Reversible Watermarking using Histogram Shifting and Pixel Differences with Inverse S-scan order and Local Prediction

Naseera P. A

Computer Science and Engineering, ICET, Muvattupuzha, India

Abstract: The Reversible Watermarking enables the embedding of Watermarks in a host image without any loss of host content, which is proposed for image authentication that if the watermarked image is deemed authentic, it can revert in to the exact copy of the original image before the embedding occurred. This paper conveys the improved histogram-based reversible watermarking scheme based pixel differences with local prediction. Before performing the embedding process flip the host image. For each pixel, calculate the difference between them. And take the difference value for finding peak value of the histogram and hide the watermark in the flipped image's histogram peaks. This will perform high security in data hiding. The reverse process is performed at the receiver.

Keywords: Reversible watermarking, difference expansion, Histogram Shifting, Image Flipping, Inverse S-scan order.

1. Introduction

In the recent years, the development of multimedia technologies and internet has provided the consumers the access to multimedia data. Hence the data may be tampered or attacked during transmission. So it is essential to protect the digital data in applications like military or medical applications [4]. A possible solution to prevent such forgery is data hiding techniques. Data hiding refers to hide data within a digital media. Media can be anything like audio, image and video. Hiding is done by modifying the contents of the digital media. Hiding process is done in such a way that modification of pixel values should be undetectable to the viewers. Image where the hiding is done is known as the watermarked image. In most hiding techniques, the host image is distorted permanently and thus it cannot be recovered back completely from the marked content. However, in various applications like military and medical applications, degradation of the overmedia is not allowed. For medical applications, even the slight changes in the image are intolerable. So it is essential to introduce the data hiding in such a way that it is reversible and quality degradation after embedding is lowered. Such reversible data hiding techniques are also known as distortionless or lossless data hiding techniques. Reversible data hiding techniques hide information within the digital media in such a way that only the authorized person could decode the hidden data and restore back to the original state.

1.1 Histogram Modification

In [9], Ni et al. introduced a reversible data hiding scheme based on histogram modification. It will describe briefly in this section. The histogram modification technique involves generating histogram and finding the peak point and the zero point and shifting histogram bins to embed message bits.

For a given host image, it will generate its histogram and find a peak point and a zero point. A peak point corresponds to the grayscale value which the maximum number of pixels in the given image assumes. On the contrary, a zero point corresponds to the grayscale value which no pixel in the given image assumes. By considering Histogram of any image and, let \( P \) be the value of peak point and \( Z \) be the value of zero point. The range of the histogram, \([P+1, Z-1]\), is shifted to the right-hand side by 1 to leave the zero point at \( P+1 \). Once a pixel with value \( P \) is encountered, if the message bit is “1,” increase the pixel value by 1. Otherwise, no modification is needed. Here the number of message bits that can be embedded into an image equals to the number of pixels which are associated with the peak point. The data extraction is actually the reverse process of data hiding. When a pixel with value \( P+1 \) is met, message bit “1” is extracted and the pixel value reduces to \( P \). When a pixel with value \( P \) is met, message bit “0” is extracted. After all message bits have been extracted, shift the range of the histogram, \([P+2, Z]\), to the left-hand side by 1.

The algorithm steps are:
1) Scan the cover image and construct its histogram
2) The gray value for which the histogram is highest is denoted the peak point \( P \), and the gray value for which the histogram is lowest is denoted by the minimum point \( Z \).
3) If \( \text{Hi}(Z)=0 \), then \( Z \) is called a zero point. For simplicity, we assume \( P<Z \).
4) Scan the image and record the positions of those pixel values to \( Z \).
5) Shift the histogram \( \text{Hi}(x) \) to the right to vacate the histogram bin at \( P+1 \).
6) Extract a data bit \( s \) from secret data \( S \). Scan the image once more.
7) If the scanned pixel value is P and the data bit to be embedded is 1, then set the pixel value to P+1
8) If the data bit to be embedded is 0, no change has to be done on the scanned pixel [1]

The similar process is required to be followed for the lossless recovery of the Original Image and the watermark.

2. Related Work

Most of the data hiding techniques are not reversible completely. The well-known LSB technique is not completely reversible due to bit replacement without “memory”. Reversible data hiding techniques are mainly classified into three main categories, first is based on data compression [2], [5], [6], second based on pixel value difference expansion [3], [10] and third based on histogram shifting [8], [13]. All these earliest technique is based on LSB replacement. In Data compression technique, the data to be embedded as well as related information’s of the image used for data recovery is compressed. Compressed data is embedded directly into the cover media using LSB replacement. Celik et al. [6] proposed data hiding technique in which each image pixel is quantized using L-level scalar technique. The residues yielded after quantization is compressed using a lossless compression algorithm called CALIC. Compressed residues along with the to-be embedded bits are embedded into the quantised image using LSB replacement. Distortions introduced on the watermarked image by this method are comparatively high. Technique based on pixel value difference expansion discovers the redundancy of pixel values in the images. Arithmetic operations are performed on the pixel pair’s inorder to explore the space for data embedding. Whether the pixel values can be expanded or not is indicated by the location map. This technique achieves higher embedding capacity and keeps the distortion low. Tian et al. [3] proposed the data hiding technique in which data bits are embedded by computing the difference between the pixel pairs. Location map which is essential for image restoration is embedded along with the data bits. Coltuc et al. [11] proposed a data hiding technique in which embedding of data bits is done by bytaking the RCM transform of the image. Reversible contrast mapping is an integer transform which is invertible even if some LSB bits are lost. Data bits are embedded in the LSB bits of such transformed pixel pairs. Complexity of the technique based on pixel value difference expansion is less, thus hacking becomes easier. Histogram based data hiding technique embeds the data in the cover media by shifting the histogram of the image. Histogram technique finds peak or zero points in the histogram and data embedding is done by shifting these peak and zero points. This technique yields higher data hiding capacity with low distortion. Histogram based reversible data hiding method was introduced by Ni et al. in [8], wheremessage is embedded within the histogram. Embedding is done by shifting the peak and zero points of the histogram. Also histogram shifting technique prevents overflow and underflow problem. Overflow is the condition that the greyvalue exceeds above 255. Underflow is the condition that the greyvalue falls below 0. Embedding based on histogram modification has been presented in [7], [8], [12].

The Proposed approach adopts the histogram shifting technique; this will improve the hiding capacity and high security for watermarking.

3. Proposed Approach

The proposed scheme improves hiding capacity and high security for the watermark. It is very difficult to find watermarked bits by an unauthorized person. Thus the new method describes an efficient extension of the histogram modification technique by considering the difference between adjacent pixels instead of simple pixel value. The distribution of pixel difference has a prominent maximum since image neighbor pixels are strongly correlated. Hence, there are a lot of candidates for embedding data; Characteristics of the pixel difference are exploited to achieve large hiding capacity while keeping the embedding distortion low. Inverse S order scanning and image flipping provide high security in embedded data. Histogram shifting technique also prevents overflow and underflow.

3.1 Calculation of pixel differences and Histogram modification

The reversible data hiding scheme is designed as follows.
1) Read the cover image and perform inverse S-scan order. (Scan the even rows of the image matrix.)
2) Then flip the scanned image. And save that value in the even position of image matrix.
3) Calculate the pixel difference d between pixels \( x_{i-1} \) and \( x_i \) by
\[
d_i = \begin{cases} x_i, & \text{if } i = 0, \\ |x_i - x_{i-1}|, & \text{otherwise} \end{cases}
\]
(1)
4) Determine the peak point \( P \) from the pixel differences.
5) If \( d_i > P \), shift \( x_i \) by 1 unit:
\[
y_i = \begin{cases} x_i + 1, & \text{if } d_i > P \text{ and } x_i \geq x_{i-1} \\ x_i - 1, & \text{if } d_i > P \text{ and } x_i < x_{i-1} \end{cases}
\]
(2)
6) If \( d_i = P \), modify \( x_i \) according to the message bit:
\[
y_i = \begin{cases} x_i + b, & \text{if } d_i = P \text{ and } x_i \geq x_{i-1} \\ x_i - b, & \text{if } d_i = P \text{ and } x_i < x_{i-1} \end{cases}
\]
(3)
Where \( y_i \) is the watermarked value of pixel \( i \).
7) Construct the watermarked bits according to the pixels \( y_i \).

At the receiving end, the recipient extracts message bits from the watermarked image by scanning the image in the same order as during the embedding.

The message bit \( b \) can be extracted by
\[
b = \begin{cases} 0, & \text{if } |y_i - x_{i-1}| = P \\ 1, & \text{if } |y_i - x_{i-1}| = P + 1 \end{cases}
\]
(4)
where \( x_{i-1} \) denotes the restored value of \( y_{i-1} \). Then the original pixel value of \( x_i \) can be restored by
\[
y_i = \begin{cases} y_i + 1, & \text{if } |y_i - x_{i-1}| > P \text{ and } y_i < x_{i-1} \\ y_i - 1, & \text{if } |y_i - x_{i-1}| > P \text{ and } y_i > x_{i-1} \\ y_i, & \text{otherwise} \end{cases}
\]
(5)
Thus, the exact copy of the original host image is obtained.

4. Conclusion

This paper proposes an efficient extension of histogram modification by considering the difference between adjacent pixels instead of simple pixel value. The distribution of pixel difference has a prominent maximum since neighbor pixels are strongly correlated. The watermark bits are embedded on the histogram peaks, so the embedding capacity is improved. Inverse S-scan order and image flipping provides high security for embedded data.

5. Acknowledgment

The Author would like to thank Femithamol. A. M. Assistant Professor, Department of Information Technology, Ilahia College of Engineering and Technology, Muvattupuzha for her moral and technical support.

References

[1] Celik, M.U., Sharma, G., Tekalp, A.M., and Saber, E.:“Reversible data hiding”. Proc. ICIP, 2002, vol. 2, pp. 157–160
[2] J. Fridrich, M. Goljan, and R. Du, “Lossless data embedding-new paradigm digital watermarking,” Eur. Assoc. Signal Process. J. Appl. Signal Process., vol. 2002, no. 2, pp. 185–196, Feb. 2002.
[3] J. Tian, “Reversible data embedding using a difference expansion,” IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003.
[4] R. Norcen, M. Podesser, A. Pommer, H. Schmidt, and A. Uhl, “Confidential Storage and Transmission of Medical Image Data,” Computers in Biology and Medicine 33, pp. 277–292, 2003.
[5] T. Kalker and F. M. J. Willems, “Capacity bounds and constructions for reversible data hiding,” Security Watermarking Multimedia Contents V, vol. 5020, pp. 604–611, Jun. 2003.
[6] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, “Lossless generalized-LSB data embedding,” IEEE Trans. Image Process., vol. 14, no. 2, pp. 253–266, Feb. 2005.
[7] L. Kamstra and H. J. A. M. Heijmans, “Reversible data embedding into images using wavelet techniques and sorting,” IEEE Trans. Image Process., vol. 14, no. 12, pp. 2082–2090, Dec. 2005.
[8] S. K. Lee, Y. H. Suh, and Y. S. Ho, “Reversible image authentication based on watermarking,” in Proc. IEEE Int. Conf. Multimedia Expo, Toronto, ON, Canada, Jul. 2006, pp. 1321–1324.
[9] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, “Reversible data hiding,” IEEE Transactions on Circuits and Systems for Video Technology, vol. 16, no. 3, pp. 354–362, Mar. 2006.
[10] D. M. Thodi and J. J. Rodriguez, “Expansion embedding techniques for reversible watermarking,” IEEE Trans. Image Process., vol. 16, no. 3, pp. 721–730, Mar. 2007.
[11] D. Coltuc and J. M. Chassery, “Very fast watermarking by reversible contrast mapping,” IEEE Signal Process. Lett., vol. 14, no. 4, pp. 255–258, Apr. 2007.
[12] M. Fallahpour and M. H. Sedaaghi, “High capacity lossless data hiding based on histogram modification,” IEICE Electron. Exp., vol. 4, no. 7, pp. 205–210, Apr. 2007.
[13] W. Hong, T. S. Chen, and C. W. Shiu, “Reversible data hiding for high-quality images using modification of prediction errors,” J. Syst. Softw., vol. 82, no. 11, pp. 1833–1842, Nov. 2009.

Author Profile

Naseera P.A received the Bachelor of Technology degree in Information Technology from Mahatma Gandhi University, Kerala. She is currently doing Master of Technology degree in Computer Science and Engineering with Specialization in Information Systems from Mahatma Gandhi University, Kerala.