Watermarking Embedding in Spatial Domain

Prabhjot Kaur
ECE Deptt. DVIET, Karnal

Reena
Asst.Prof, DVIET, Karnal

Abstract: Due to improvement in imaging technology and the ease with which digital content can be reproduced and manipulated there is a strong need for a digital copyright mechanism to be put in place. Digital Watermarking is being seen as a potential solution to this problem. Digital authenticate it. In spatial domain technique watermarking is a technology which embeds a watermark signal into the host image to the watermark image is embedded into the cover image. The spatial domain is slightly modifies the pixels of one or two randomly selected subsets of an image. Modification might include flipping the low order bit of each pixel It deals with hiding secret bits of information with a digital content as a cover.

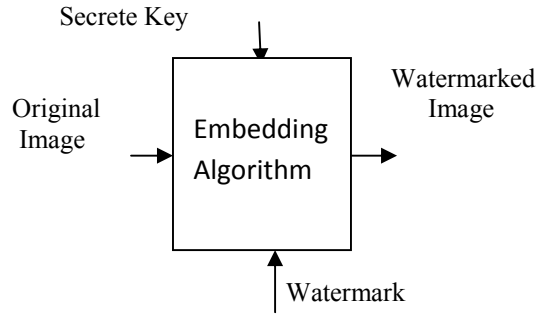
Keywords: Spatial domain, least significant bits, most significant bits, watermarked image,

I Introduction

With the ever-growing expansion of digital multimedia and the internet digitizing of visual data such as images and video has become popular .However ,this advancement in technology has double impact .First impact is that ,it has permitted faster and more efficient storage ,transfer and processing lf digital data. The second impact is, duplication and manipulation of digital contents has also become very easy and undetectable ,which allows fast and error free movement of any unauthorized digital data and possibly manipulated copy of such information, grow in popularity in the recent years, security concerns over Copyright protection of digital multimedia data has also been increasingly emphasized. One of the most promising solutions appears to add author information (watermark) into the visual data as a secondary signal that is not perceivable and is bonded so well with the original data that it is undividable. Techniques to embed and recover such secondary information or stamps (called watermark) is digital watermarking.

II Watermark Embedding and Extraction

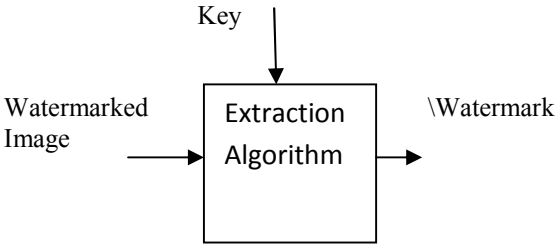
A watermarking algorithm embeds a visible or invisible watermark in a given multimedia object. In the watermarking embedding scheme



"Fig. 1: Watermarking Embedding"

The input to the scheme is watermark, the cover image data and optional or secret key. The watermark can be any nature, such as a number, text, an image. The secret or public key is used to enforce the security

For the detection scheme the input is watermarked image, watermark image and optional or secrete key and depends upon the original data and original watermark.



"Fig. 2: Watermarking Extraction"

The output of the watermark recovery process is either the recovered watermark or some kind of confidence measure indicating how likely it is for the given watermark image at the input to be present in the data under inspection.

A. Evaluation parameters of a watermarking technique

Mean Square Error

The mean square error between the original image f (m, n) and the reconstructed image g (m, n) is given by

$$MSE=\frac{1}{N}\times\frac{1}{M}\sum_{n=0}^{N-1}\sum_{m=0}^{M-1}(f(m,n)-g(m,n)^2)$$

Here N×M represents the size of the image.

The MSE is a very useful measure as it gives an average value of the energy lost in lossy compression of the original image. A human observing two images affected by the same type of degradation will generally judge the one with smaller MSE to be closer to the original. A very small MSE can be taken to mean that the image is very closer to the original. Original image and reconstructed image (watermarked image) are the grayscale of the

images to compare to measure value of the energy lost in lossy compression of the original image.

Peak Signal to Noise Ratio

A more subjective qualitative measurement of distortion is the peak signal to noise ratio. The peak signal to noise ratio (PSNR) is used to evaluate the image quality by calculating the mean square error (MSE) between the images to compare.

$$PSNR=10\times \log_{10}[\frac{2^{b}-1)^{2}}{MSE}]$$

For an 8-bit image, b=8 which gives the PSNR value as

$$PSNR=10\times\log_{10}[\frac{(255)^{2}}{MSE}]$$

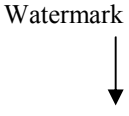
The PSNR is expressed in dB. The PSNR evaluation parameter is superior measurement method. It uses a constant value in which to compare the noise against instead of a fluctuating signal. We calculate PSNR between original image and watermarked image that we output from the embedding process. The higher the PSNR shows the better quality of watermarked image. So, if we have bigger PSNR, it shows least difference between original image and watermarked image that shows more robustness' against attacks.

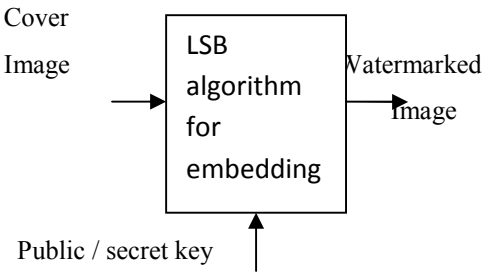
III WATERMARKING IN SPATIAL DOMAIN

In spatial domain technique the watermark image is embedded into the cover image. The spatial domain is slightly modifies the pixels of one or two randomly selected subsets of an image. Modification might include flipping the low order bit of each pixel. This concept is used most often when discussing the frequency with which image values change that is over how many pixels does a cycle of periodically repeating intensity variations occur. One would refer to the number of pixels over which a pattern repeats in the spatial domain.

A. LSB-MSB Watermark Embedding Scheme

LSB coding is one of the earliest methods. It can be applied to any form of watermarking. In this method the LSB of the carrier signal is substituted with the watermark. The bits are embedded in a sequence which acts as the key. The watermark encoder first selects a subset of pixel values on which the watermark has to be embedded. The cover image and the watermark image are the inputs for the watermarking embedding process. LSB-MSB approach of LSB invisible watermarking scheme, uses the least significant bits of the original image is masked and substituted by the most significant bits of the watermark image. LSB-MSB watermarking scheme is used to embed invisible watermark in famous test image. These approaches decrease the authentication distortion and increase the efficiency of secure authentication. So implementation in this process by embedding data as pixels into the image and then provide authentication by comparing the original and the embed image. The public key is used to enforce security if the watermark image is not to be read by unauthorized parties, a key can be used to protect the watermark. The output of the watermarking scheme is converted to watermarked image.





"Fig. 3: Watermarking Embedding Scheme "

The figure 3 shows the LSB watermarking embedding scheme. The cover image, watermark image and the public key are the inputs for the watermarking embedding process. The public key is an optional key for the LSB watermarking embedding scheme. In this process the invisible watermark is embedded into the standard test image.

Algorithm for LSB-MSB embedding watermarking scheme

(1) Read image i.e. cover image.

(2) Calculate its size let $m_1 * m_2$.

(3) Read watermark image i.e. CS image.

(4) Calculate its size let $n_1 * n_2$.

(5) If the $((n_1 * n_2) \geq (m_1 * m_2))$

Print (watermark not fit in to cover image).
Else, follow step number 6 to 10.

(6) Reset the content of LSB bit plane in the cover image...

(7) Calculate the value of MSE, PSNR & Correlation between cover image and watermark image\

IV SIMULATION OF LSB-MSB ALGORITHM

The famous standard test image: Cameraman (256×256) and shown in figure 4.1 is taken as the cover image or base image to embed a (120×100) watermark image. N LSB MSB watermarking scheme is used to embed watermark. Where n is the number of bits used. It is quite obvious that smaller the value of n, lesser is the deterioration in the quality of the image. As we increase the number of bits, the image quality further degrades and becomes more visible to the naked eye n LSB MSB watermarking scheme is used to embed invisible watermark in famous test image. Where n is the number of bits used. It is quite obvious that smaller the value of n, lesser is the deterioration in the quality of the image. As we increase the number of bits, the image quality further degrades and becomes more visible to the naked eye. By changing the value of the variable 'bits' from 1 to 7, we calculate the values of PSNR and MSE which shows the quality of the image.

"Fig. 4.1: (a) Cover Image (Cameraman) "

"Fig 4.1: (b) Watermark"

"Fig. 4.1: (a) Cover Image (Cameraman), (b) Watermark "

CASE-1 Using 1 LSB-MSB algorithm for embedding invisible watermarked image

MSE=0.0503, PSNR=61.112db

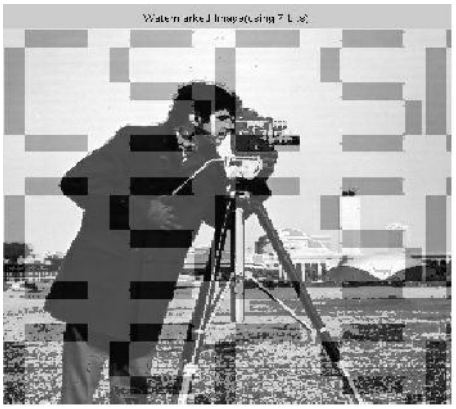
"Fig. 4.2: Recovered Watermarked Images Using 1 LSB-MSB Algorithm"

CASE-2 Using 3 LSB-MSB algorithms for embedding invisible watermarked image

MSE=0.788, PSNR=49.164db

"Fig**. 4.3: Recovered Watermarked Images Using 3 LSB-MSB Algorithms"**

CASE-3 Using 7 LSB - MSB algorithm for embedding invisible watermarked image



MSE=14.781, PSNR=35.335db

"Fig. 4.4: Recovered Watermarked Images Using 7 LSB-MSB Algorithms

.

Approaches	Cameraman Watermarked Image	
	MSE	**PSNR**
1 LSB-MSB	0.050	61.11
2 LSB-MSB	0.201	55.08
3 LSB-MSB	0.788	49.16
4 LSB-MSB	3.446	42.75
5 LSB-MSB	11.54	37.50
6 LSB-MSB	12.11	37.29
7 LSB-MSB	14.78	35.33

" Table 4.1 Results of LSB-MSB Algorithm**"**

V CONCLUSION AND RESULTS

The table 4.1 shows that when we use 1 LSB-MSB algorithm the value of MSE and PSNR is 0.050 and 61.11 db for cameraman image. And when we use 2 LSB-MSB algorithms the value of the MSE and PSNR is 0.201 and 55.08 db for the cameraman image. When number of using bits increases, the value of PSNR is decreases and the value of MSE is increase

REFERENCES

[1] Yanqun Zhang "Digital Watermarking Technology: A Review" 2009 ETP International Conference on Future Computer and Communication

[2] Houtan Haddad Larijani and Gholamali Rezai Rad "A New Spatial Domain Algorithm for gray scale images watermarking" Proceedings of the International Conference on Computer
and Communication Engineering 2008 May 13-15, 2008 Kuala Lumpur, Malaysia

[3] Ibrahim Nasser, Ying Weng, Jianmin Jiang "Novel Multiple Spatial Watermarking Technique In Color Images "Fifth International Conference on Information Technology: New Generations

[4] Munesh Chandra "A DWT Domain Visible Watermarking Techniques for Digital Images"2010 International Conference on Electronics and Information Engineering (ICEIE2010)

[5] Vikas Saxena, J.P Gupta "Collusion Attack Resistant Watermarking Scheme for Colored Images using DCT" IAENG International Journal of Computer Science, 34:2, IJCS_34 _2_02

[6] Reza Mortezaei, Mohsen Ebrahimi "A new lossless watermarking Scheme based on fuzzy integral and DCT domain"2010 International Conference on Electronics and Information Engineering (ICEIE 2010)

[7] Afzel Noore "An Improved Digital Watermarking Technique for Protecting JPEG images" WPM P2.08 0-7803-7721-4/ 03 □ 2003 IEEE

[8]Dhruv Arya" A Survey Wavelet Domain of Frequency and
Digital Watermarking Techniques" International Journal of Scientific & Engineering Research, Volume 1, Issue 2, November-2010 1 ISSN 2229-5518

[9] Mansi Hasija, Alka Jindal" Contrast of Watermarking Techniques in
different domains" IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 2, May 2011 ISSN (Online): 1694-0814

Prabhjot Kaur received her B.Tech degree in Electronics and communication from Doon Valley institute of engineering and technology under Kurukshetra Universty. At present, she is pursuing her Master in Technology.Her research works includes Image Processing.

Er. Reena received her B.Tech degree in Electronics and communication from Doon Valley institute of engineering and technology under Kurukshetra Universty. She received her M.Tech degree from UIET, Kurukshetra. She was assistant professor in UIET, Kurukshetra for six months. At present she is working as an assistant professor in Doon valley Institute of engineering and technology from last one year and 4 months.