International Journal of Advance Research in Science and Engineering
Vol. No. 5, Issue No. 08 , August 2016
www.ijarse.com
IJARSE
ISSN 2319 - 8354

COLOR IMAGE WATERMARKING USING BLOCK SELECTION BY LUMINANCE METHOD

Saurabh Sony[1], Sachin Srivastava[2]

ABSTRACT

In this project new watermarking scheme is presented based on log-average luminance. A monochrome image of 1024 bytes is usedas the watermark. To embed the watermark, 16 blocks of size 8X8 are selected and used to embed the watermark image into the original image. If the byte of the watermark image represented white color (255) a value a ris added to the image pixel luminance value, if it is black (0) the a is subtracted from the luminance value. To extract the watermark, the selected blocks are chosen as the above, if the difference between the luminance value of the watermarked image pixel and the original image pixel is greater than 0, the watermark pixel is supposed to be white, otherwise it supposed to be black. Experimental results show that the proposed scheme is efficient against changing the water- marked image to gray scale, image cropping, and JPEG compression.

Keywords— Watermarking, Luminance, Gray-scale, log-average luminance, spatial domain, Color Image Watermarking, Discrete Cosine Transform, Discrete Wavelet Transform, Restoration Parameter.

I. INTRODUCTION

The In spatial domain technique the watermark is embedded directly into the pixel data. A 32X32 monochrome image (1024 bytes) is used as a watermark. Original image is converted from RGB to YC_bC_r color space. The image is divided into 8X8 blocks. The log-average luminance is computed for the image and for each block of the image[3].Blocks that are used in watermark embedding are those blocks that have a log-average luminance equal or greater than the log-average luminance of the entire image. Only 16 blocks are needed to embed the watermark. The monochrome watermark image only has two colors, black and white. Each byte of the watermark image is embedded into the original image by changing the pixels Y value of the selected blocks. The a is added to Y value of the pixel if the watermark pixel is white (255) or a is subtracted if the color is black (0),where a is an integer value. To extract the watermark the same steps of embedding watermark is performed. The luminance value of the watermarked image pixel is subtracted from the luminance of the original image pixel.

If the result is greater than or equal to zero the watermark pixel is supposed to be white. Otherwise, when the result of subtraction is less than zero, the watermark pixel supposed to be black. computer will be disassembled has a significant influenced on the total profit, i.e. the sum of the component values.

Therefore, maximization of the total component value is considered as an optimization criterion**.** In order to solve the general version of the problem, we also construct and experimentally test a number of heuristic algorithms and mathematically define the comparison between various heuristics & ant colony optimization algorithm.

II. LITERATURE SURVEY

Evaluation of project request is major purpose of preliminary investigation. It is the collecting information that helps committee members to evaluate merits of the project request and make judgment about the feasibility of the proposed project. At the heart of any system analysis is detailed understanding of all important facts of the business area under investigation. The key questions are What is being done? How it is being done. How frequently does it occur? How great is the volume of transactions or decision. How well is the task being performed? Does a problem exist? If a problem exists, how serious is it? What is the underlying cause?

To answer the above questions, system analysts discuss with different category of person to collect facts about their business and their operations. When the request is made, the first activity the preliminary investigation begins. Preliminary investigation has three parts- Request clarification, Feasibility study and Request approval.

Request Clarification:- An information system is intended to meet needs of an organization. Thus the first step is in this phase is to specify these needs and requirements. The next step is to determine the requirements met by the system. Many requests from employees and users in the organizations are not clearly defined. Therefore, it become necessary that project request must examine and clarified properly before considering system investigation. Information related to different needs of the System can be obtained by different users of the system. This can be done by reviewing different organization's documents such as current method of storing sales data, complaint data etc. By observing the onsite activities the analyst can get close information related to real system.

III. PROCESS MODEL

3.1 Software Development Life Cycle

There is a large number of software models used for guiding the software development process. Normally every software model contains almost same life cycle except there are some difference process techniques. In this software we have used the linear sequential model because it is easiest one to implement and we have to follow the straightforward techniques for developing the software.

3.1.1 Stages of Waterfall Model

REQUIREMENTS

The first phase involves understanding what you need to design and what is its function, purpose etc. Analysis As per the requirements, the software and hardware needed for the proper completion of the project is analyzed in this phase.

International Journal of Advance Research in Science and Engineering
Vol. No. 5, Issue No. 08 , August 2016
www.ijarse.com
IJARSE
ISSN 2319 - 8354

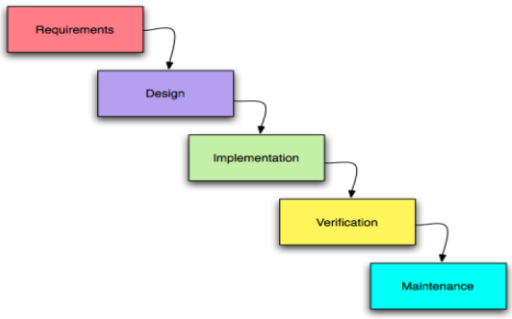


Fig3.1 1 STAGES OF WATERFALL MODEL

3.1.2 Implementation of the Module

Therefore in case of blind technique we only have the watermarked image and we apply algorithms on that in order to obtain the watermark.[3][1]

Algorithm 3.1.3 Watermark insertion into the color image

Require: A color image (.jpg file format) and one monochrome image of 32*32.

1: Convert the color image from RGB to Ycbcr.

2: Then divide the image into the block size of 8*8.

3: After that the block selection operation is performed.

4: Select the first 16 blocks whose luminescence value is equal to or greater than the luminescence of the entire image.

5: Embed the watermark i.e, monochromatic image.

6: Convert image from Ycbcr to RGB.

7: Save the resulting image.

Algorithm 3.1.4 Watermark extraction from the watermarked image

Require: A original color image (.jpg file format) and watermarked image(.jpg file format).

1. Convert the color image from RGB to Ycbcr.

2. Find the log average luminance of both the images i.e, original and watermarked. After that the block selection operation is performed ie the blocks whose Log average luminescence value is equal to and greater than that will be selected.

3. Select the first 16 blocks whose luminescence value is equal to or greater than the luminescence of the entire image.

4. Extract the watermark i.e, monochromatic image.

5. Convert image from Ycbcr to RGB.

6. Save the resulting image

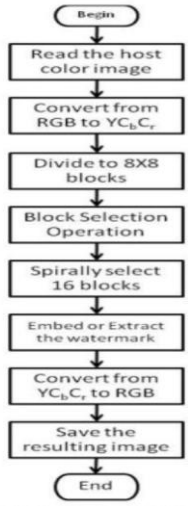


Figure 4.1: Flow Chart

4.1 Watermark Insertion

The proposed non-blind algorithm in spatial domain directly inserts the watermark information into the pixels. The watermark is embedded by repositioning the selected vertices according to the groups they belong. The repositioning of selected vertices are performed by increasing the vertex normal distance.

4.2 Embedding Process

Fig. 4-01 shows the process of watermark embedding process. The embedding process takes following steps:

Conversion from RGB to YCbCr color space

Convert the RGB image into YCbCr color space using the following equations

Y = 0.299*R + 0.587*G + 0.114*B

Cb = 0.596*R - 0.275*G - 0.321*B

Cr = 0.212*R - 0.523*G - 0.311*B

where R, G, and B are red, green and blue components of RGB color space respectively.

Log-average Luminance

The block selection criteria are depended on log-average luminance for the entire image and log-average luminance for each block. The log-average luminance Lavg is calculated as shown in the equation:

$$L_{avg} = exp(\text{å}log(d+Yx;y)=N)$$

where, Lavg is the Log-average luminance, Y(x,y) is the Luminance Y of the pixel at (x,y), delta is a small value to avoid taking the log of a completely black pixel whose luminance is zero and N is the number of pixels in the image.[4][3]

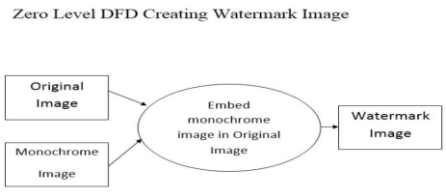


Figure 4.2: Zero Level Data flow diagram of Embedding

Block Selection Criterion

The original 512*512 host image is divided into 8OE8 and each block is converted to YCbCr color space. The blocks which we select to embed are those having log-average luminance closer to the log-average luminance of the whole image. The log-average luminance is calculated as per the method given in the step 2. DCT transform is applied to the Y component of each selected block. Each values of the watermark image are embedded into each selected block of the host image. The watermark values are embedded in the DC component values of the selected blocks. The watermark is extracted from the watermarked image using the same selected blocks and DCT coefficients that have been used in the embedding process.

4.3 Watermark Extraction

The proposed watermarking algorithm is non-blind in nature as it requires cover object as well as watermarked object at the time of extraction. The watermark information can simply be obtained by subtracting the pixels of the original image from the watermarked image. Thus we then obtain the watermark that we have inserted or embed in the original image. [5][2]

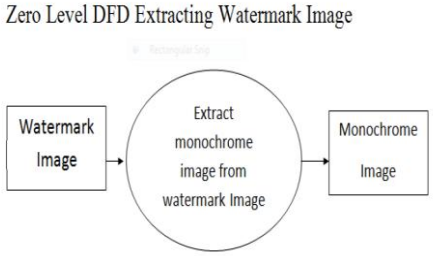


Figure 4.3: Zero Level Data flow diagram of Extraction

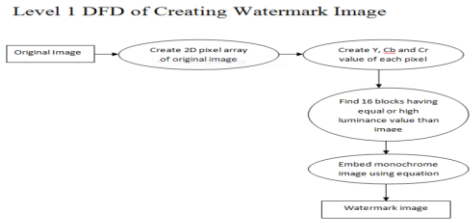
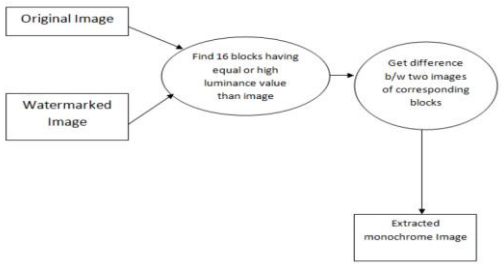


Figure 4.4: Level 1 Data flow diagram

Level 1 DFD of Extracted Monochrome image from Watermarked Image



4.4 Execution Time Comparison

The execution time of the proposed watermarking algorithms depends on the size of the color and, system configuration and also on the secure code which decides how and where pixels are selected for watermark embedding. The execution time for watermark embedding is found to lie between 1.89 to 132 seconds for proposed algorithm, when executed on Pentium dual core 1.86 GHz processor. The algorithm takes less time in execution as compared to other algorithm and produces output of better perceivable visual quality. The proposed algorithm take less time to insert the watermark when compared to other which reports 3.5 to 192.6 seconds when executed on Pentium-IV 3.4 GHz processor. The execution time for watermark insertion also depends on number, luminescence and positions of pixels to be watermarked.

4.5 Attacks on Watermarking

The watermark should not be noticeable to the viewer nor should the watermark degrade the quality of the content. The term ¸ Simperceptible˘T is widely used in this case. However, if a signal is truly imperceptible, then perceptually based lossy compression algorithms either introduce further modifications that jointly exceed the visibility threshold or remove such a signal, Gonzalez and Woods (2008). It is then important to develop techniques that can be used to add imperceptible or unnoticeable watermark signals in perceptually significant regions to counter the effects of signal processing.

4.5.1 Active Attacks

Here, the hacker tries deliberately to remove the watermark or simply make it undetectable. This is a big issue in copyright protection, fingerprinting or copy control for example.

4.5.2 Passive Attacks

In this case, the attacker is not trying to remove the watermark but simply attempting to determine if a given mark is present or not. Cox et al (2002) suggest that, protection against passive attacks is of the utmost importance in covert communications where the simple knowledge of the presence of watermark is often more than one want to grant.

4.5.3 Collusion Attacks

In collusive attacks, the goal of the hacker is the same as for the active attacks but the method is slightly different. In order to remove the watermark, the hacker uses several copies of the same data, containing each different watermark, to construct a new copy without any watermark. This is a problem in fingerprinting applications (e.g. In

the film industry) but is not the widely spread because the attacker must have access to multiple copies of the same data and that the number needed can be pretty important.

4.5.4 Forgery Attacks

This is probably the main concern in data authentication. In forgery attack the hacker aims at embedding a new, valid watermark rather than removing one. By doing so, it allows him to modify the protected data as he wants and then, re-implants a new given key to replace the destructed (fragile) one, thus making the corrupted image seems genuine.

V. RESULT ANALYSIS

The results are produced from tests applied on different color images (girl, penguins). The block size is taken as constant (8x8).Table 1 show the quality measure PSNR and the Similarity for different images using different tests such as Cropping, JPEG compression, and change the colored image to grayscale image.As we see, the similarity is not affected by image cropping and color image to grayscale conversion.In compression, the quality of the watermark is decreased as the compression factor is increased. tests are performed on different color images and show some robustness against various attacks. More robustness can be achieved by adding the watermark in frequency domain using transforms like (DFT, DCT, or DWT). We also can use grayscale or color watermark instead of the monochrome watermark used in this paper.

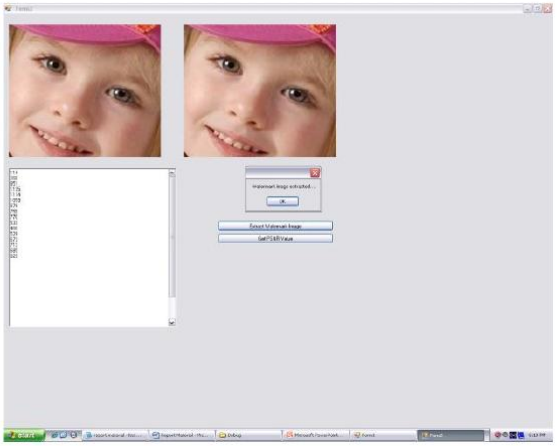


Figure 5.1: Watermark Image Extracted

5.1 Performance Evaluation

It is observed that the distortion reduces by suitable selection of pixels. There is improvement upto 31.58% on numerical distortion as in shown. The main requirement of watermarking algorithm is that it should not produce visible change over the color image. The watermarking algorithms proposed by Jamal A. Hussien [3].produce the Luminescence method of Watermarking while both our Flowchart proposed in chapter-3 and chapter-4 are free

from such type distortion. The approach proposed in this chapter specifically addresses the affect of increasing/decreasing the brightness and changing the position of blocks for watermark embedding on the distortion.

Table 5.1: VARIOUS TEST ON DIFFERENT COLOR IMAGES

IMAGES	PSNR VALUES
Baboons	62.499
Baby	51.834
Penguins	28.034
Peppers	19.623
Face	21.537
Tulips	60.765
Kola	27.4738
Chrysanthemum	12.638
Dessert	40.678
Jelly fish	25.0456

table 5.1: various test on different color images images psnr values

VI. CONCLUSION

In this chapter, we proposed a non-blind, secure and robust watermarking algorithm in spatial domain. The proposed algorithm is based on the watermark is embedded in the selected pixels based on luminescence obtained from color image. In the proposed algorithm insertion and deletion of watermark information is done in two different steps. The watermark is embedded by checking the luminance value of the block which constitutes the sixteen pixels of size 8*8,and then an monochrome image of size 32*32 is embedded. The proposed watermarking scheme is also robust against various distortion and distortion-less attacks. In case of distortion attacks like impressive, watermark is distorted to some extend. The execution time of watermarking scheme depends on the number of blocks and pixel's brightness selected for watermark embedding of color image. The execution time is found to lie between 2.84 to 208 seconds for different test objects when executed on Pentium dual core 1.86 GHz processor. Image Watermarking has become an important data authentication technique nowadays for image products. The proposed scheme can be used to watermark digital images without distorting the vital regions that are of interest to the customer. Hence, the value of the image is preserved. At the same time, the ownership of the digital image can be proven whenever required on the production of the key by the legal owner, thereby, keeping a check on illegal copying of the copyrighted image.

VII. FUTURE SCOPE

1. Experimental test results show best watermark invisibility when the addition factor a is 3.
2. Many tests are performed on different color images and show some robustness against various attacks.

3. More robustness can be achieved by adding the watermark in frequency domain using transforms like (DFT, DCT, or DWT).

4. We also can use gray scale or color watermark instead of the monochrome watermark used in this paper.

REFERENCES

[1] CHAREYRON, G., AND TRÉMEAU, A. Watermarking of color images based on a multi-layer process. CGIV'02, Poitiers, France (2002), 77–80.

[2] HARTUNG, F., AND KUTTER, M. Multimedia watermarking techniques. Proceedings of the IEEE 87, 7 (1999), 1079–1107.

[3] HUSSEIN, J. A. Spatial domain watermarking scheme for colored images based on log-average luminance. arXiv preprint arXiv:1001.3496 (2010).

[4] MOHAMMED, A. A., AND HUSSEIN, J. A. Efficient video watermarking using motion estimation approach. 593–598.

[5] MOHANTY, S. P., GUTURU, P., KOUGIANOS, E., AND PATI, N. A novel invisible color image watermarking scheme using image adaptive watermark creation and robust insertion-extraction. 153–160.

[6] I brahim Nasir, Ying Weng, Jianmin Jiang, "A New Robust Watermarking Scheme for Color Image in Spatial Domain"

[7] Deepa Kundur and Dimitrios Hatzinakos, "Digital watermarking using multiresolution wavelet decomposition"

[8] Xiang-Gen Xia, Charles G. Boncelet and Gonzalo "Wavelet Transform based watermark for digital Images", R. Arce : OPTICS EXPRESS, 7 December 1998 / Vol. 3, No. 12, PP 497-511

[9] 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: Publication: 17 November 2007

[10] D. Taskovski, S. Bogdanova, M. Bogdanov, " Digital watermarking in wavelet domain"

[11] Maha Sharkas, Dahlia ElShafie, and Nadder Hamdy ,"A Dual Digital-Image Watermarking Technique", Transaction on Engineering, computing and technology, Vol 5, April 2005 ISSN 1305-5313

[12] Rafael C. Gonzalez, R.E.Woods, Steven:, "Digital image processing using MATLAB:"

[13] Peter Meerwald, " Digital image watermarking in the wavelet Transform domain " P.Hd thesiss

[14] Houng- Jyh Mike Wang, Po-Chyi Su and C.-C. Jay Kuo, "Wavelet-based digital image watermarking" OPTICS EXPRESS, 7 December 1998 / Vol. 3, No. 12,PP 491-496 [15] M. Kuttera and F. A. P. Petitcolas, " A fair benchmark for image watermarking systems"

[16] Selena Kay and Ebroul Izquierdo, " Robust content based image watermarking"

[17] Chirawat Temi, Somsak Choomchuay, and Attasit Lasaku "A Robust Image Watermarking Using Multiresolution Analysis "Wavelet- Proceedings of ISCIT2005

[18] Abou Ella Hassanien, " A Copyright Protection using Watermarking algorithm" Informatica, 2006, Vol. 17, No. 2, PP 187–198

[19] www.amara.com/current/wavelet.html " An introduction about Wavelets- Amara Graps "

[20] Vallabha V Hampiholi, " Multiresolution Watermark Based on Wavelet Transform for Digital images"