Reversible Data Hiding With De and RW (De-Difference Expansion, RW-Reversible Watermarking)

J.Saranya¹, G. Shanmugapriya², R. Sangeetha³
¹,²,³Final Year, Semester – VIII.

Abstract: In the past two decades, Reversible Data Hiding (RDH) additionally mentioned as lossless or invertible knowledge concealing has gradually become a really active analysis space in the field of information hiding. In some sensitive scenarios permanent distortion is strictly prohibited. So, in order to solve this problem we go for Reversible Data Hiding (RDH). It proposed to embed the authentication information into a digital medium and enable the legitimate user to extract the embedded authentication information for verifying the authenticity of received data. The project focuses on imperceptivity of both hidden and act of data embedding. The history of technical developments, the current state of arts and possible future are presented and discussed. It is expected that Reversible Data Hiding (RDH) technology and its application in the real world will continue to move ahead in a rapid manner thus providing efficient and advantage yielding results.

Index Terms—Difference Expansion, Lossless invertible data hiding, Reversible Data Hiding, Reversible Water Marking.

I. INTRODUCTION

DATA HIDING has received much attention from the research community in the past more than two decades [1], [2]. By this technique, it can embed secret data into a cover medium, and later enable the intended user to extract the embedded data from the marked medium for various purposes. However, for most data hiding methods, the retrieval of the cover medium without any distortion is been a great question. So in these type of scenarios, such permanent distortion is strictly forbidden and the exact recovery of the original cover medium is required. To solve this issue, reversible data hiding (RDH), also called lossless or invertible data hiding, is proposed to losslessly recover both the embedded data and the cover medium [3], [4]. That is, with the RDH, besides the embedded data, the cover medium can be exactly recovered from the marked data as well. The first RDH algorithm is the one proposed by Barton in a US patent in 1997 [5]. He proposed to embed the authentication information into a digital medium, and enable legitimate users to extract the embedded information for verifying the authenticity of the received data. So far, there is a rapid increase of applications that utilize RDH, and several examples have been reported in the literature including image authentication [6], [7], medical image processing [8], [9], video error-concealment coding, stereo image coding, vector map recovery in CAD (computer-aided design) engineering graphics [10], [11], and data coloring in the cloud etc. As a special type of data hiding, the RDH has its own pros and cons when compared with conventional data hiding techniques such as digital watermarking and steganography. For digital watermarking, its main concern lies in how to efficiently extract the embedded data from a degraded marked medium. It considers the robustness as top priority, but rarely cares about the cover medium recovery. Whereas, steganography conceals data into a cover medium in a way that the embedded data is undetectable. It focuses on imperceptivity of both the hidden data and the act of data embedding, i.e., the embedded data is not only imperceptible to human eyes but also to potential analyzers. Compared with these two data hiding techniques, the specific property of RDH is the perfect recovery of both of the cover medium and the embedded secret data. In general, RDH is a fragile technique and it poses no robustness against possible attacks. In the rest of this paper, various subjects on RDH are presented; the various RDH schemes in image spatial domain are presented. Two major approaches: difference expansion (DE) and Reversible watermarking (RW), together with some effective procedures are described. RDH for JPEG compressed images, which are actually widely utilized in reality. Section IV presents the so-called robust RDH, meaning that if an image with reversible data hiding has been lossy compressed, while the original image will not be able to recover exactly, but the hidden message can still be recovered if the compression is not very severe. V addresses the RDH for encrypted images, which is expected to be very useful for cloud computation. In Section VI, the RDH for video and RDH for audio are presented. Surprisingly, the number of the published papers on RDH for video
and audio is relatively much smaller, indicating that more research works are called for. Finally, a summary is made at the end of the paper.

A. RDH IN PREVIOUS CENTURIES:

At first several RDH schemes developed at the early stage were designed for the purpose of fragile authentication. As a representative of this type of methods, we now describe Honsinger et al.’s method [12]. In this method, the marked image is obtained by adding the secret data with the original image, and then taking the resulted value modulo 256. Its data embedding can be formulated as \( J D (I C M) \mod 256 \), where \( I, M, \) and \( J \) are respectively the cover image, the payload derived from the hash function of the cover image, and the marked image. In the authentication side, the payload \( M \) can be reconstructed from the marked image, then subtract the payload from the marked image to losslessly recover the original image. The modulo-256 operation can prevent the overLow/underLow problem in data embedding, i.e., a pixel value either exceeds the upper or the lower bound, thus guaranteeing the reversibility of data hiding. However, a drawback of this method is that the marked image may suffer a salt-and-pepper noise when the cover image contains some boundary pixels with the value of 255 or 0. Moreover, since fragile authentication does not need much data to be embedded into a cover medium, the capacity of this type of methods is not large.

B. DIFFERENCE EXPANSION:

In [13] and [14], Tian presented a promising high capacity RDH method based on DE. With DE, integer Haar wavelet transform is first applied to the cover image to derive difference values, and then these values are expanded to create vacancies for reversible data embedding. Here, we present the major step of Tian’s DE method. For a pixel pair \( (x_0; x_1) \), the nearest their integer average and difference are \( h = x_1 - x_0 \) and \( h' = 2c \) respectively. In order to embed one bit \( m \), one can see that DE is actually a kind of IT, and DE can be viewed as the first IT-based RDH. Later on, Alattar [17] proposed a new method by generalizing DE from the viewpoint of IT. Specifically, Alattar improved Tian’s method by generalizing DE from pixel pair to pixel block of arbitrary size.

C. THEORETICAL INVESTIGATION ON RDH:

One basic problem for RDH is , for a given distortion limit upper bound of the payload is reversibly embedded with the cover medium. Clearly, with this transformation, \( n \) bits are embedded into \( n C 1 \) pixels, and it is possible to increase the maximum embedding rate to 1 bpp by taking sufficient large \( n \). In [18], Colucc and Chassery proposed a method based on the so-called reversible contrast mapping which is an IT of integer pair. A specific feature of this method is that, compared with DE, it does not need additional lossless data compression, and thus it is efficient in terms of computational complexity. In [19], based on invariance of the sum of pixel pairs and pairwise difference adjustment, DE is improved by Weng et al. by using two different pixel pair
considering the magnitude of difference value. In [20], Wang et al. generalized DE also by using a new IT. They showed that the embedding rule of DE can be reformulated as a transformation of integer pair and gave a novel algorithm by extending the transformation. The method [21] is recently extended by Qiu et al. in [31] exploiting adaptive embedding. In [22] and [23], from another IT viewpoint for DE, the authors proposed a new IT which maps the cover pixel block \( x D (x_0; x_1; \ldots ; x_n) \) to the secret message \( m D (m_1; m_2; \ldots ; m_n) \) to the marked pixel. One basic problem for RDH is, for a given distortion constraint, what is the upper bound of the payload that can be reversibly embedded into a cover medium. For a special cover which is an independent and identically distributed integer sequence, this problem has been solved by Kalker and Willems [93] who formulated RDH as a special rate-distortion problem, and obtained the upper bound under a given distortion constraint 1 as:

\[
\text{rev}(1) D = \max_{Y} \left( \frac{H(Y\ y)}{H(X\ x)} \right)
\]

where \( \text{rev} \) denotes the reversible embedding capacity, \( X \) and \( Y \) denote respectively the cover and marked sequence, and \( H \) is the entropy function. The maximum entropy in (10) is over all transition probability matrices \( P_{Y|X} (y|x) \) satisfying the distortion constraint \( X \sim x P_X (x)P_{Y|X} (y|x)D(x; y) \leq 1 \) where the metric \( D(x; y) \) is usually denoted as the square error distortion, i.e., \( (x - y)^2 \). Eq. (10) indicates that the amount of secret data carried by a marked sequence in a reversible manner is just the difference of entropies between the marked and covers sequence. Notice that, in practical embedding schemes, for a cover image, it is usually projected to a dimensional space to derive an i.i.d. cover sequence (e.g., the prediction-error sequence), and then one applies (10) to the generated image. Cover sequence instead of the cover image.

D. REVERSIBLE WATERMARKING:

The enormous increase in the use of digital content has increased the issues such as online data vulnerability and copyrights violation. One of the prominent solutions is the watermarking of the digital content. Beside watermarking, there exist other interesting methods that can also provide protection to the digital content e.g., cryptography, steganography etc. Steganography and watermarking both come under data hiding techniques i.e., they are used to hide secret information in the cover work. However, there exist subtle difference between steganography and watermarking i.e., steganography conceals the very existence of secret information. If the existence of secret information is revealed, steganography fails. Whereas, in water marking the existence of secret information can be known. Ideally, the goal of watermarking. Through suitable watermarking techniques, the protection of the data can be ensured and one can know whether the received content has been tampered with or not. However, watermarking can cause damage to the sensitive information present in the cover work, and thus at the receiving end, the exact recovery of cover work may not be possible. In some applications, even the slightest distortion in the cover work is intolerable. For example, in the field of medical imagery, if a medical image is modified using conventional watermarking, the small change may affect the interpretation significantly and a physician may make a wrong diagnosis. Similarly, in case of military application, changes due to embedding of secret information can substantially alter the cover image and therefore, the decision taken may cost considerably. Consequently, there is a strong need to restore the cover work to its original form. Reversible watermarking, also known as lossless watermarking, allows full extraction of the embedded information along with the complete restoration of the cover work. Reversible watermarking can thus be considered as a special case of watermarking.

E. CONTRAST ENHANCEMENT:

To evaluate the effect of contrast enhancement, the RCE is calculated in the methods. However, the RCE value cannot be used to represent the visual quality because it may be high for an enhanced image with visual distortions. Although the visual quality can be improved by applying the schemes introduced in under some circumstances, the enhanced contrast does not necessarily lead to good image quality. Meanwhile, PSNR is still used in as a reference of image quality due to the lack of a
suitable image quality evaluator. Since PSNR is not always suitable for image quality assessment, other criteria need to be found to guide the process of RDH more efficiently. In the following, we will introduce using the Structural SIMilarity (SSIM), the methods specially developed for the contrast changed images, and the no reference methods for image quality assessment, respectively.

![Figure 1](image1.png)

**1. Lossless Compression and Encryption**

Fridrich et al. propose this algorithm. Space to hide data is found by compressing proper bit-plane that offers minimum redundancy to hold the hash (authentication information). Lowest bit-plane offering lossless compression can be used unless the image is not noisy. In completely noisy image some bit-planes exhibit strong correlation. These bit-planes can be used to find enough room to store the hash. Hash length is generally 128 bit using MD5 algorithm. The algorithm starts lossless compression from 5th bit-plane and calculates redundancy by subtracting compressed data size from number of pixels. The authors use the JBIG lossless compression method to compress the bit-planes. During embedding the algorithm first calculates the hash of the original image, finds the proper bitplane, and adds the hash with the compressed bit-plane data. Then it replaces selected bit-plane by concatenated data. For more security the concatenated hash with compressed data is encrypted using symmetric key encryption based on 2-dimensional chaotic maps. This algorithm takes variable sized blocks and gives the encrypted message as long as the original message, so no padding is needed. Other public or symmetric key algorithms can be used, but they require padding to embed the encrypted message and hence increase distortion. During decoding after key bit-plane selection the data is decrypted and hash is separated from the compressed original bit-plane data. The bit-plane is replaced by the decompressed data; hence the exact copy of the original image is found. The hash of the reconstructed image is calculated and compared with the extracted hash; if both are same the image in question is authentic. The advantages of this algorithm are (i) high capacity, (ii) security is equivalent to the security provided by cryptographic authentication, and (iii) can be applied for the authentication purposes of JPEG files, complex multimedia objects, audio files, digitized hologram, etc. The disadvantages are (i) noisy image forces the algorithm to embed information in higher bit-plane when the distortions are higher and easily visible, (ii) single bit-plane in a small image does not offer enough space to hide hash after compression, so two or more bit-planes are required and the artifacts must be visible, and (iii) capacity is not high enough to embed large payload.

**2. Reversible Data Hiding at Low Pixel-Levels**

Mehmet et al. proposed a reversible data hiding technique that uses prediction based conditional entropy coder utilizing static portions of the input signal as side-information to improve the compression efficiency. Hence the lossless data embedding capacity is increased. This spatial domain method is the modification of generalized LSB embedding technique and uses very simple signal features: lowest levels of raw pixels. It follows the general principal of lossless embedding. The algorithm searches the whole image to have the first L (say, L = 4) lowest levels of pixel values. It compresses these pixel values using CALIC lossless image compression algorithms and check whether it gives enough space (128-bit for hash). If the given capacity is lower than expectation the algorithm increases L and continues searching. Once it finds enough capacity, it concatenates the hash with compressed pixel values. The concatenated bit-string is converted into L-ary symbols to replace the lowest L-levels of pixel values. The decoding process is just the reverse of the embedding phase. The advantages are (i) simple algorithm, and (ii) higher capacity can be found with the increase of embedding level L. The disadvantages are (i) capacity depends on image structure, smooth images give higher capacity than irregular textured images, and (ii) artifacts are visible with the increase of embedding level L. Though the algorithm gives a very high capacity, it gives incredible distortions to the original image.

**3. High Capacity Watermarking Based on Difference Expansion**

In [24][25] Tian propose a high quality reversible watermarking method with high capacity based on difference expansion. Pixel differences are used to embed data; this is because of high redundancies among the neighboring pixel values in natural images. During embedding (i) differences of neighboring pixel values are calculated, (ii) changeable bits in that differences are determined, (iii) some differences are chosen to be expandable.
by 1-bit, so changeable bits increases, (iii) concatenated bit-stream of compressed original changeable bits, the location of expanded difference numbers (location map), and the hash of original image (payload) is embedded into the changeable bits of difference numbers in a pseudo random order, (iv) use the inverse transform to have the watermarked pixels from resultant differences. During watermark extraction – (i) differences of neighboring pixel values are calculated, (ii) changeable bits in that differences are determined, (iii) extract the changeable bit-stream ordered by the same pseudo random order as embedding, (iv) separate the compressed original changeable bit-stream, the compressed bit-stream of locations of expanded difference numbers (location map), and the hash of original image (payload) from extracted bit-stream, (v) decompress the compressed separated bit-streams and reconstruct the original image replacing the changeable bits, (vi) calculate the hash of reconstructed image and compare with extracted hash. The advantages are – (i) no loss of data due to compression-decompression, (ii) also applicable to audio and video data, and (iii) encryption of compressed location map and changeable bit-stream of different numbers increases the security. The disadvantages include – (i) there may be some round off errors (division by 2), though very little, (ii) largely depends on the smoothness of natural image; so cannot be applied to textured image where the capacity will be zero or very low, and (iii) there is significant degradation of visual quality due to bit-replacements of gray scale pixels [26].

F.EXPERIMENTAL VERIFICATION:
We have applied our method on various gray level images and we show the results of the proposed method applied on and the image of Girl(512 × 512 pixels) fig.1. We have encrypted the original image by using the RDH algorithm in mode to get encrypted image illustrated in Fig.1. The size of the blocks is 16 pixels (128 bits). From this encrypted image we have then embedded bits to get the marked and encrypted image illustrated in Fig. 2.
I. REFERENCES:


**Funding Source**


**I . REFERENCES:**


