Dual Watermarking For High Protective Copyright System

Sagar R Dhole, Student,Computer Department,Sinhgad Institute of Technology,Lonavala
Rahul S.Shahane, Student,Computer Department,Sinhgad Institute of Technology,Lonavala
KrishnaV.Varat, Student,Computer Department,Sinhgad Institute of Technology,Lonavala
Ganesh N.Falake, Student,Computer Department,Sinhgad Institute of Technology,Lonavala

ABSTRACT

Dual Watermarking is used forcopyright protection and authentication. In theproposed system, a Dual Watermarking Schemebased on BPCS and Alpha Channel maskingalgorithm, will be developed to improve therobustness and protection along with security.Our project implemented the BPCS (Bit Plane Complexity Segmentation) technique to embed data into bitmap files. The ultimate goal is to embed as much data as possible into a cover image without detection by human perception or statistical analysis. Our first attempt to implement this hiding technique was on 8-bit grayscale images as our cover object. After accomplishing that version, we manipulated it into a second version that was also capable of using 24-bit color images.First outline the BPCS embedding and extraction technique for grayscale images and explain the subtle differences in the color version. It will also compare and contrast the results of embedding data at different thresholds and capacities for both grayscale and color images.

KeyWords*:* Dwt,watermarking,bpcs,alpha channel masking

Introduction

“A digital watermark is a digital signal or pattern inserted into a digital document such as text, graphics or multimedia, and carries information unique to the copyright owner, the creator of the document or the authorized consumer[1].”

Digital Watermarking is used for copyright protection and authentication. In the proposed system, a Dual Watermarking Scheme based on BPCS Algorithm and Alpha Channel

/Transparency Channel Masking Algorithm will be developed to improve the robustness and protection along with security[2]. Two watermarks will be embedded in the host image. The secondary is embedded into primary watermark and the resultant watermarked image can then be transmitted over a non secure channel. This provides an efficient and secure way for image security and transmission. The watermarked image is decrypted and a reliable watermark extraction scheme can be developed for the extraction of the primary as well as secondary watermark from the image.

Existing System

Digital watermarking is a technique which allows an individual to add hidden copyright notices or other verification messages to digital audio, video, or image signals and documents. Such hidden message is a group of bits describing information pertaining to the signal or to the author of the signal (name, place, etc.). The technique takes its name from watermarking of paper or money as a security measure. Digital watermarking is not a form of steganography, in which data is hidden in the message without the end user's knowledge, although somewatermarking techniques have the steganographic feature of not being perceivable by the human eye[1][6].
The enormous popularity of the World Wide Web in the early 1990's demonstrated the commercial potential of offering multimedia resources through the digital networks. Since commercial interests seek to use the digital networks to offer digital media for profit, they have a strong interest in protecting their ownership rights. Digital watermarking has been proposed as one way to accomplish this.

Proposed system

A digital watermark is a digital signature or pattern inserted into digital image. Since the signal or pattern is present in each unaltered copy of original image, the digital watermark may also serve as a digital signature for the copies. A given watermark may be unique to each copy (e.g, to identify the intended recipients), or be common to multiple copies. In either case, the watermarking of the document involves the transformation of the original into another form. This distinguishes digital watermarking from digital fingerprinting where the original file remains intact, but another file is created that "describes" the original file's content.

where the original file remains intact, but another file is created that "describes" the original file's content.

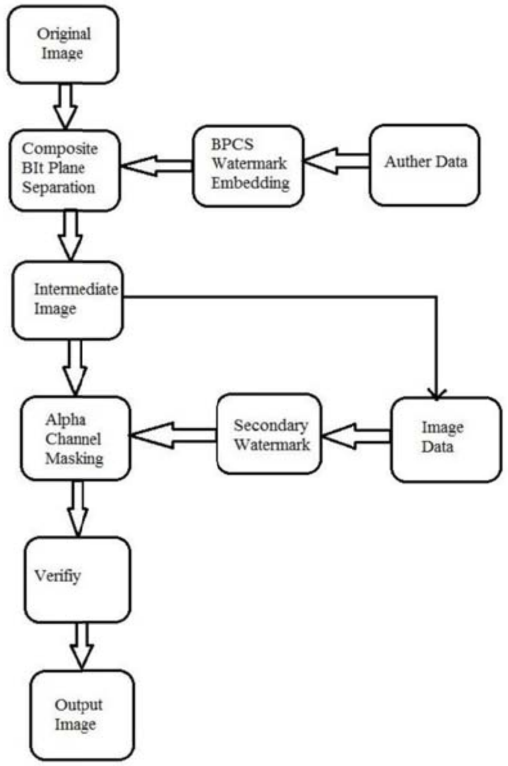

Fig.1 System Flow Diagram

1) Primary Watermark

Primary watermark shall contain the author and copyright information of the image. This information will be embedded on original image so that an image shall always carry its copyright information with it. We shall achieve this using BPCS Steganography[4].

2) Secondary Watermark

We will use intermediate image data (grayscale component of the intermediate image) itself as the data to be watermarked on the intermediate image[1]. This data will help us determine if there is any modification or damage done to the original image and also reconstruct the original image to some extent. We shall do this using Alpha Channel / Transparency Channel masking.

Modules

A. Image Bit Plane Decomposition

B. TGA Image Generation (BMP, PNG to TGA)

C. Primary Encryption Using BPCS

D. Alpha Channel Masking

E. Watermark Verification

A. Image Bit Plane Decomposition

1) The carrier image is divided into 8 different Bit-Planes. All the bit-planes are divided into small pieces of the same size, which is called bit-plane blocks, such as 8 × 8[2].

2) Calculate the complexity of every block. The complexity is defined as the amount of all the adjacent pixels that get different values (onepixel is 0, and the other is 1. The maximum possible value of the complexity is denoted as max C .

3) Setting the complexity threshold of the bit-plane block is max C, here α is a parameter. The bit-plane block whose complexity is larger than max C is used to embed secret information. The smaller the value of the more secret information can be embedded[2].

4) Secret information is formed into bit-plane blocks. The bit-plane block can replace the original one straightly if its complexity is greater than max C. Yet, it need to take conjugate processing with the checkerboard pattern block(as shown in Figure1) if the complexity is less than or equal to max C, than take the new block replace the original one.

5) Make a record of the blocks that have taken conjugate processing and this information also need to be embedded into the carrier. The embedding of this extra information cannot produce effect on the embedded secrets, and it must be correctly picked up.The process of secret information extraction is simple. Firstly, pick up all the pieces of the carrier data whose complexity is greater than max C, and then pick up the extra embedded information mentioned in step (5) to confirm the blocks that have taken conjugate processing. These blocks need take XOR operation with tessellated chock to get the recovery of secret.

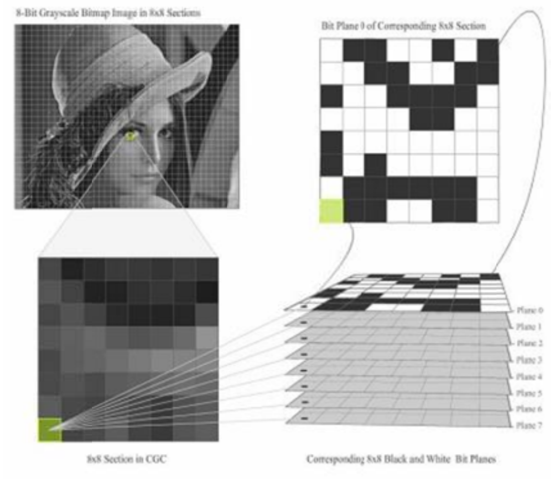
8-Bit Grayscale Bitmap Image in 8x8 Sections
Bit Plane 0 of Corresponding 8x8 Section
Plane 0
Plane 1
Plane 2
Plane 3
Plane 4
Plane 5
Plane 6
Plane 7
8x8 Section in CGC
Corresponding 8x8 Black and White Bit Planes

Fig.2 Image Bit Plane Decomposition

B. TGA Image Generation (BMP, PNG TO TGA)

We are converting the image into TGA format for the better security because TGA image cannot modify easily and the image is of 32 bit so it contains alpha channel also so we are convert the image into TGA format.

C. Primary Encryption Using Bpcs

The BPCS steganography provides a high hiding capacity because the more significant bit planes are used to hide the message. It also provides a lower perceptibility of the hidden message in the stegoimage, because only sufficiently complex blocks are replaced by secret message, and generally, these blocks have a lower visual sensibility for Human Visual System (HVS). However, although the BPCS steganography shows excellent properties, regarding hiding capacity and imperceptibility, it can be vulnerable to the extraction of the hidden message, due to its spatial domain data hiding realization.

D. Alpha Channel Masking

A method for embedding a digital watermark onto a host image’s alpha channel is described. Blending factors which form an alpha channel define the proportion of foreground and background colors which in turn are combined to result in an actual color for each pixel. Here, the blending factors corresponding to areas along edges in the host image is of interest. The host image is first divided into blocks of subimages[7]. A dominant edge found in any subimage is used to divide the pixels on that block into three groups:the group of foreground- color only pixels, the group of background-color only pixels, and the group of foreground-background blended color pixels. The blending factors for the pixels in the last group are modified to embed each bit of a watermarking pattern. Because the modified pixels belong to the area around an image edge, change to the original image due to watermark embedding is less perceptible.

E.VERIFICATION

We can verify the watermark using this module. In this module we can verify the attack of any anonymous user if he/she damage the original data

We can see the modification also and we claim on the unauthorized user for damaging the data.

Experimental Results And Analysis

The length of the black-and-white border in a binary image is a good measure for image complexity. If the border is long, the image is complex, otherwise it is simple. The total length of the black-and-white border equals to the summation of the number of color-changes along the rows and columns in an image. For example, a single black pixel surrounded by white background pixels has the boarder length of 4.
We will define the image complexity αby the following.

$$\alpha = \frac{k}{\text{The max. possible B W changes in the image}} \ldots (1)$$

Where, k is the total length of black-and-white border in the image. So, the value ranges over

$0 \leq \alpha \leq 1.$ … (2)

(1) is defined globally, i.e., ɑis calculated over the whole image area. It gives us the global complexity of a binary image.
However, we can also use ɑfor a local image complexity (e.g., an 8 ×8 pixel-size area). We will use such ɑas our local complexity measure in this paper[2].

Overall, the results went fairly as expected. Increasing the threshold at which bit planesare determined to be complex decreased the embedding capacity, but also decreased thedistortion. Embedding at full capacity (based upon the threshold) of the image includingevery bit plane proved to add distortion (although typically worse at lower thresholds)because the higher bit planes are visually much less tolerant to change.

An interesting observation is that grayscale images had a slight advantage over the colorimages in the sense that only grayscale values could be changed as opposed to acombination of values for each color plane. When pushed to higher limits, the grayscaleimages could look altered compared to the original, but still appear unaltered without

comparison to the original. In color images, when pushing the limits of threshold andcapacity, noticeable color distortions occurred that clearly indicated some kind of changeto the original image.

Conclusion

This paper deals with dual watermarking scheme, which includes encryption, to improve rightful ownership, protection and robustness.

First generation of copyright marking schemes is not strong enough. Existing schemes provide only limited measures of marking.Can only meet few requirements at a time.

For the extraction of watermark, a reliable watermark decryption scheme and an extraction scheme is constructed for both primary and secondary watermark. Robustness of this method is carried out by variety of attacks.

References

[1] Dual Watermarking Scheme with Encryption Proceedings of the Int. Conf. on Information Science and Applications ICISA 2010 Chennai, India. 6 February 2010.

[2] Wu J, Zhang R eta. Reliable Detection of BPCS Steganography[J].Journal of Beijing University of Posts and Telecommunications, 2009, 32(4): 113-121

[3] Mussarat Abdullah,and Fazal Wahab "Key Based Text Watermarking of E-Text Documents in an object based Environment using Z-axis for Watermark Embedding",world academy of engg and technology 46,2008

[4] Cl.Song, S.Sudirman and M.Merabti, "A Spatial and Frequency Domain Analysis of the Effect of Removal Attacks on Digital Image Watermarks", Proc 11th of PostGraduate Network Symposium, 119-124, June, 2010.

[5] Mohamed Saehab,ElisaBertino,ArifGhafoor "Watermarking Relational Databases Using Optimization-Based Techniques" 2011

[6] Copyright Protection of Online Application using Watermarking,march 2011

[7] "Alpha Channel Digital Image Watermarking Method."NataponPantuwong and NoppornChotikakamthornICSP2008 Proceedings.