are changed into binary values as x7x6x5x4x3x2x1x0, y7y6y5y4y3y2y1y0, z7z6z5z4z3z2z1z0, and v7v6v5v4v3v2v1v0 in order.

Next, a new stream of three-bit v2v1v0 are calculated where the XOR(·) is an exclusive-or operation

3.2 Extracting and recovering algorithm

In extracting and recovering algorithm, the parity bits checking step is firstly applied to inspect whether the bit errors were occurred or not using eq.

$$\begin{cases} v_2' = XOR\left(c_{1_{(i,j)}}', v_2\right) \\ v_1' = XOR\left(c_{1_{(i,j+1)}}', v1\right) \\ v_0' = XOR\left(c_{2_{(i,j)}}', v_0\right) \end{cases}$$

The pixel pair of the cover image can be recovered from two-pixel pairs and of the stego-images.

$$\left(c_{(i,j)}, c_{(i,j+1)}\right) = \left(\frac{c_{1_{(i,j)}}' + c_{2_{(i,j)}}'}{2}, \frac{c_{1_{(i,j+1)}}' + c_{2_{(i,j+1)}}'}{2}\right)$$

Generalized PVO-K Embedding Technique for Reversible Data Hiding

1.1 RDH Method Based On PVO

The PVO method proposed by Li et al. provided a new predictor for the prediction error expansion, with both largest and smallest pixel values being used in a block for embedding data. The embedding process is firstly divide the cover image into blocks of pixels, and number the pixels in each block, i.e.,(x1; x2; :::; xn1×n2). Then, sort the pixels in ascending order to get an ordered sequence (xπ(1); xπ(2); :::; xπ(n1×n2)).

After that, count two prediction errors according Equation (1), wherein, the non-negative integer dmax represents the difference between the largest pixel value and the second-largest pixel value; and a non-positive integer dmin represents the difference between the smallest pixel value and the second-smallest pixel value.The secret message b 2 f0; 1gcan be embedded when the maximum prediction error is 1 or the minimal prediction error is -1. Prediction errors are modified according to Equation (2)and Equation (3).At last, revise the largest and smallest pixel values using Equation (4) and proceed to the next block until all blocks have been processed or all secret data have been embedded

$$\begin{cases} d_{\max} = x_{\pi(n1\times n2)} - x_{\pi(n1\times n2-1)} \\ d_{\min} = x_{\pi 1} - x_{\pi 2} \end{cases} \tag{1}$$

$$d'_{\max} = \begin{cases} d_{\max}\ if d_{\max}{=}0 \\ d_{\max}{+}b\ if d_{\max}{=}\,1 \\ d_{\max}{+}1\ if d_{\max} > 1 \end{cases}, \tag{2}$$

$$d'_{\min} = \begin{cases} d_{\min}\ if d_{\min}{=}0 \\ d_{\min} - b\ if d_{\min}{=}-1 \\ d_{\min} - 1\ if d_{\min} < -1 \end{cases}. \tag{3}$$

$$\begin{matrix} x'_{\pi(n1\times n2)} = x_{\pi(n1\times n2-1)} + d'_{\max} \\ x'_{\pi(1)} = x_{\pi(2)} + d'_{\min} \end{matrix}\ . \tag{4}$$

Because the order of the pixel values remains unchanged after embedding the secret data, the secret data can be extracted in the extraction phase from the largest valued and smallest-valued pixels according to reverse process of the embedding procedure. At the same time, the pixel values can be changed back to the original values.

1.2 RDH Method Based On PVO-K

Like IPVO, PVO-K also was proposed for the purpose of using the prediction error \0", which is discarded in the PVO method, but the difference is that PVO-K treats the largest or smallest pixel values as a unit for embedding secret data. Similar to these methods, we take the procedure of embedding secret data into a maximum number of pixels as an example; assume that the sorted pixel values in a block are:xπ(1) ≤ ::: ≤ xπ(n1×n2-K) < x π(n1×n2-K+1) = ::: = xπ(n1×n2),where K is the number of largest-valued pixels, and the prediction error is calculated using Equation (5)

$$d_{\max} = x_{\pi(n1\times n2-K+1)} - x_{\pi(n1\times n2-K)}. \qquad (5)$$

When the prediction error is \1", one bit of secret data can be embedded; otherwise, the K pixel values are shifted. The prediction errors are modified by Equation (6).

$$d'_{\max} = \begin{cases} d_{\max}+b \; if d_{\max}=1 \\ d_{\max}+1 \; if d_{\max}>1 \end{cases} . \qquad (6)$$

Then the largest pixel values are modified by Equation (7), where, i 2 fn1 × n2 - K + 1; n1 × n2 - K + 2; :::; n1 × n2g.

$$x'_{\pi(i)} = x_{\pi(i)} + d'_{\max}. \qquad (7)$$

The common factor of PVO-K and other PVO-based methods is that the original block sorting remains constant after embedding the secret data, which makes the extraction process more convenient.

2 Proposed Scheme

In this section, we propose a generalized scheme for the PVO-K method with respect to embedding capacity, and it is called GePVO-K. First, we introduce how to embed one bit of secret data in each largest-valued pixel by modifying the largest and the second-largest pixel values. Some examples are provided to demonstrate our approach. Then, the process of embedding secret data in each smallest-valued pixel is presented. Finally, we show the detailed steps of the embedding and extraction procedures.

2.1 Embedding Secret Data in Largestvalued Pixels and Data Extraction

Procedure

As mentioned in the previous sections, if the PVO-K algorithm embeds one bit of secret data in a block that has K largest-valued or smallest-valued pixels, all of the K pixels must be modified in the same way. Ou et al. [15] indicated that when PVO-1 and PVO-2 are used together to increase the embedding capacity of traditional PVObased methods; however if K > 2, the block should not be used to embed secret data, because a larger K will lead to a greater distortion caused by more changes in the pixels values. In nature images, especially in the blocks of the smooth region, K is often greater than 2, so the smooth region always is ignored, which makes less embedding capacity. For this phenomenon, we propose an improved method that still utilizes the largest-valued and smallestvalued pixels in the block to embed secret data, but one bit of secret data can be embedded in each pixel. Here, we present the details of embedding secret data in the largest-valued pixels as well as the extracting procedure.

2.1.1 Embedding Secret Data in Largest-valued Pixels

First, the cover image should be divided into blocks. Let the size of block B be n1 ×n2. Then, each block is visited in a zigzag manner to establish a location map, and the rules for establishing the map are as follows. If the block has the pixel values that may overflow/underflow, such as "0," "1," "254," "255," the block's position is recorded as "2;" if all of the pixel values in the block are the same, the block's position is recorded as "1;" the remaining blocks are normal blocks, and their positions are recorded as "0s."

2.1.2 Extracting Secret Data from Larger valued Pixels and Restoring the Pixel Values

As can be seen from Equation (11), for a normal block (i.e., its recorded number in the location map is 0), the original ordering may be changed after the secret data have been embedded. Because some largest-valued pixel of the original block may become the second-largest after embedding the secret data, so, in the camouflage block, information can be hidden only in the largest-valued or the second-largest pixels. We can determine whether the secret data are completely hidden in the largest-valued pixels or in both the largest-valued and the second-largest pixels. Therefore, we can completely extract the secret data revise the pixel values

Comparisons

There are 4 schemes of reversible data hiding discussed above in the Haar discrete wavelet transform the zig-zag scan takes advantage of the characteristics of chosen wavelet sub-bands and ensures a more accurate prediction, in the second approach which uses (7,4) hamming code to enhance the security, the secret information is distributed among dual image with the help of shared secret key in the third approach a modulus function was used to generate stego-images and to recover the cover image from the two stego-images, and the gap function was also used to obtain dual stego-images with less distortion and finally in the fourth approach PVO (pixel value ordering) technique has been proposed embeds the data in each of the largest-valued and smallest-valued pixels and therefore, the maximum embedding capacity improves significantly. All the four schemes try to improve the quality, security of the image, make it distortion less and increase the message carrying capacity of the image sent.

Conclusions and Future Work

Due to rising use of the social media, the compressed techniques are always used in the process of uploading images. Due to this hiding embedded secret data in the compressed images is becoming more popular. In this paper, we sort out the basic prerequisites in data hiding for compressed images and compare four representative methods with different hiding techniques. The future development depends on the capacity requirement. How to embed more secret data with the analogous bit-rates is the challenging issue. A good tradeoff between the hiding capacity and image quality is achieved in the above discussed schemes. Work is still on in the above discussed scheme to improve the quality and efficiency of the signal images sent. The demand of reversible data hiding will only increase as the use of social media and internet at large comes to access to more and more people around the world.

REFERENCES

[1] Reversible data hiding scheme based on the Haar discrete wavelet transform and interleaving prediction method Fan Li1 & Qian Mao1 & Chin-Chen Chang2

[2] Dual image based reversible data hiding scheme using (7,4) hamming code Biswapati Jana1 · Debasis Giri2 ·Shyamal Kumar Mondal

[3] Authenticable reversible data hiding scheme with less distortion in dual stego-images Ki-Hyun Jung

[4] Generalized PVO-K Embedding Technique for Reversible Data Hiding Jian-Jun Li1, Yun-He Wu1, Chin-Feng Lee2 and Chin-Chen Chang

[5] Alattar AM (2004) Reversible watermark using the difference expansion of a generalized integer transform.IEEE Trans Image Process 13(8):1147–1156

[6] Al-Qershi OM, Khoo BE (2013) Two-dimensional difference expansion (2D-DE) scheme with a characteristics-based threshold. Signal Process 93(1):154–162

[7] Al-Qershi OM, Khoo BE (2014) Controlling hiding capacity using image characteristics with a 2D-DE data hiding scheme. AEU Int J Electron Commun 68(4):346–350

[8] Calderbank AR, Daubechies I, Sweldens W, Yeo BL (1998) Wavelet transforms that map integers to integers. Appl Comput Harmon Anal 5:332–369

[9] Chan YK, Chen WT, Yu SS, Ho YA, Tsai CS, Chu YP (2009) A HDWT-based reversible data hiding method. J Syst Softw 82(3):411–421

[10] Chang CC, Lin CC, Tseng CS, Tai WL (2007) Reversible hiding in DCT-based compressed images. Inf Sci 177(13):2768–2786

[11] Chang CC, Chou YC, Kieu D (2008) An information hiding scheme using Sudoku. In: The 3rd Int Conf on Innovative Computing Information and Control. Liaoning, Dalian

[12] Chang CC, Pai PY, Yeh CM, Chan YK (2010) A high payload frequency-based reversible image hiding method. Inf Sci 180(11):2286–2298

[13] Chen B, Zhang WM, Ma KD, Yu NH (2014) Recursive code construction for reversible data hiding in DCT domain. Multimed Tools Appl 72:1985–2009

[14] Chui CK (ed) (1992) Wavelets: a tutorial in theory and applications. Academic, San Diego

[15] Daubechies I, Sweldens W (1998) Factoring wavelet transforms into lifting steps. J Fourier Anal Appl 4(3):351–353

[16] Dragoi IC, Coltuc D (2014) Local-prediction-based difference expansion reversible watermarking. IEEE Trans Image Process 23(4):1779–1790

[17] Fridrich J, Goljan M, Du R (2002) Lossless data embedding for all image formats. In: Proc. SPIE, pp 572–583

[18] Hsu FH, Wu MH, Yang CH, Wang SJ (2014) Image reversibility in data embedding on the basis of blocking-predictions. Peer-to-Peer Networking Appl 7(4):723–736

[19] Huang FJ, Qu XC, Kim HJ, Member HJW (2016) Reversible data hiding in JPEG images. IEEE Trans Circuits Syst Video Technol 26(9):1610–1621

[20] Ker A (2005) Improved detection of LSB steganography in grayscale images. Inf Hiding Lect Notes Comput Sci 3200:97–115

[21] Kim HJ, Sachnev V, Shi YQ, Nam J, Choo HG (2008) A novel difference expansion transform for reversible data embedding. IEEE Trans Inf Forensics Secur 4(3):456–465

[22] Li X, Yang B, Zeng T (2011) efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection. IEEE Trans Image Process 3524–3533

[23] Lin CC, Tai LW, Chang CC (2008) Multilevel reversible data hiding based on histogram modification of difference images. Pattern Recogn 41(12):3582–3591

[24] Lin CC, Tai LW, Chang CC (2008) Multilevel reversible data hiding based on histogram modification of difference images. Pattern Recogn 41(12):3582–3591

[25] Lin YK (2012) High capacity reversible data hiding scheme based upon discrete cosine transformation. J Syst Softw 85(10):2395–2404

[26] Luo T, Jiang GY, Yua M, Xu HY, Shao F (2016) Inter-view local texture analysis based stereo image reversible data hiding. Digital Signal Process 48:116–129

[27] Mao Q, Li F, Chang CC (2015) Reversible data hiding with oriented and minimized distortions using cascading trellis coding. Inf Sci 317:170–180

[28] Mielikainen J (2006) LSB matching revisited. IEEE Signal Process Lett 13(5):285–287

[29] Ni Z, Shi YQ, Ansari N, Su W (2006) Reversible data hiding. IEEE Trans Circuits Syst Video Technol 16(3):354–362

[30] Qian Z, Zhang X (2012) Lossless data hiding in JPEG bitstream. J Syst Softw 85(2):309–313

[31] Shen SY, Huang LH (2015) A data hiding scheme using pixel value differencing and improving exploiting modification directions. Comput Secur 48:131–141

[32] Tai WL, Yeh CM, Chang CC (2009) Reversible data hiding based on histogram modification of pixel differences. IEEE Trans Circuits Syst Video Technol 19(6):906–910

[33] Thodi DM, Rodriguez JJ (2007) Expansion embedding techniques for reversible watermarking. IEEE Trans Image Process 16(3):721–730

[34] Tian J (2003) Reversible data embedding using a difference expansion. IEEE Trans Circuits Syst Video Technol 13(8):890–896

[35] Tsai P, Hu YC, Yeh HL (2009) Reversible image hiding scheme using predictive coding and histogram shifting. Signal Process 89(6):1129–1143

[36] Tseng HW, Hsieh CP (2009) Prediction-based reversible data hiding. Inf Sci 179(14):2460–2469

[37] Vignesh Kumar PR (2016) Reversible data hiding using texture synthesis approach. International Conference on Circuit, Power and Computing Technologies [ICCPCT]

[38] Wu HZ, Wang HX, Shi YQ PPE-based reversible data hiding. IH&MMSec '16 Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security, pp. 187–188

[39] Xuan G, Yang C, Zhen Y, Shi Y, Ni Z (2005) Reversible data hiding using integer wavelet transform and companding technique. Digital Watermarking Lect Notes Comput Sci 3304:115–124

[40] Yang HC, Tsai HM (2010) Improving histogram-based reversible data hiding by interleaving predictions. IET Image Process 4(4):223–234

[41] Zhang X, Wang S (2006) Efficient steganographic embedding by exploiting modification direction. IEEE Commun Lett 10(11):1–3

[42] Chang CC, Chou YC (2009) Information hiding in dual images with reversibility. In: 2009 Third

[43] International Conference on Multimedia and Ubiquitous Engineering. IEEE, pp 145–152

[44] Chang CC, Kieu TD, Chou YC (2007) Reversible data hiding scheme using two steganographic images. In: TENCON 2007-2007 IEEE Region 10 Conference. IEEE, pp 1-4

[45] Chang CC, Kieu TD, Chou YC (2008) A high payload steganographic scheme based on (7, 4) hamming code for digital images. In: 2008 International Symposium on Electronic Commerce and Security. IEEE, pp 16–21

[46] Chang CC, Lu TC, Horng G, Huang YH, Hsu YM (2013) A high payload data embedding scheme using dual stego-images with reversibility. In: Communications and Signal Processing (ICICS) 2013 9th International Conference on Information. IEEE, pp 1–5

[47] Fridrich J, Goljan M, Du R (2001) Invertible authentication. In: Photonics West 2001-Electronic Imaging (pp. 197-208). International Society for Optics and Photonics

[48] Fu MS, Au OC (2001) Halftone image data hiding with intensity selection and connection selection. Signal Process Image Commun 16(10):909–930

[49] Kim HJ, Kim C, Choi Y, Wang S, Zhang X (2010) Improved modification direction methods. Comput Math Appl 60(2):319–325

[50] Kim C, Shin D, Shin D (2011) Data hiding in a halftone image using hamming code (15, 11). In:Intelligent Information and Database Systems. Springer, Berlin Heidelberg, pp 372–381

[51] Kieu TD, Chang CC (2011) A steganographic scheme by fully exploiting modification directions. Expert Syst Appl 38(8):10648–10657

[52] Lee CF, Huang YL (2013) Reversible data hiding scheme based on dual stegano-images using orientation combinations. Telecommun Syst 52(4):2237–2247

[53] Lee CF, Chen HL (2012) Adjustable prediction-based reversible data hiding. Digit Signal Process 22(6):941–953

[54] Lee CF, Chen HL, Tso HK (2010) Embedding capacity raising in reversible data hiding based on prediction of difference expansion. J Syst Softw 83(10):1864–1872

[55] Lee CF, Wang KH, Chang CC, Huang YL (2009) A reversible data hiding scheme based on dual steganographic images. In: Proceedings of the 3rd International Conference on Ubiquitous Information Management and Communication. ACM, pp 228–237

[56] Lien BK, Chen SK, Wang WS, King KP (2015) Dispersed data hiding using hamming code with recovery capability. In: Genetic and Evolutionary Computing. Springer International Publishing, pp 179–187

[57] Lien BK, Lin YM (2011) High-capacity reversible data hiding by maximum-span pairing. Multimed Tool Appl 52(2-3):499–511

[58] Liao PS, Pan JS, Chen YH, Liao BY (2005) A lossless watermarking technique for halftone images. In: Knowledge-Based Intelligent Information and Engineering Systems. Springer, Berlin Heidelberg, pp 593-599

[59] Lu ZM, Luo H, Pan JS (2006) Reversible watermarking for error diffused halftone images using statistical features. In: Digital Watermarking. Springer, Berlin Heidelberg, pp 71–81Multimed Tools Appl

[60] Lu TC, Tseng CY, Wu JH (2015) Dual imaging-based reversible hiding technique using LSB matching.Signal Process 108:77–89

[61] MA ZP, LI FY, Zhang XP (2013) Data hiding in halftone images based on hamming code and slave pixels. Journal Shanghai University (Natural Science Edition) 2:003

[62] Ni Z, Shi YQ, Ansari N, Su (2006) Reversible data hiding. IEEE Trans Circuits Syst Video Technol 16(3):354–362

[63] Pan JS, Luo H, Lu ZM (2006) A lossless watermarking scheme for halftone image authentication. Int J Comput Sci Netw Secur 6(2b):147–151

[64] Qin C, Chang CC, Hsu TJ (2015) Reversible data hiding scheme based on exploiting modification direction with two steganographic images. Multimed Tool Appl 74(15):5861–5872

[65] Tian J (2003) Reversible data embedding using a difference expansion. IEEE Trans Circuits Syst Video Techn 13(8):890–896

[66] Tseng HW, Hsieh CP (2009) Prediction-based reversible data hiding. Inf Sci 179(14):2460–2469

[67] Westfeld A (2001) F5a steganographic algorithm. In: Information Hiding. Springer, Berlin Heidelberg,pp 289–302

[68] Yu FX, Luo H, Chu SC (2009) Lossless data hiding for halftone images. In: Information Hiding and Applications. Springer, Berlin Heidelberg, pp 181–203

[69] Chang CC, Kieu TD, Chou YC (2007) Reversible data hiding scheme using two steganographic images. Proceedings of IEEE Region 10 International Conference (TENCON) pp 1–4

[70] Chang CC, Chou YC, Kieu TD (2009) Information hiding in dual images with reversibility. Proceedings of the 3rd International Conference on Multimedia and Ubiquitous Engineering pp 145–152 37.00 40.00 43.00 46.00 49.00 52.00 55.00 58.00 61.00 64.00 15,000 5,000 115,000 165,000 215,000 265,000 315,000 365,000 415,000 465,000 515,000

[71] Lu et al.'s method [11] : 1st stego-image Lu et al.'s method [11] : 2nd stego-image Chang et al.'s method [6] : 1st stego-image

[72] Chang et al.'s method [6] : 2nd stego-image Chang et al.'s method [7] : 1st stego-image Chang et al.'s method [7] : 2nd stego-image

[73] Chang et al.'s method [8] : 1st stego-image Chang et al.'s method [8] : 2nd stego-image The proposed method : 1st stego-image

[74] The proposed method : 2nd stego-image The proposed method : stego-image with authentication on Embedding Capacity PSNR dB bits

[75] Lu et al.'s method [11] : 1st stego-image Lu et al.'s method [11] : 2nd stego-image Chang et al.'s method [6] : 1st stego-image

[76] Chang et al.'s method [6] : 2nd stego-image Chang et al.'s method [7] : 1st stego-image Chang et al.'s method [7] : 2nd stego-image

[77] Chang et al.'s method [8] : 1st stego-image Chang et al.'s method [8] : 2nd stego-image The proposed method : 1st stego-image

The proposed method : 2nd stego-image The proposed method : stego-image with authentication on Embedding Capacity PSNR dB bits (a) Airplane (b) Baboon

[78] Lu et al.'s method [11] : 1st stego-image Lu et al.'s method [11] : 2nd stego-image Chang et al.'s method [6] : 1st stego-image

[79] Chang et al.'s method [6] : 2nd stego-image Chang et al.'s method [7] : 1st stego-image Chang et al.'s method [7] : 2nd stego-image

[80] Chang et al.'s method [8] : 1st stego-image Chang et al.'s method [8] : 2nd stego-image The proposed method : 1st stego-image

[81] The proposed method : 2nd stego-image The proposed method : stego-image with authentication on Embedding Capacity PSNR dB bits 37.00

[82] Lu et al.'s method [11] : 1st stego-image Lu et al.'s method [11] : 2nd stego-image Chang et al.'s method [6] : 1st stego-image

[83] Chang et al.'s method [6] : 2nd stego-image Chang et al.'s method [7] : 1st stego-image Chang et al.'s method [7] : 2nd stego-image

[84] Chang et al.'s method [8] : 1st stego-image Chang et al.'s method [8] : 2nd stego-image The proposed method : 1st stego-image

[85] The proposed method : 2nd stego-image The proposed method : stego-image with authentication on Embedding Capacity PSNR dB bits (c) Lena d) Man Fig. 12 Performance comparison of PSNR with embedding capacity

[86] Multimed Tools Appl3. Chang CC, Lu TC, Horng G, Huang YH, Hsu YM (2013) A high payload data embedding scheme usingdual stego-images with reversibility. Proceedings of the 3rd International Conference on Information, Communications and Signal Processing pp 1–5

[87] Cheddad A, Condell J, Curran K, Kevitt PM (2010) Digital image steganography: survey and analysis of current methods. Signal Process 90:727–752

[88] Huang HC, Chang FC (2013) Hierarchy-based reversible data hiding. Expert Syst Appl 40(1):34–43

[89] Huang HC, Chang FC, Fan WC (2011) Reversible data hiding with histogram-based difference expansion for QR code applications. IEEE Trans Consumer Electronics 57(2):779–787

[90] Jana B (2016) High payload reversible data hiding scheme using weighted matrix. Optik 127:3347–3358

[91] Jung KH, Yoo KY (2015) Steganographic method based on interpolation and LSB substitution of digital images. Multimedia Tools and Applications 74(6):2143–2155

[92] Khan A, Siddiqa A, Munib S, Malik SA (2014) A recent survey of reversible watermarking techniques. Inf Sci 279:251–272

[93] Lee CF, Huang YL (2013) Reversible data hiding scheme based on dual stegano-images using orientation combinations. Telecommun Syst 52(4):2237–2247

[94] Lu TC, Tseng CY, Wu JH (2015a) Dual imaging-based reversible hiding technique using LSB matching. Signal Process 108:77–89

[95] Lu TC, Wu JH, Huang CC (2015b) Dual-image-based reversible data hiding method using center folding strategy. Signal Process 115:195–213

[96] Ma YJ, Zhu YS, Liu XY (2016) A novel reversible watermarking scheme for relational databases protection based on histogram shifting. Journal of Information Hiding and Multimedia Signal Processing 7(2):266–276

[97] Nissar A, Mir AH (2010) Classification of steganalysis techniques: a study. Digital Signal Processing 20: 1758–1770

[98] Qin C, Chang CC, Hsu TJ (2015) Reversible data hiding scheme based on exploiting modification direction with two steganographic images. Multimedia Tools and Applications 74(15):5861–5872

[99] Subhedar MS, Mankar VH (2014) Current status and key issues in image steganography: a survey.Computer Science Review 13(14):95–113

[100] Wang Z, Bovik AC (2002) A universal image quality index. IEEE Signal Processing Letters 9(3):81–84

[101] Wang Z, Bovik AC, Sheikh HR, Simoncelli EP (2004) Image quality assessment: from error visibility to structural similarity. IEEE Trans Image Process 13(4):600–612

[102] Zhang X, Wang S (2006) Efficient steganographic embedding by exploiting modification direction. IEEE Commun Lett 10:781–783

[103] K. Bharanitharan, C. C. Chang, H. R. Yang, and Z. H. Wang, \Efficient pixel prediction algorithm for reversible data hiding," International Journal of Network Security, vol. 18, no. 4, pp. 750{757, 2016.

[104] [2] M. U. Celik, G. Sharma, A. M. Tekalp, et al., \Lossless watermarking for image authentication: a new framework and an implementation," IEEE Transactions on Image Processing, vol. 15, no. 4, pp. 1042{1049, 2006.

[105] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber,\Lossless generalized-lsb data embedding," IEEE Transactions on Image Processing, vol. 14, no. 2, pp. 253{266, 2005.

[106] C. K. Chan and L. M. Cheng, \Hiding data in images by simple lsb substitution," Pattern Recognition, vol. 37, no. 3, pp. 469{474, 2004.J. Fridrich, M. Goljan, and R. Du, \Lossless data embedding: new paradigm in digital watermarking," EURASIP Journal on Applied Signal Processing, vol. 2002, no. 1, pp. 185{196, 2002.

[107] Y. Hu, H. K. Lee, and J. Li, \De-based reversible data hiding with improved overflow location map," IEEE Transactions on Circuits and Systems for Video Technology, vol. 19, no. 2, pp. 250{260, 2009.

[108] B. Jana, D. Giri and S. K. Mondal, \Dual-image based reversible data hiding scheme using pixel value difference expansion," International Journal of Network Security, vol. 18, no. 4, pp. 633{643, 2016.

[109] L. Kamstra and H. J. Heijmans, \Reversible data embedding into images using wavelet techniques and sorting," IEEE Transactions on Image Processing, vol. 14, no. 12, pp. 2082{2090, 2005.

[110] S. K. Lee, Y. H. Suh, and Y. S. Ho, \Reversiblee image authentication based on watermarking," in 2006 IEEE International Conference on Multimedia and Expo, pp. 1321{1324, IEEE, 2006.

[111] F. Li, Q. Mao, and C. C. Chang, \A reversible data hiding scheme based on iwt and the sudoku method," International Journal of Network Security, vol. 18, no. 3, pp. 410{419, 2016.

[112] X. Li, J. Li, B. Li, and B. Yang, \High-fidelity reversible data hiding scheme based on pixel-valueordering and prediction-error expansion," Signal Processing, vol. 93, no. 1, pp. 198{205, 2013.

[113] M. Liu, H. S. Seah, C. Zhu, W. Lin, and F. Tian, \Reducing location map in prediction-based difference expansion for reversible image data embedding," Signal Processing, vol. 92, no. 3, pp. 819{828, 2012.International Journ