Steganography- A Technique to Hide the Information using LSB Algorithm

C.Dhivya ,G.Sharmila ,S.Keerthanadevi ,S. Gangalakshmi,M.E
Srividya College Of Engineering And Technology

ABSTRACT

In this paper, a simple and robust watermarkingalgorithm is presented by using the third and the fourthleast significant bits (LSB) technique. The proposedalgorithm is more robust than the traditionalLSB techniquein hiding the data inside the image. Using the proposedalgorithm, we will embed two bits in the third and fourthLSB. Experimental results show that the quality of thewatermarked image is higher.

I INTRODUCTION

Steganography is the art and science of communicating in a way which hides the existence of the communication. Steganography plays an important role in information security. It is the art of invisible communication by concealing information inside other information. The term steganography is derived from Greek and literally means “covered writing”. A Steganography system consists of three elements: cover image (which hides the secret message), the secret message and the stegano-image(which is the cover object with message embedded inside it).

Digital watermarking is the technique of embedding a digital signal (audio, video or image) or hide a small amount ofdigital data which cannot be easily removed is called digital watermarking. Digital watermarking is also called dataembedding. Watermarking can be applied to images, audio, video and to any software also. Digital watermarking is usedto hide the information inside a signal, which cannot be easily extracted by the third party. Its widely used application iscopyright protection of digital information. It is different from the encryption in the sense that it allows the user to access,view and interpret the signal but protect the ownership of the content.Figure represents the general framework ofwatermarking.

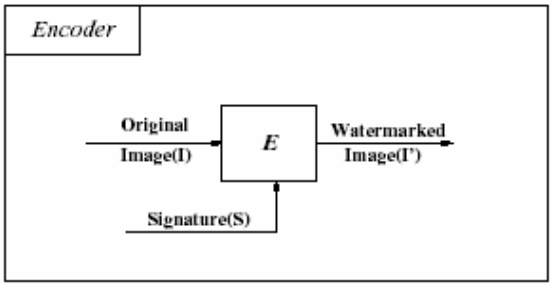


Fig. encoding process of watermarking

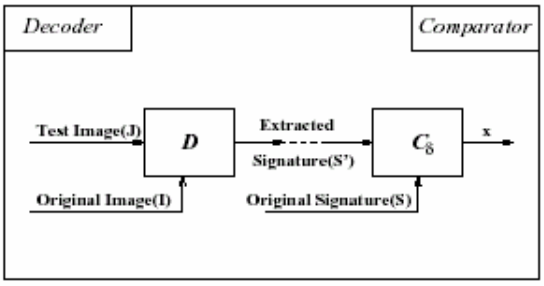


Fig. decoding process of watermarking

The Steganography system which uses an image as the cover, there are several techniques to conceal information inside cover-image. The spatial domain techniques manipulate the cover-image pixel bit values to embed the secret information. The secret bits are written directly to the cover image pixel bytes. Consequently, the spatial domain techniques are simple and easy to implement.

II LITERATURE REVIEW

ErsinElbasi et al embed the watermark in a tree structure in the Discrete Wavelet Transform domain. For watermark embedding, the two level DWT decomposition of an NxN gray scale image I is computed. The same PRN sequence is embedded into the DWT coefficients higher than a given threshold T1 in the LL2 and HH2 bands. The watermark is also embedded into the children of DWT coefficients. The original DWT coefficients are replaced by the modified DWT coefficients. The final step is to compute the inverse DWT to obtain the watermarked image I'. For watermark detection, the DWT of the watermarked and possibly attacked image I* is computed. All the DWT coefficients higher than a given threshold T2 in the LL2 and HH2 bands are selected. Then the sum Z of all attacked DWT coefficients multiplied by either the embedded watermark or other random PRN sequence is computed, divided by the length of the PRN sequence. The sum is also computed for the children of modified DWT coefficients. A predefined threshold T is chosen for LL2 and HH2 bands and the HH1 band. In each band, if Z exceeds T, the conclusion is that the watermark is present.

Gil-Je Lee et al, presented a simple and robust watermarking scheme by using random mapping function. The idea of the proposed algorithm is watermark embedding which can be more robust than the traditional LSB technique. Using the proposed algorithm, it makes the secure random coordinate of cover image to increase the robustness of the watermarked image. SaeidFazli et al, investigated trade-off between imperceptibility and robustness of LSB watermarking. In this algorithm significant bit-planes of the watermark image are put instead of lower bit-planes of the asset picture. So, they investigate the effect of image compression on the watermark, and finally they evaluate the robustness and imperceptibility by measuring the distortion due to watermarking using two quality metrics: MSE and 1 – SSIM.

III PROPOSED SYSTEM

The Least Significant Bit (LSB) is one of themain techniques in spatial domain image Steganography. The LSB is the lowest significant bit in the byte value of the image pixel. The LSB based image steganography embeds the secret in the least

significant bits of pixel values of the cover image (CVR).

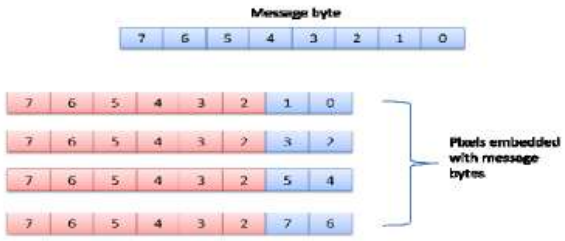


Fig.Proposed LSB Algorithm

The concept of LSB Embedding is simple. It exploits the fact that the level of precision in many image formats is far greater than that perceivable by average human vision. Therefore, an altered image with slight variations in its colors will be indistinguishable from the original by a human being, just by looking at it. In conventional LSB technique, which requires eight bytes of pixels to store 1byte of secret data but in proposed LSB technique, just four bytes of pixels are sufficient to hold one message byte. Rest of the bits in the pixels remains the same.

The principle of embedding is fairly simple and effective. If we use a grayscale bitmap image, which is 8- bit, we would need to read in the file and then add data to the least significant bits of each pixel, in every 8-bit pixel. In a grayscale image each pixel is represented by 1byte consist of 8 bits. It can represent 256 gray colors between the black which is 0 to
the white which is 255. The principle of encoding uses the Least Significant Bit of each of these bytes, the bit on the far right side. If data is encoded to only the last two significant bits (which are the first and second LSB) of each color component it is most likely not going to be detectable; the human retina becomes the limiting factor in viewing pictures. For the sake of this example only the least significant bit of each pixel will be used for embedding information. If the pixel value is 138 which is the value 10000110 in binary and the watermark bit is 1, the value of the pixel will be 10000111 in binary which is 139 in decimal. In this example we change the underline pixel. Features of LSB (Least-Significant-Bit)

Advantages:

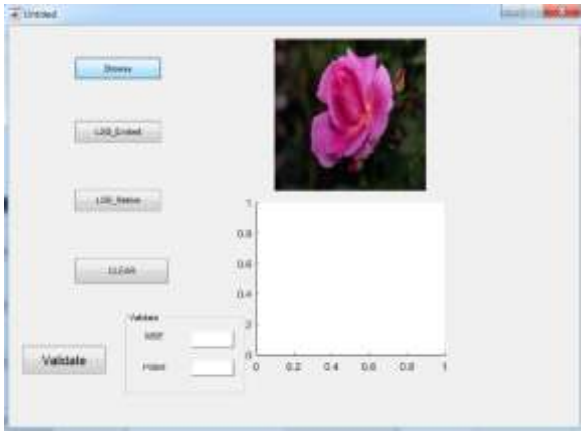
a. It is simple to understand

b. Easy to implement

c. It results in stego-images that contain hidden data yet appear to be of high visual fidelity.

IV SIMULATION RESULTS

MATLAB is a high-performance language for technical computing. Matlab function is an easy to use, user interface function that guides a user through the process of either encoding & decoding a



message into or from the image respectively.

Fig cover image

In this paper,Matlab is implemented for processing LSB steganography technique with different frame size 256*256, 128*128, 64*64 and simulation results are shown.

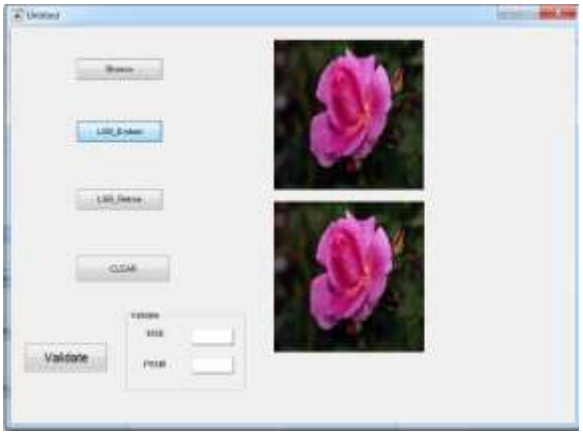


fig Embedded Image

Fig Extracted Image

Fig Performance Matrix

CONCLUSION

This paper proposed a new LSB based digitalwatermarking scheme with the fourth and third LSB inthe grayscale image. After we have embedded the secretdata in the third and fourth LSB in the image in determinecoordinates, we got watermarked image withoutnoticeable distortion on it. Therefore, this digitalwatermarking algorithm can be used to hide data insideimage.

image.

REFERENCES

[1] I.J. Cox, M.L. Miller, J.A. Bloom, Digital watermarking, Morgan Kaufmann, 2001.

[2] Mohannad Ahmad AbdulAziz Al-Dharrab," Benchmarking Framework for Software Watermarking" King Fahd University ofPetroleum and Minerals, Dhahran, Saudi Arabia, June 2005.

[3] J. Nagra, C. Thomborson, and C. Collberg, (2002), A functionaltaxonomy for software watermark- ing, in M. Oudshoorn, ed.,`Proc. 25th Australasian Computer Science Conference 2002',ACS, pp. 177-186.

[4] ErsinElbasi and Ahmet M. Eskicioglu," A SEMI-BLINDWATERMARKING SCHEME FOR IMAGES USING A TREE STRUCTURE", Sarnoff Symposium, 2006 IEEE

[5] SaeidFazli and GholamrezaKhodaverdi, "Trade-off betweenImperceptibility and Robustness of LSB Watermarking using SSIM Quality Metrics", 978-0-7695-3944-7/10 $26.00 © 2010IEEE DOI 10.1109/ICMV.2009.68

[6] Gil-Je Lee, Eun-Jun Yoon, Kee-Young Yoo, "A new LSB basedDigitalWatermarking Scheme with Random Mapping Function",978-0-7695-3427-5/08 $25.00 © 2008 IEEE DOI 10.1109/UMC.2008.33

[7] Gaurav Bhatnagar, Balasubramanian Raman," A new robustreference watermarking scheme based on DWT-SVD", 0920-5489/$ – see front matter © 2008 Elsevier B.V. All rights reserved. doi:10.1016/j.csi.2008.09.031