A Simplified Approach For Implementation Of Digital Watermarking

Vivek Upneja
MTECH* Jagannath University Computer science
Jaipur, India
E-mail: viveku12@gmail.com

Abstract: Digital watermarking is a technique in which we embed a watermark image into a host image in order to maintain credibility and authencity of the image and thus giving the owner his due credit as internet is vast and full of fraud and malicious people .So we need a technique like watermarking for ownership protection. Many basic techniques like spatial domain and spectral domain watermarking are available but they are quite vulnerable and can easily be detected. In this paper i would describe a robust invisible digital water marking technique which is less vulnerable and also the distortion is quite less and can be applied to all types of image with ease of understanding and implementation .By using the matrix nature of image and by applying matrix operation the work of watermarking has been quite simplified and thus we get a desirable output with least variations.

Keywords: Cover image , invisible watermark ,watermark value, PSNR

I. INTRODUCTION

In the recent, development of new devices and powerful software have made it easy for people worldwide to access create, and manipulate multimedia data over the internet. Internet and wireless networks offer widespread channels to deliver and to exchange much multimedia information. However, the ease offered by the information technology era cannot be fully realized without proper security and protection of multimedia data.[1]
Their are two types of watermark visible and invisible. A visible watermark is a visible translucent image that is overlaid on the primary image. Visible watermarks change the signal to much amount such that the watermarked signal is totally different from the actual signal, for example. the logo or seal of the organization allows the primary image to be viewed, but still marks it clearly as the property of the owning organization**.** An invisible watermark is an embedded image which cannot be seen, but which can be detected algorithmically. Invisible watermarks do not change the signal to a perceptually great extent, i.e., there are only small variations in the output signal. An example of an invisible watermark is when some bits are added to an image modifying only its least significant bits[3].

Requirements of a watermark:-
a. Imperceptibility: In watermarking, we traditionally seek high fidelity, i.e. the Watermarked image must look or sound like the original.
b. Robustness: It is more a property and not a requirement of watermarking. The watermark should be able to survive any reasonable processing inflicted upon the cover image. (carrier here refers to the content being watermarked).
c. Security: The watermarked image should not reveal any clues of the presence of the watermark, with respect to un-authorized detection, or indefectibility [2]
d. Efficiency: Efficiency is the speed of the algorithm for embedding and extracting the watermark.
e. Capacity: It is the extent or size of watermark a that a cover image can hold.

II RELATED WORK

After studying some of the most used techniques like spatial and frequency domain techniques used for watermarking.
Only spatial techniques are not robust to some attacks to the signal like cropping and zooming, whereas most frequency domain techniques and mixed-domain techniques are quite robust to such attacks.[2]
LSB Embedding: LSB encoding is very simple and has been used for a variety of purposes. In this method the least significant bit of every component is replaced by the watermark information bit. This method is widely accepted it was also used in attacks on 9/11 in America so it is obsolete or outdated old fashioned, easily perceptible and also as we are using only least significant bit so this method could store only small out of information and easily attacked.[7]

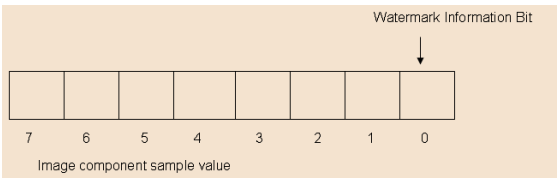

Fig. LSB encoding

CDMA Spread Spectrum: Code Division Multiple Access (CDMA) is a transmission technique in which the frequency spectrum of a data-signal is spread using a code uncorrelated with that signal and unique to every addressee. It is used in spread spectrum systems to enable multiple-access. [6]
The characteristics of a watermarking algorithm depends upon the application is designed for.

III Proposed Technique

In this work I am taking an image as a cover image and taking an watermark image and embedding the watermark image into the cover image as this is the invisible

watermark technique and then applying a reverse process to extract the original watermark from the watermarked image. After that we are calculating the PSNR value from that extracted watermark image.

Watermark Embedding Algorithm

1. Read the RGB cover image. **A(i,j)**
2. Read the watermark which we have to embed in cover image. **B(i , j)**
3. Resize the watermark image to cover image.
4. Create a zeros matrix of cover image size. **C (i , j)**
5. Convert this cover image and watermark image to matrix form.
6. Select the minimum watermark value for PSNR calculation.
7. Add the cover image and resized watermark image matrix and then assign it to zeros matrix by the factor of watermark value. (Embedding is done).
   C(i , j) =A(i , j) + B(i , j) * Watermark Value
8. The resultant matrix is watermarked image matrix.
9. Convert this watermarked image matrix to its image format.
10. Finally we have obtained the watermarked image.

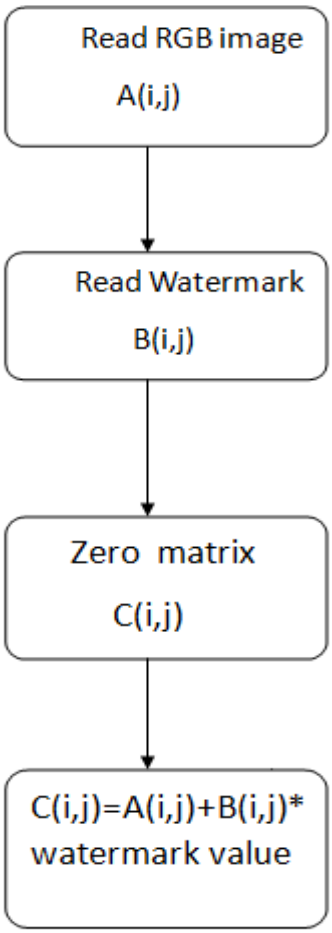

Fig. Flowchart for embedding

Watermarking Extraction algorithm

1. Read the watermarked image from the embedding process. **C(i , j)**
2. Read the cover image. **A(i , j)**
3. Create a zeros matrix of cover image size. **D(i , j)**
4. Subtract the watermarked image from cover image matrix and assign it to zeros matrix.

   D(i , j) = C(i , j) – A(i , j)/Watermark value
5. The resultant matrix is watermark image matrix.
6. Convert this watermark image matrix to its image format.
7. Finally we have obtained the watermark image

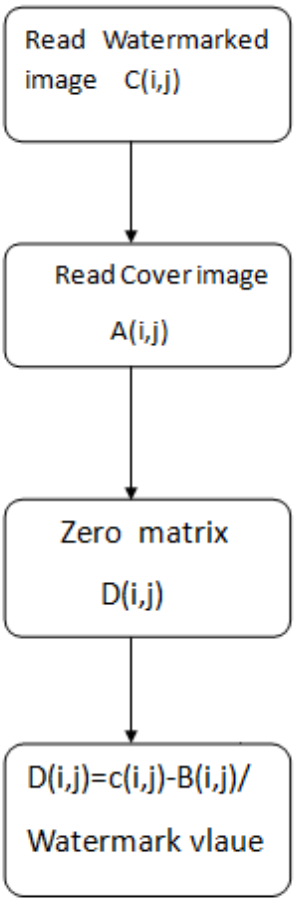

Fig. Flowchart for extracting

IV Result and Implementation

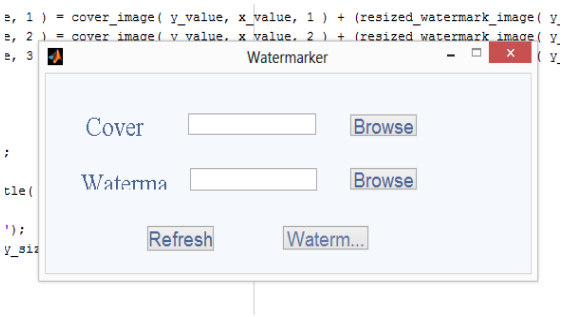

Fig.Interface for implementation

Fig: Cover Image

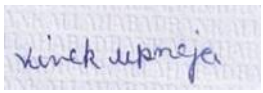

Fig.watermark

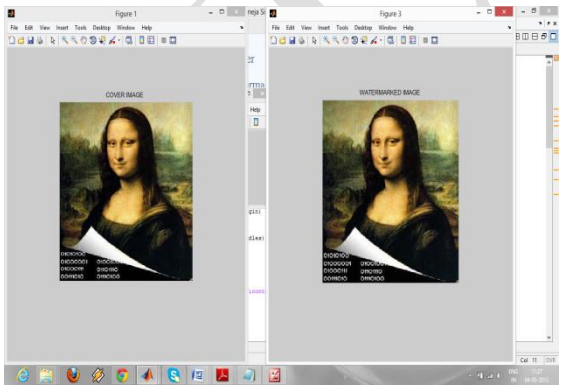

Fig:Cover image and watermarked image

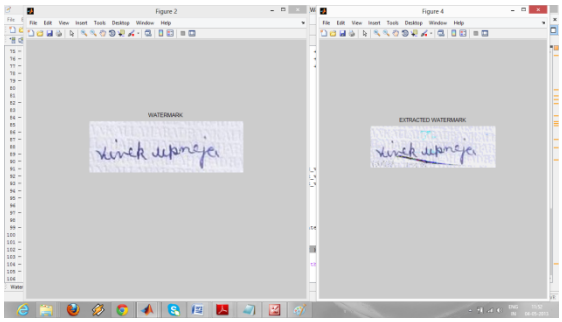

Fig:Watermark and Extracted watermark

PSNR calculations

The phrase peak signal-to-noise ratio, often abbreviated PSNR, is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale.

The PSNR is most commonly used as a measure of quality of reconstruction of lossy compression codecs (e.g., for image compression). The signal in this case is the original data, and the noise is the error introduced by compression. When comparing compression codecs it is used as an approximation to human perception of reconstruction quality, therefore in some cases one reconstruction may appear to be closer to the original than another, even though it has a lower PSNR (a higher PSNR would normally indicate that the reconstruction is of higher quality). One has to be extremely careful with the range of validity of this metric; it is only conclusively valid when it is used to compare results from the same codec (or codec type) and same content.[5] . It is most easily defined via the mean squared error (MSE) [8] which for two m×n monochrome images I and K where one of the images is considered a noisy approximation of the other is defined as:

```
Mean_square_error = sum( sum( sum( ( watermark_image - extracted watermark image).^2))) / double( watermark_x_size * watermark_y_size * 3 )
```

The PSNR between the original watermark and the extracted watermark taken from the watermarked image:

PSNR =35.1185db

V CONCLUSION

The presented technique is robust and very less vulnerable to various attacks.

My technique is more robust as compared to the contemporary methods. This can be substantiated by the fact that when we watermark an image and in the next step try to extract the same, we get an exact watermark as was embedded and distortion of the image is non noticeable. This peculiar feature was achieved by taking minimum value of the watermark.

This technique could be made more secure by applying cryptography on the watermark and then applying watermark to the image.

Acknowledgement

I would like to thanks all my faculty of jagannath university jaipur for their encouragement.

REFERENCES

[1] Ching-Yung Lin,"Watermarking and Digital Signature Techniques for Multimedia Authentication and Copyright Protection", PhD Thesis, ColumbiaUniversity, 2000

[2] R. G. van Schyndel, A. Z Tirkel, and ***C.*** E Osborne, "A digital watermark", ***in*** *Proceedings, IEEE International Conference on Image Processing*, vol. 11, pp. 86-90, 1994.

[3] R. J. Anderson and F. A. P. Petitcolas. (1999) Information Hiding: An Annotated Bibliography. [Online]. Available: http://www.cl.cam.ac.uk/~fapp2/ steganography/ bibliography/

[4] Robust LSB watermarking optimized for local structural similarity" in Electrical Engineering (ICEE), 2011 19th Iranian Conference, May 2011.

[5] Digital watermarking algorithm using LSB" in Computer Applications and Industrial Electronics (ICCAIE), 2010

[6] Harlekar, S., and Kak, S.C., "Performance analysis of a d-sequence based direct sequence CDMA system", LSU report,

[7]] Techniques and applications of digital watermarking and Conte1nt protection by Michael Konrad Arnold, Martin .

[8] J. E. Farrell, Image quality evaluation in colour imaging: vision and technology. MacDonald, L.W. and Luo, M.R. (Eds.), John Wiley, pp. 285-313, 1999

AUTHOR'S BIOGRAPHIES

Completed B.Tech in 2010, pursuing Mtech from jagannath university in computer science.