Reversible Data Hiding Based On Faster Numerical Methods

Anitha Raj B, GajalakshmiN

PG Scholar, Dept of Information Technology, K.L.N College of Information Technology, Pottalpalayam, Sivagangai, Tamil Nadu, India.

Assistant Prof, Dept of Information Technology, K.L.N College of Information Technology, Pottalpalayam, Sivagangai, Tamil Nadu, India.

Abstract:In implement prediction-based reversible steganographic scheme based on image in painting. In this scheme the reference pixels are adaptively selected according to the distribution characteristics of the content of the image. Image in painting based on partial differential equations is used to complete the prediction process by the reference pixels. The histogram prediction error is shifted to embed the secret bits reversibly. During the extraction procedure, the same reference pixel can be exploited to conduct the prediction, which guarantees the lossless recovery of the cover image.
Key words :- rever steganographic, image in painting, histogram prediction error.

I.INTRODUCTION

Reversible data hiding can be used for medical, military, and legal applications, which do not allow any modification in the digital representation of the cover image. Two main categories of reversible data hiding methods for images are, Methods based on difference expansion. Methods based on histogram shifting. The accuracy of the prediction result depends on how the reference pixels are chosen and how these reference pixels are utilized for prediction. More reference pixels lead to a more accurate prediction result but they occupy more spaces that could be used for embedding the bits.

The property of reversibility means that the original form of the image, before the secret bits were embedded, can be recovered completely after the embedded bits are extracted. cover image due to the risk of misinterpretations. In general, there are two main categories of reversible data hiding methods for images, i.e., methods based on difference expansion and methods based on histogram shifting The peak point of the image histogram was selected and the pixel values in the range from its right one to the zero point were increased by one to create one vacant histogram bin for embedding. The number of secret bits that could be embedded depended on the pixel number of the peak point in the histogram. The information of the peak point and zero point was required in the procedure of extracting the embedded data and recovering the cover image.

It introduced a binary tree structure that can be utilized to predetermine the peak point used for embedding secret messages. Consequently, only the level of the binary tree must be shared by the sender and the receiver. Recently, many researchers have proposed reversible data hiding methods based on the prediction mechanism these methods are extensions of the method

based on difference expansion and the method based on histogram shifting. The key idea of the prediction-based method is that the prediction process is conducted first to estimate the cover image pixels, and the prediction error, i.e., the difference between the cover image and the prediction result, is used to embed the secret data by difference expansion or histogram shifting.

The consistency of the prediction results in the embedding and extracting procedures ensures the correctness of the extraction of the secret bits and the recovery of the cover image. It indicated that the cover image can be divided into its prediction result and the corresponding prediction error. The predictor they used was a low-complexity algorithm with an inherent edge-detection mechanism. The prediction error was expanded according to the embedding data and combined with the prediction result to produce the stego image.

II.LITERATURE REVIEW

In 2003, Tian proposed a reversible data hiding method based on difference expansion [1]. In his work, the cover image was divided into a series of nonoverlapping, neighboring pixel pairs, and the difference of each pixel pair was doubled. Then,the doubled difference was either kept reserved or modified according to the parity of the embedding secret bit. On the receiver side, the embedded secret data can be extracted easily from the least significant bit (LSB) of the differences of the pixel pairs in the stego image. But the additional information of the location map was needed to solve the underflow and overflow problems. Ni *et al*. [6] presented a method based on histogram shifting to embed secret data reversibly. The peak point of the image histogram was selected and the pixel values in the range from its right one to the zero point were increased by one to create one vacant histogram bin for embedding. The number of secret bits that could be embedded depended on the pixel number of the peak point in the histogram. The information of the peak point and zero point was required in the procedure of extracting the embedded data and recovering the cover image.

III.MODULE DESCRIPTIONS

Preprocessing

In preprocessing method median filter is used to remove noise from the input test images. It is often desirable to be able to perform some kind of noise reduction on an image or signal. The **median filter** is a nonlinear digital filtering technique, often used to remove noise.[5] Such noise reduction is a typical pre-processing step to improve the results of later processing. Median filtering is very widely used in digital image processing.

Adaptive Reference Pixel Choosing

The reference pixels in the smooth region of the cover image lead to a more accurate prediction result than the same number of reference pixels in the complex region. we can increase the number of reference pixels in the complex region to obtain a more accurate prediction result, which may result in greater hiding capacity and better visual quality of the stego image[1]. On the other hand, the number of reference pixels in the smooth region can be reduced to save more possible embeddable pixels, which does not influence the result of the prediction significantly.

Pixel Prediction Based on Image Inpainting.

After all reference pixels in the cover image have been decided, the non reference pixels are predicted by the image inpainting technique to generate the prediction image. The inpainting-based prediction process is totally dependent on the reference pixels of the cover image. [12]Image inpainting is a technique that can fill in or remove the chosen regions of digital images. By using this method good similarity between the cover image and the prediction image can be achieved.

Conditions

$$\frac{\partial P(x, y; t)}{\partial t} = \text{div} \left[\frac{\varphi(|\kappa|)}{|\nabla P(x, y; t)|} \nabla P(x, y; t) \right] \forall (x, y) \in \Omega$$

The above Partial Differential Equation(PDE) is solved by using Fast Numerical Method whereas in existing technique it can be solved by using Finite Difference Method.

Embedding Procedure

During the embedding procedure, the difference image E, i.e., the prediction error between P and Pe, is modified according to the distribution of its histogram and the embedding secret bits.[7] Then, the modified difference image E is added to the prediction image Pe to generate the final stego image Ps. The total number of embedded secret bits, i.e., total hiding capacity, is equal to the number of the difference image pixels. The embedding procedure is equivalent to shifting the histogram of the difference image between the two groups of peak point and zero point.

Extraction and Recovery Procedures

During the extraction procedure, the embedded bits can be extracted, and the cover image can be recovered losslessly. To guarantee the success of extraction and recovery, the parameters, μ, T1, T2, α1, β1, α2, β2, must be transmitted to the receiver side through the secure channelslessly. prediction image Pe can be acquired from the stego image Ps by applying CDD-based inpainting.

Performance Evaluation

Peak Signal-to-Noise Ratio, and MSE value are computed. PSNR is an *approximation* to human perception of reconstruction quality. Although a higher PSNR generally indicates that the reconstruction is of higher quality, in some cases it may not. PSNR is most easily defined via the mean squared error (*MSE*). Given a noise-free *m×n* monochrome image *I* and its noisy approximation *K*, *MSE* is defined as:
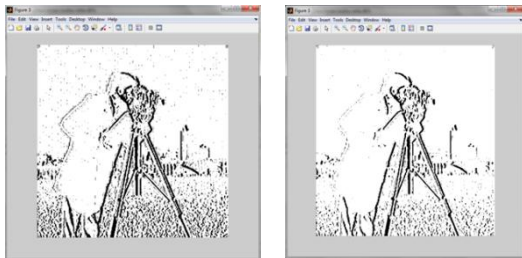
$$MSE = \frac{1}{m\,n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$
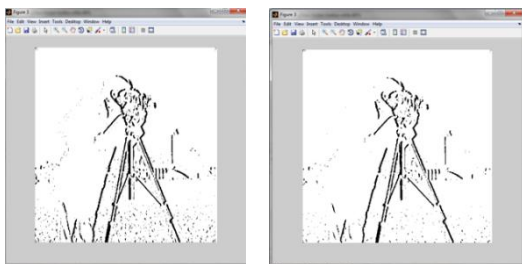
The PSNR is defined as:

$$PSNR = 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right)$$
$$= 20 \cdot \log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right)$$
$$= 20 \cdot \log_{10}(MAX_I) - 10 \cdot \log_{10}(MSE)$$

IV.EXPERIMENTAL RESULT

In this paper noise was removed in the cover image,using thresholds reference pixel was choosen and PSNR value is calculated to the cover image. Embedding procedure is still in process.

(a) (b)

(c) (d)

(a)

Binary mask *Q* with *T1* = 2, *T2* = 20. (b) Binary mask *Q* with *T1* = 4, *T2* = 40. (c) Binary mask *Q* with *T1* = 6, *T2* = 60. (d) Binary mask *Q* with *T1* = 8, *T2* = 80.

V.CONCLUSION

According to the reference pixels that were chosen, the PDE-based inpainting algorithm using the Fast Numerical model can generate the prediction image. Use of the adaptive strategy for choosing reference pixels and the inpainting predictor, the accuracy of the prediction result was high, and larger numbers of embeddable pixels are acquired.Thus, the embedded secret data can be extracted from the stego image correctly.

VI.FUTURE WORK

In Future Work , RSA is an algorithm for public-key cryptography that is based on the presumed difficulty of factoring large integers, the factoring problem. RSA stands for Ron Rivest, Adi Shamir and Leonard Adelman. A user of RSA creates and then publishes the product of two large prime numbers, along with an auxiliary value, as their public key. The prime factors must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime factors can feasibly decode the message. Whether breaking RSA encryption is as hard as factoring is an open question known as the RSA problem.

Because RSA encryption is a deterministic encryption algorithm (i.e., has no random component) an attacker can successfully launch a chosen plaintext attack against the cryptosystem, by encrypting likely plaintexts under the public key and test if they are equal to the cipher text. A cryptosystem is called semantically secure if an attacker cannot distinguish two encryptions from each other even if the attacker knows (or has chosen) the corresponding plaintexts. As described above, RSA without padding is not semantically secure.

REFERENCES

[1]. J. Tian, "Reversible data embedding using a difference expansion," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 890–896, Aug. 2003.

[2]. Chuan Qin, Chin-Chen Chang, *Fellow, IEEE, Ying-Hsuan Huang, and Li-Ting Liao,"* An Inpainting-Assisted Reversible SteganographicScheme Using a Histogram Shifting Mechanism" *IEEE Trans. Circuits Syst. Video Technol., vol. 23, no. 7, July.* 2013.

[3]. C. Qin, S. Wang, and X. Zhang, "Simultaneous inpainting for image structure and texture using anisotropic heat transfer model," *Multimedia Tools Appl.*, vol. 56, no. 3, pp. 469–483, 2012.

[4]. H. C. Huang and W. C. Fang, "Authenticity preservation with histogrambased reversible data hiding and quadtree concepts," *Sensors*, vol. 11, no. 10, pp. 9717–9731, 2011.

[5]. Z. Zhao, H. Luo, Z. M. Lu, and J. S. Pan, "Reversible data hiding based on multilevel histogram modification and sequential recovery," *Int. J. Electron. Commun.*, vol. 65, no. 10, pp. 814–826, 2011.

[6]. Z. C. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 16, no. 3, pp. 354–362, May 2006.

[7]. C. Qin, F. Cao, and X. Zhang, "Efficient image inpainting using adaptive edge-preserving propagation," *Imag. Sci. J.*, vol. 59, no. 4, pp. 211–218, 2011.

[8]. W. Hong and T. S. Chen, "Reversible data embedding for high quality images using interpolation and reference pixel distribution mechanism," *J. Visual Commun. Image Representation*, vol. 22, no. 2, pp. 131–140, 2011.

[9]. C. F. Lee, H. L. Chen, and H. K. Tso, "Embedding capacity raising in reversible data hiding based on prediction of difference expansion," *J. Syst. Software*, vol. 83, no. 10, pp. 1864–1872, 2010.

[10]. L. X. Luo, Z. Y. Chen, M. Chen, X. Zeng, and Z. Xiong, "Reversible image watermarking using interpolation technique," *IEEE Trans. Informat. Forensics Security*, vol. 5, no. 1, pp. 187–193, Mar. 2010.

[11]. W. L. Tai, C. M. Yeh, and C. C. Chang, "Reversible data hiding based on histogram modification of pixel differences," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 19, no. 6, pp. 906–910, Jun. 2009.

[12]. H. W. Tseng and C. P. Hsieh, "Prediction-based reversible data hiding," *Informat. Sci.*, vol. 179, no. 14, pp. 2460–2469, 2009.

[13]. D. Liu, X. Y. Sun, F. Wu, S. P. Li, and Y. Q. Zhang, "Image compression with edge-based inpainting," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 17, no. 10, pp. 1273–1287, Oct. 2007.