ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

Capacity and Security analysis of watermark image truly imperceptible

Monika Verma[1], Praveen Yadav[2]

Student, M.Tech C.S.E., B.I.T.S. Bhiwani, India[1]

Asst. Professor Dept. of C.S.E., B.I.T.S. Bhiwani, India[2]

Abstract: In this paper capacity and security of invisible watermarked is enhanced. It provides secure, imperceptible robust communication of high amount of information by hiding secret bits of information with a digital content as a cover .Objective of information hiding is to embedding secret information as much as possible without perception of carrier is affected. To hide the secure data information hiding algorithm LSB bit Based on high frequency domain in color image is proposed which provides high imperceptibility and high capacity of information hiding. It allows adding high amount of hidden copyright notices or other verification messages as much as possible to images which is imperceptible to human eyes.

Keywords: Digital Watermarking, Invisible Watermarking, Security, Capacity, Imperceptibility, PSNR, Frequency domain.

I Introduction

With increasing use of Internet and effortless copying, tempering and distribution of digital data, copyright protection for multimedia has become important issue. One of the most promising solutions appears to add author's information (Watermark) [1] into visual data as a secondary signal that is not perceivable and is bonded so well with original data that is inseparable.

Digital Watermarking is a technique which allows an individual to add hidden copyright notices or other verification messages to digital audio, video or images signal and documents [2]. Hidden information can be use to protect the copyright ownership of image. The purpose of Information hiding is to ensure that hidden information not arise the attacker's attention thereby reduce the possibility of being encroached and get rid of the fatal flaw in the data encryption technology. Currently the Carrier used as information hiding has many different format such as text, images, audio or video etc. But there are no essential differences in the used method. Currently image is carrier of information hiding used to hide storage and hide communication most frequently because its redundancy has a large space. In the process of hidden storage, the researcher's goal is to hide information in image as much as possible on the premise of imperceptibly of information hiding [3].There are many hidden algorithms but the embedding capacity and security of information hiding remains to be improved. This article presents the way of solution to above problem by a new algorithm based on frequency domain [4] to color image. This algorithm is used for embedding multiple watermarks into image and extraction of watermarks from image is proposed.

This paper is divided into six sections. Section 2 describes Proposed System. Section 3 describes Research Methodology, Watermark embedding and extracting Method. Section 4 includes Implementation and Watermark embedding and extracting algorithms. Section 5 describes experimental results. Conclusions are made in section 6.

II PROPOSED SYSTEM

Security is always the major issues while transferring data over the network. Watermarking technique provides a secure data transmission over the network. Without affecting the imperceptibility of image, high security and capacity of Watermark data are very important issue to be tackled. This section describe proposed Watermarking algorithm for increasing the security and capacity of Watermarked data. The proposed method embed the watermark at high frequency using Watermarking technique at frequency domain [5].The capacity of data can be achieved by dividing the cover image in a series of segments [6].For representing the segments of image there is one metric for each segment. Secure data will be stored in last 3 bits of each smaller segment separately. The data is store on the high intensity pixel frequency of LSB [7] in each area. The Capacity of text embedding depends upon image size. After calculating the capacity of given text multiple text file can be add into the image [8]. Security is being increased by selection of random image segment to store the data behind the segment of image [9].The selection of random segment is done by using random generator function. Selection of random segments for hiding the data makes impossible for intruder to reveal the data until they do not know where the data is hiding.

III RESEARCH METHODOLOGY

Research methodology is the way of systematically solving the research problem. It is science of studying how research is conducted scientifically.

A. Research Approach

Digital Watermarking method can be divided into two groups, the spatial domain method and the frequency domain method. The spatial domain watermarking scheme [10] involves embedding watermarks by directly changing pixel values of host image. Spatial domain algorithms are simple and watermark can be damage easily.

Frequency domain watermarking scheme involves embedding watermark by modifying the transform co-efficient after the image has been transformed to the transform domain. Frequency domain algorithms can resist versus intensity attack and watermark information cannot be damaged easily. Research approach used for this proposed work is watermarking at frequency domain [11].For embedding watermark into image invisible watermarking [12] is used. In Invisible digital watermarking information is added as digital data to audio, picture and video but it cannot be perceived as such[13](although it may be possible to detect that some amount of information is hidden in the signal).

B. Embedding Method

In our approach watermark embedding process is described as follows:-The first work is to get the input text and source image. The given data is converted into its binary values and those binary values are changed into numenic code. The purpose of this data conversion is to make the given data not understandable to the hacker. Now the actual watermarking approach will be apply to hide the data over the image and the output is watermarked word document.

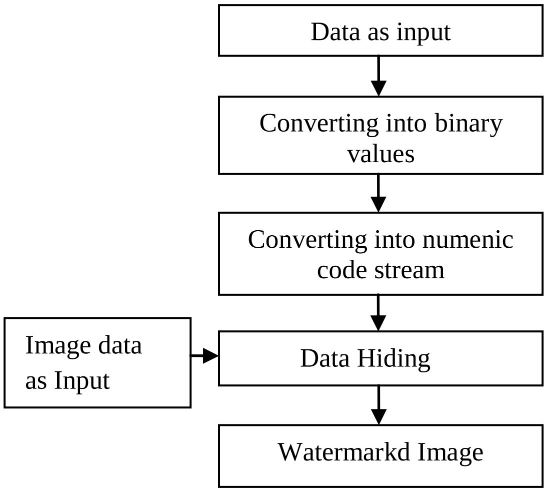
Data as input
Converting into binary values
Converting into numenic code stream
Image data as Input
Data Hiding
Watermarkd Image

Fig: 1 Embedding process of watermark into image.

C. Extracting Method

In this process input is image with data hidden inside and the hidden data is extracted by giving a correct key. The extracted data will be in the form of numenic code stream so they are converted into binary values and using those binary values data is formed.

In this process the first work is to extract the watermarked image. Now perform the algorithm in reverse order to scan it and to retrieve the data back. Once data is retrieved in binary format will be stored to the specified location.

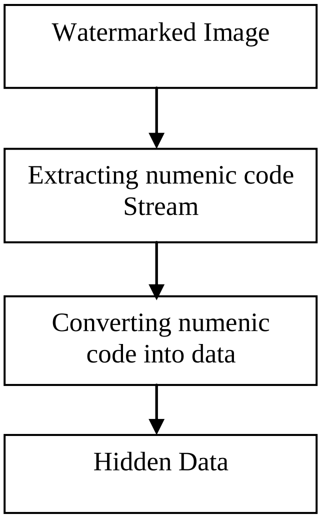
Watermarked Image
Extracting numenic code Stream
Converting numenic code into data
Hidden Data

Fig: 2 Extraction process of watermark from watermarked image

IV IMPLEMENTATION

Algorithm for embedding Watermark:-Matrix Encoding technique is used for embedding data into image. Mi (n*n): The sub image matrix. Each element of Mi will be referred according to its row and column as P(r, c). Ni (n*n): The selected LSB values matrix with row and column as (i, j) and embed the text data, save into Ni matrix.

The number (m) of bits used to hide the data could be of two or three bits, so elements of the matrix Ni will be all less than or equal to (2m-1).If three LSBs are used to hide the data, then the elements of Ni are all less than or equal to (2m -1). Depending on the size of the image and the number of bits to hide in that image, the size of the matrix (n*n) is determined ; so n could be 2, then Ki, Mi, Ni will all be of size (2*2); and going to embed (m-bits) within (96 bit); (m could be 2 or 3 bits) If n=3 then Ki, Mi, Ni will all be of size (3*3), and going to embed m-bits within 216 bit; and if n=4, then going to embed m-bits within 384 bit; and so on.

A. Algorithm for Embedding the Watermark

- Read the colored (RGB) image and divide the image into (4 x 4) sub images Mi, (i=1, 2, 3...) ;(each sub image contain 16 pixels).

- Use a random generator function to determine the position to start hiding the data.
- For each sub image Mi, the following process will be done:

i. Convert least three bits from the blue color byte to decimal for each pixel P(r, c) in Ni, the results will be saved in Ni (4x4) decimal matrix. All elements of Ni are in the range (0…2m -1).

ii. To hide the converted binary form 011110101110…., convert each three bits to the equivalent decimal number (i.e. 011 is converted to D= 3), then find V and sign S.

iii. If sign S is negative, add the value of V to one of the pixels P(r, c) in the sub image Mi, the values of (r, c) are calculated depending on the values of (i, j) of the point Ni.

iv. Otherwise (if S is positive) subtract value of V from the pixel P(r, c). In sub image Mi, the values of (r, c) are calculated depending on values of (i, j) of the point Ni. This process will force the value of modulation function to be equal to the embedded data.

B. Algorithm for Extracting the Watermark

- Read the watermarked image
- Divide the image into (4 x 4) sub images Mi, (i=1, 2…); (each sub image contains 16 pixels).
- Use a random generator function to determine the position to start hiding the data.
- For each sub image Mi, the following process will be done:

(Repeat following process)

i. Read data area from the sub matrix and retrieve as an array of bits.

ii. Reverse the Encoding Process by reperforming Ex-or operation on the data bits 011110101110….., convert each three bits to the equivalent decimal number (i.e. 011 is converted to D= 3), then find V and sign S.

iii. If the sign S is negative, add the value of V to one of the pixels P(r, c) in the sub image Mi, the values of (r, c) are calculated depending on values of (i, j) of the point Ni.

iv. Otherwise (if S is positive) subtract value of V from the pixel P(r, c) in the sub image Mi, the values of (r, c) are calculated depending on values of (i, j) of the point Ni.

- Convert the data back in Text/Image format.
- Store data in the form of file.

V EXPERIMENTAL RESULTS

In experimental results, image Lena is used and text file is added as watermark over the image. Then capacity of embedded text file and the PSNR values are calculated. The Image is shown as source image. The quality of watermarked images is calculated in terms of PSNR [14] (Peak Signal to Noise Ratio). If the value of PSNR is less, the watermark is more perceptible. Histograms are used to show difference between source image and watermarked image. In fig3 source image and embedded image are shown. Source image is indicated by original image and embedded image is indicated by watermarked image.

Fig: 3. Source image

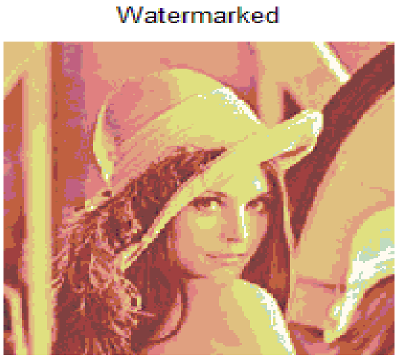

Fig: 4 watermarked image.

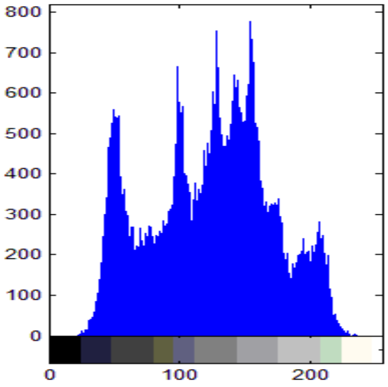

Fig: 5 Source image histogram

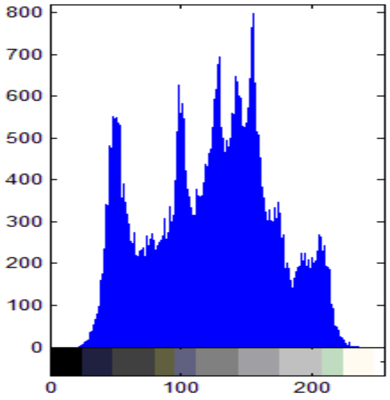

Fig: 6 Watermarked image histogram.

In the above source image and watermarked image color luminance is not change. The histogram of source and watermarked images are same as shown in fig. 4.

Research in the watermarked image to check image perceptual quality, embedded data capacity, histogram and PSNR

TABLE I
Result table of watermarked image

Image name	Image Size	Embedded data Capacity	PSNR(:; :;1)	PSNR(:; :;2)	PSNR(:; :;3)
Lena	256*256	1.9943	55.8941	55.9125	55.9286

A. Histograms Results

An image histogram is a type of histogram that acts as a graphical representation of the tonal distribution in an image. It plots the number of pixels for each tonal value. By looking at the histogram for a specific image a viewer will be able to judge the entire tonal distribution at a glance. The horizontal axis of the graph represents the tonal variations, while the vertical axis represents the number of pixels in that particular tone. Two histograms are generated, one for source image and another for watermarked image. Histograms are showing frequency components of pictures. There are very minor differences in both source image histogram and watermarked image histograms because watermark is embedded at LSB of high frequency components or coefficients. Fig4 shows histogram for source image and watermarked image. Histograms of source image & watermark image are same and only minor difference in graph is at very few places in high frequency components but not easy visible by HVS (human visual system).

B. PSNR (Peak Signal to Noise Ratio)

The Peak signal-to-noise ratio (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. PSNR is usually expressed in terms of the logarithmic decibel. Perceptibility expresses amount of distortion caused by watermark embedding. In other words, it indicates how much visible is the watermark. It is measured by peak signal-to-noise ratio (PSNR). Less is the value of PSNR; the more perceptible is the watermark. It shows for imperceptibility of image, PSNR value should be high. Table shows larger PSNR, that shows watermark embedded in image is totally imperceptible. Imperceptibility of watermark makes watermark more secure. Because source image and watermarked image are same, it's PSNR (peak signal to noise ratio) is also same.

$$\text{MSE } (I, I^1) = \frac{1}{MN} \sum_{y=1}^{M} \sum_{x=1}^{N} [I(x,y) - I'(x,y)]^2$$

$$(\text{PSNR})_{db} = 10 \log_{10}(255^2/\text{MSE})$$

The PSNR is employed to evaluate the difference between an original image and watermarked image. For the robust capability, mean square error (MSE) measures the difference between an original watermark I and corresponding extracted watermark $I^{1.}$ If a method has a lower MSE (I, I^1), it is more robust.

C. Comparison with other related methods

The results of proposed methods are compared with two related ones which are shown in table 2. "Image Quality Assessment Based on Multiple Watermarking Approaches" with the help of this paper we compare the result of proposed approach show that watermark strength and PSNR both are improved. So, successfulness of proposed approach to enhance the security and capacity of watermark data is shown in table 2.

TABLE II
. Comparisons table (Embedding/Detection results for Lena image)

Method	W-Param.	Lena
SWT variant	W-strength *α11, α12, α21*	0.057 0.220 0.980
	Watermarked image PSNR (*dB*)	48.64
DWT	W-strength *α11, α12, α21*	0.065 0.230 1.100
	Watermarked image PSNR (*dB*)	47.96
Proposed Approach	W-strength	1.994
	Watermarked image PSNR (*dB*) (-,-,1)(-,-,2)(-,-,3)	55.8941 55.9125 55.9286

V1 CONCLUSION

In the paper an invisible watermarking technique based on matrix encoding technique is used for embedding multiple watermark files in color image. Watermark data is encrypted in frequency domain. A general coding type framework is used to provide useful and constructive tools in analysis and design of watermarking .The proposed approach helps in achieving robustness, high capacity, high security, truly imperceptibility and implementation efficiency.

Advantages:

(1)Proposed invisible watermarking system is secure because data is stored in randomly selected segments of image.

(2)Proposed system is efficient.

(3)Proposed system is computationally costly and unpredictable. Even if algorithm is known it is very hard for intruder to extract the data.

(4)High capacity of watermark is embed into color image as cover image is divided into series of segments for storing the data.

(5)Before embedding the watermark is encrypted. This provides an additional level of security for watermarks. Even if hacker knows the watermarking key, he will not be able to identify the watermark because it is encrypted.

REFERENCES

[1] Chiou-Ting Hsu and Ja-Ling Wu, “Hidden Digital Watermarks in Images” *IEEE Transactions On Image Processing,* Vol. 8, No. 1, PP. 58-68 1999.

[2] Anastasios Tefas, Nikos Nikolaidis, and Ioannis Pitas,“Image Watermarking Techniques & Applications”.*The Essential guide to image*, Chapter 22, 2008

[3] XIE Qing, XIE Jianquan, XIAO Yunhua “A High Capacity Information Hiding Algorithm In Color Image*” IEEE* ,2010 .

[4] .Khaled Mahmoud, Sekharjit Datta, and James Flint,” Frequency Domain Watermarking:An Overview” *The International Arab Journal of Information Technology*, Vol. 2, No. 1, PP.33-47, 2005.

[5] E. Ganic and A. M. Eskicioglu, “A DFT-Based Semi-Blind Multiple Watermarking Scheme for Images,” *4th New York Metro Area Networking Workshop*, The Graduate Center, The City University of New York, September 10, 2004.

[6] Athanasios Nikolaidis and Ioannis Pitas “Region-Based Image Watermarking” *IEEE Transaction On Image Processing,* Vol.10, No.11, PP. 1726 – 1740, 2001

[7] Abdullah Bamatraf, Rosziati Ibrahim and Mohd. Najib Mohd. Salleh, “A New Digital Watermarking Algorithm Using Combination of Least Significant Bit (LSB) and Inverse Bit” *journal of computing,* Vol. 3, issue 4, April 2011.

[8] XIE Qing, XIE Jianquan, XIAO Yunhua “A High Capacity Information Hiding Algorithm In Color Image” *IEEE* ,2010

[9] Sabyasachi Samanta, Saurabh Dutta, Goutam Sanyal “An Enhancement of Security of Image using Permutation of RGB-Components” *IEEE* 2011

[10] FrankY. Shih, Scott Y.T. Wu, “Combinational image watermarking in the spatial and frequency domains” *Science Direct*, Vol. 36, No. 4, PP. 969-975, 2003.

[11] Ganic, E., Dexter, S.D., Eskicioglu, A.M., "Embedding Multiple Watermarks in the DFT Domain Using Low and High Frequency Bands" *IS&T/SPIE's 17th Annual Symposiun on Electronic lmaging, Security, Steganography, and Watermarking of Multitnedia Contents VII Conference,* San Jose, CA, January 17-20, 2005.

[12] Yongjian Hu, Sam Kwong and Jiwu Huang,“Using Invisible Watermarks to Protect Visibly Watermarked Images” Vol.5, PP. 584-587, *IEEE*, 2004

[13] Dr.M.Mohamed Sathik and S.S.Sujatha, “An Improved Invisible Watermarking Technique for Image Authentication” *International Journal of Advanced Science and Technology* Vol. 24, PP.61-74, 2010.

[14] Rakhi Dubolia, Roop Singh, “Digital Image Watermarking by using Discrete WaveletTransform and Discrete Cosine Transform and Comparision Based on PSNR” *IEEE International Conference on Communication Systems and Network Technologies(CSNT)*, PP. 593-596, 2011.

[15] Kamran Hameed, Adeel Mumtaz, and S.A.M. Gilani, “Digital Image Watermarking in the Wavelet Transform Domain” *World Academy of Science, Engineering and Technology* , Vol.13, PP. 86-89, 2006.

[16] R. Mehul and R. Priti, “Discrete Wavelet Transform Based Multiple Watermarking Scheme,” *Proceedings of IEEE Region 10 Technical Conference on Convergent Technologies for the Asia-Pacific*, Bangalore,India, October 14-17, 2003

[17] Dhruv Arya, “A Survey of Frequency and Wavelet Domain Digital Watermarking Techniques” *International Journal of Scientific & Engineering Research*, Volume 1, Issue 2, 2010.