Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 11, November 2014, pg.447 – 454

RESEARCH ARTICLE

AN EFFICIENT WAY OF DATA HIDING USING HISTOGRAM SHIFTING MECHANISM

R.KEERTHANA, M.CHANDERKUMAR
PG STUDENT, ASSISTANT PROFESSOR
FATIMA MICHAEL COLLEGE OF ENGG AND TECH, TAMIL NADU, INDIA
EMAIL: *keerth.ramachandran@gmail.com*

***Abstract:** In proposed system a novel prediction-based reversible steganographic scheme based on image inpainting was used. In my work first the reference pixel are chosen adaptively according to the distribution characteristics of the image content. In the existing system only one secret image was hided in the original image, but in my proposed system first the cover image (original image) was divided into two blocks of pixels such as b1 and b2. In the first block (b1) secret image was embedded and in the second half (b2) a secret text was hided. After hiding the secret data in the two blocks the corresponding blocks are merged together. This image is said to be Stego image. This Stego image is look same the original image*

***Index Terms**— Embedding rate, image inpainting, prediction-error shifting, reversible steganography, visual quality*

1.INTRODUCTION

Steganography is the art of secret way of communication.In this reversible Steganography was used which is used to retain the original image even after the secret message was embedded.This 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 due to the risk of misinterpretations. 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. 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 due to the risk of misinterpretations. 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. In this 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. Different from cryptography, the main goal of data hiding is to conceal the hidden data by the carrier media, so that the hidden data is transferred without drawing suspicions. The hiding algorithms are to maintain the natural appearance of the cover media and to keep uninvolved people from even thinking the information exists. To hide information inside an image, there are several available domains where steganography algorithms exploit such as spatial domain or DCT domain. Among various types of images, JPEG format is a commonly used standard of lossy compression for photographic images. JPEG

images can typically gain 30:1 compression ratio with little perceptible loss in image quality. Another advantage of JPEG standard is that the degree of compression can be adjusted, allowing a selectable tradeoff between storage size and image quality.

In this work, a secret communication scheme is proposed, in which the data is doubly protected by both encryption stage and hiding stage. The message to be embedded is first processed by applying some encryption techniques. After the encryption stage, the scrambled message is then embedded into a JPEG image by managing different quantization tables. The final result is a JPEG image containing some certain regions with different image quality. The recipient performs reverse steps to extract the information: first extract the pattern of the scrambled message, and then use the key which was shared previously to decipher the message.

The Principle of This Message Hiding Scheme

Consider the case when a set of coefficients is quantized by an amount, i.e., a block of size 8X 8 contains DCT coefficients from to maps to a QT of the same size. Each DCT coefficient is quantized by the corresponding amount in QT and then rounded to the nearest integer (the rounding rule may vary between different schemes

$$\hat{c}_{ij} = round\left(\frac{c_{ij}}{q_{ij}}\right). \qquad (1)$$

If that DCT set is recalculated and then the set is quantized a second time by an amount, which after reconstruction gives the DCT coefficients set . Except in the case of (which means no more quantization), the difference between and will be minimal only whenq2=q1. In other words, if was previously quantized by a value , in which , means that it was processed with lower quality, and then the difference

defined by (2) reaches minimum value as , if we consider the difference in (2) as a function of q2.

$$difference = \sum_{i,j} \left\| c_1^{ij} - c_2^{ij} \right\|^2 (i,j = 1,\ldots,8). \quad (2)$$

Besides, the difference also reaches a local minimum as reaches. To embed a secret message into a JPEG image, some specific regions of the image are compressed with lower quality. The regions with lower quality are employed to carry the hidden information, and an embedded image is used as a media for secret communication.

Encryption Stage:

The image to be embedded is first passed through an encryption stage. Here we simply apply an automorphism algorithm [7], [8] to permute the pixels in the hidden message. In fact, any encryption algorithm can be applied in this stage, provided that the algorithm itself and the key are strong enough. An image, after applying some modulo operation, becomes a random pattern. For example, after applying this operator with the parameter ω =2 on the original image 66 items. We have scrambled image like the image next to the original one; ω is the parameter for changing the divisor in this modulo operation and is considered the key for decryption. To be even more secured, in practice this step can be repeated with several rounds, and different sets of ω and η can be applied. Hence the key that the recipient needs to reconstruct hidden image is the set of those ω and η values

Steganalysis:

Steganalysis is the art and science of detecting hidden messages from images made from stegosystems. Steganalysis is a fast growing science and relatively new.

Most steganalysis publications are written in the last 10 years. The purpose of steganalysis is to distinguish if an image contains a secret message or not. Researches on this field tend to find statistical properties of images that the stego-system doesn't conserve or find methods that one can find out if the image was altered at all or not. Thus, steganalysis is considered successful if it can guess whether an image contains a hidden message or not with a probability higher than random guessing.

2.LITERATURE SURVEY

2.1. Simultaneous inpainting for image structure and texture using anisotropic heat transfer model

A PDE-based image inpainting method using anisotropic heat transfer model, which can simultaneously propagate the structure and texture information.In structure inpainting, the propagating direction and intensity are related to image contents,and the strength of propagation along gradient direction is made inversely proportional to the magnitude of gradient. In texture inpainting, the added texture term reflects periodicity along the texture and its perpendicular direction. For numerical implementation, the step size of finite difference is adaptively chosen according to the curvature, leading to fewer iteration steps and satisfactory inpainting quality. Compared with other high order PDE methods and layered methods, the proposed approach is more concise and doesnt need image decomposition. Image inpainting, on the other hand, is to imitate human professionals in repairing pictures using some mathematical models and computer algorithms to recreate the missing content in the image. The objective is to produce visually satisfactory or acceptable results, rather than a good estimate of the original since there is simply no original. Inpainting of digital images has found

applications in such areas as restoration of historical photographs, filling in or removing chosen areas in images, and wiping out visible watermarks.

2.2 Reversible data hiding based on multilevel histogram modification and sequential recovery

Data hiding, also called information hiding, plays an important role in information security. It aims at embedding imperceptible confidential information in cover media such as still images, videos, audios, 3D meshes, etc. It consists of several branches such as steganography, watermarking, visual cryptography, etc. The data hiding scheme proposed in this work can be classified into the category of steganography. Steganography is usually used for covert communications. Thus the high embedding capacity is the main concern in this kind of technique. In contrast, watermarking is usually used for copyright protection and announcement. Thus researchers aim at improving the robustness of watermark content against intentional or unintentional attacks. Therefore, most available data hiding methods can provide a higher capacity than that provided by watermarking schemes. This advantage broadens the application scenarios of data hiding. A reversible data hiding scheme based on histogram modification. Its principle is to modify the histogram constructed based on the neighbor pixel differences instead of the host image's histogram. Many peak points exist around the bin zero in this histogram due to the similarity of adjacent pixel values. Besides, many zero points exist in both sides of the bin zero. Here the peak point refers to the height of histogram bin with the largest statistical value (i.e., the count falling in the corresponding bin), and the zero point means the histogram bin with zero value. In our case, all the differences are classified into levels of[−255, 255] and each level corresponds to a histogram bin. Henceit is reasonable to modify the histogram with a multilevel mechanism for hiding more secret data. In decoder, the host image pixels are recovered one by one. That is, each pixel is recovered aided by its previously

recovered neighbor. Meanwhile, the secret data is extracted from the marked adjacent pixels' differences.

2.3. Efficient image inpainting using adaptive edge-preserving propagation

An image inpainting algorithm based on adaptive edge-preserving propagation for structure repairing. Neighbouring information is progressively propagated into damaged region. The optimal size and location of the window containing damaged pixel are adaptively chosen according to the intact degree and colour distribution. To preserve sharpness of edges, contributing weights of the pixels in neighbouring window are decided by their direction with isophote and distance with damaged pixels. Compared with typical partial differential equation (PDE)-based methods, the proposed approach is more concise and efficient, and can give satisfactory results for structural information repairing. Experiments are carried out to show effectiveness of the method.

3.CONCLUSION

In order to enhance the availability of embeddable space and reduce the prediction error simultaneously, an adaptive strategy based on the distribution characteristics of image content was adopted, in which fewer reference pixels were chosen in the smooth regions of cover images and more reference pixels were chosen in the complex regions. According to the reference pixels that were chosen, the PDE-based in painting algorithm using the CDD model can generate the prediction image effectively that has the similar structural and geometric information as the cover image. Through the 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. In this paper , the merge and sort algorithm used to split image into two blocks then data will be hided on both

blocks then image get compresssed into image that image will same like original image that is stego image.

REFERENCES

[1] 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.

[2.] 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.

[3] 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

[4] M. Fallahpour, D. Megias, and M. Ghanbari, "Reversible and high capacity data hiding in medical images," *IET Image Process.*, vol. 5,no. 2, pp. 190–197, 2011.

[5] 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.

