TECHNIQUE FOR PROTECTING A DIGITAL IMAGE BY NON REMOVABLE WATERMARKING

Shubham Sahai*, Raghvendra Singh**, Rahul Kumar Chaudhary***
* (Student, B.Tech (Computer Science and Engg.), IMS Engineering College (GBTU), Ghaziabad, India
Email: shubhamsahai.cse2012@gmail.com)
** (Student, B.Tech (Computer Science and Engg.), IMS Engineering College (GBTU), Ghaziabad, India
Email: raghvendrasingh24@gmail.com)
*** (Student, B.Tech (Computer Science and Engg.), IMS Engineering College (GBTU), Ghaziabad, India
Email: rahulchaudhary90@gmail.com)

ABSTRACT

Authentication of multimedia contents has gained much attention in recent time. In this paper, we propose a secure watermarking technique. The watermarking that would be helpful in protecting an image from the unauthorized users so that they cannot edit the image in image editing applications like adobe photoshop, Picasa and paint. This would be done by destroying the image as soon as it is edited. In this way, it will prevent the further reproduction of the edited image. It can be applied to all types of image including the famous formats like jpeg, bmp, gif, tif, and tiff.

1. INTRODUCTION

Digital watermarking is the process of embedding information into a digital signal which may be used to verify its authenticity or the identity of its owners, in the same manner as paper bearing a watermark for visible identification. In visible digital watermarking, the information is visible in the picture or video. Typically, the information is text or a logo, which identifies the owner of the media. The watermark may be intended for widespread use and thus, is made easy to retrieve or, it may be a form of steganography, where a party communicates a secret message embedded in the digital signal. In either case, as in visible watermarking, the objective is to attach ownership or other descriptive information to the signal in a way that is difficult to remove. It also is possible to use hidden embedded information as a means of covert communication between individuals. One application of watermarking is in copyright protection systems, which are intended to prevent or deter unauthorized copying of digital media. An effective visible watermarking must satisfy the some features[1]. Another application is in source tracing. A watermark is embedded into a digital signal at each point of distribution. If a copy of the work is found later, then the watermark may be retrieved from the copy and the source of the distribution is known.

The ease by which digital images can be manipulated, has always raised many concerns about the possibility to reliably trust their content. Digital data authentication is thus one of the most important and investigated security applications.

In our proposed approach, the image authentication is done with the help of watermarking.

2. WATERMARK GENERATION

Up till now, there are many image visible watermarking schemes are reported in the literature The IBM digital library organization has used a spatial domain visible watermarking technique to mark the digitized pages of manuscript from the Vatican archive[1] presented a compressed-domain visible watermarking approach for MPEG-1 and MPEG-2 video streams.. The visible watermark is inserted into the DCT coefficients and is adaptive to the local video features. Kankanhalli and Rajmohan (1999) [2] have proposed a visible watermarking technique in DCT domain in which the location and strength of the watermark image to be embedded is varied in accordance with the content of the host image to be watermarked. . Mohanty and Ramakrishna (2000)[3] have improved Kankanhalli and Rajmohan's scheme [2] and strengthened the adaptivity of the visible watermark. Yong [4] have described a visible watermarking based on integer wavelet transform with parameters. Yang [5] presented a reversible visible watermarking scheme, which can be applicable to the applications, in which the visible watermark is expected to protect copyright but the authorized user can remove it losslessly to recover the original image. In order to achieve reversibility, a new reconstruction/recovery scheme is devised. Tsaia and Chang (2010)[6] proposed a secure reversible visible watermarking approach To obtain optimal balance between the watermarked image visual quality and the watermark visibility, we have used an image adaptive visible watermarking algorithm developed by Wenfei Zeng and Yanpeng Wu [7]. in this study, Both the HVS masking characteristics of the host image and the watermark image such as texture and contrast are fully exploited in the watermark insertion stage.

Human visual system masking characteristics: In order to use an effective visible watermarking, it is necessary to take into account the HVS masking characteristics of the visible watermark image and the host image. The following factors will be considered in our scheme given by Kankanhalli and Rajmohan [2][8][9].

- Human eyes have different sensitivity to different luminance, most sensitive to medium luminance usually, Weber ratio keeps const 0.02 within a large range of medium gray and sensitivity declines nonlinearly within the low and high luminance range. We can define contrast sensitivity as follows:

$$\omega(i,j) = \frac{|I(i,j) - 128|}{128} \qquad (1)$$

where, I(i, j), $0 \le i < M, 0 \le j < N$ is the pixel value at the spatial position (i, j) of the host image I with size MxN

- Human eyes are more sensitive to the noise in image smooth areas than that of image texture areas. Let H(i,j) be the entropy of the 4x4 neighborhood of pixel (i,j), greater entropy value is corresponding to the image texture or edge area, while less entropy value corresponds to image smooth area., so we can use the entropy H(i,j) to depict the texture characteristics of the 4x4 neighborhood of pixel (i,j)

Based on all the above considerations, we use a visual perception factor computational model to incorporate the effect of HVS masking characteristics into the visual factor of each pixel as follows.

$$J(i,j) = \omega(i,j) \times H(i,j) \qquad (2)$$

Determination of the scaling and embedding factors: In this watermarking scheme, to achieve high PSNR value for the watermarked image and good watermark invisibility, we exploit the perceptual features of both the host image and the watermark image. So the following formula is used to embed the visual watermark in the watermark insertion stage[2].

$$\begin{aligned} I'(i,j) &= \alpha(i,j) \times I(i,j) + \beta(x,y) \times w(x,y), \\ 0 \le i &< M, 0 \le j < N, 0 \le x < m, 0 \le y < n \end{aligned} \qquad (3)$$

Where the α(i,j) and β(x,y) are the scaling factor for host image and the embedding factor for the watermark respectively. I(i,j) and w(x,y) denote the pixel values of host image F with size MxN in location (i,j) and the watermark image W with mxn in location (x,y) respectively.

The proposed algorithm inserts the watermark directly in spatial domain, which utilizes both the original image and the visible watermark image features. The scaling factor α(i,j) and the embedding factor β(x,y) are calculated as follows.

Step 1: Divide the host image and the watermark image into 4x4 sub-blocks, respectively

Step 2: Compute the visual factor J for each pixel using Eq. 2

Step 3: Obtain the scaling factor α(i,j) and the embedding factor β(x,y) by scaling the visual factor J as follows

$$\begin{cases} \alpha(i,j) = (b-a) \times \dfrac{J(i,j) - \min(J)}{\max(J) - \min(J)} + a \\ \beta(x,y) = (d-c) \times \dfrac{J(i,j) - \min(J)}{\max(J) - \min(J)} + c \end{cases} \qquad (4)$$

where, a, b, c, d are the predetermined parameters, Functions max() and min() return the maximum and minimum respectively

Visible watermark embedding: In watermark embedding, we take full advantage of both the original image features and the watermark image features. The detailed watermark embedding strategy is composed of the following steps.

Step 1: The original image I (to be watermarked) and the watermark image W are divided into blocks of size 4x4

Step 2: Calculate the scaling factor α(i,j) and the embedding factor β(x,y) for each sub-block by using Eq. 4

Step 3: Select the sub-blocks of the original image for watermark embedding

Step 4: Modify the pixel value of the selected host image sub-blocks using Eq. 3 and then the watermarked image is obtained

(a) Lena (b) Boat

(c) Cameraman (d) F-16

Figure 1: Sample Images

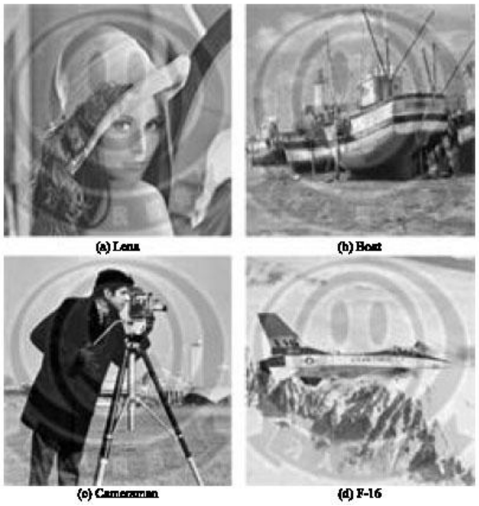

Figure 2: Watermarked Images

The above Figures 1 shows the unwatermarked sample images while Figure 2 shows the images which are watermarked by the above algorithm.

3. MAKING THE WATERMARKING AS NON-REMOVABLE

Once the watermarking is done on the image the resultant image is stored at the desired location. An exe file is made in C which will contain all the original pixels of the watermarked image. This .exe file is bonded to the image to form a complete file which contains both, the image as well as the executable file. The executable file does the task of comparing the original pixels to the present pixels of the image. The check is performed every time when the image is opened. When the image opened in any image editing software and it is edited, the current pixel value of the image changes. If the image is edited and saved then the new pixel values are different from those stored in the executable file which is bounded to the image. On opening the edited image, the current pixels is compared to the original pixels. If the pixels are found same, then there is no change in the image. On the other hand if there is any change in the pixel values of the image, all pixel values are set to 0 thus giving the blank image. In this way the image is destroyed when edited. Figure 3 shows the combination of two files into one to make a resultant file.

Jpg file
Exe file
Jpg file

Figure 3:Binding .jpg with .exe file

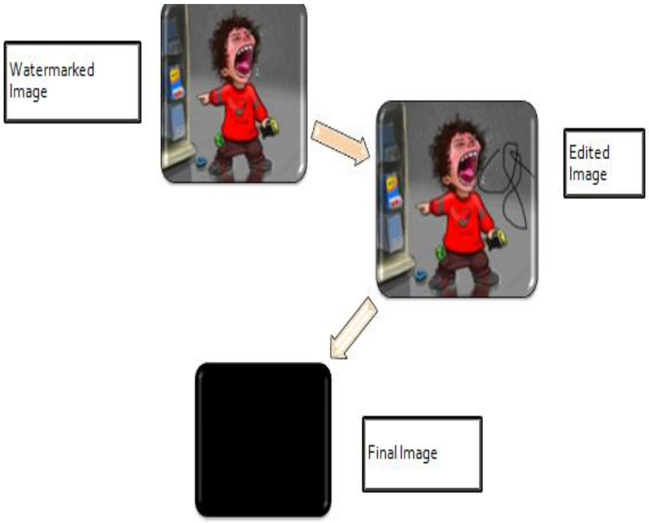

Figure 4: Flow of Control

The complete flow of control is shown in Figure 4.

4. DATA FLOW DIAGRAM AND FLOW CHART

The data flow diagram of the process can be represented as follows in Figure 5 and the flow chart is used to depict the process in Figure 6.

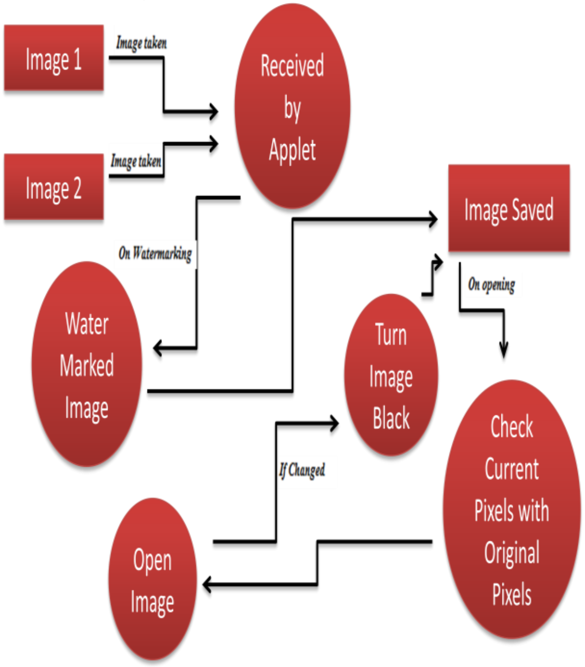

Figure 5: Data Flow Diagram

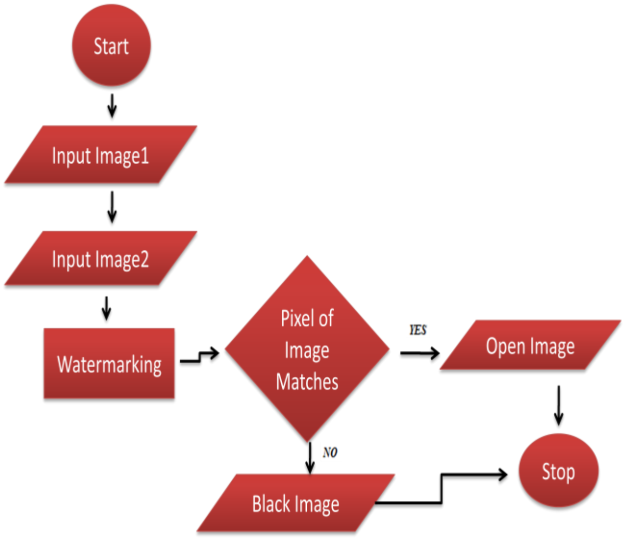

Figure 6:Flow Chart

5. EXPECTED IMPROVEMENTS

The method discussed in this paper is very efficient for primary usage as it can secure images in mostly all formats, but it is not feasible when the image is captured with the help of the print screen button. The image if captured with print screen , contains lots of useless data and hence results in degrading the quality of the image and the executable file which is present behind the image is no more present, due to which the comparison between the pixels cannot occur. The procedure used for watermarking is very simple and as such does not involve any type of algorithm in it. The watermarking can also be done with the help of more complex algorithm which can give a proper structure to the whole process. The simple concept is used because here we are only talking about the visible image watermarking.

6. RESULT

As expected, the process of non removable watermarking is efficiently carried out and hence we can provide the desired security to the digital image. The transparency of the image can also be set so that the resultant image does not get changed to a greater extent. The application is easy to use and has a good user interface.

7. CONCLUSION

Digital Watermarking provides for the protection of intellectual property in the digital world. Just as plagiarism runs loose in the real world, unauthorized copying of data, whether it be audio, visual, or video, exists in the cyber world and is accomplished with the click of a mouse. Digital Watermarking attempts to copyright the digital data that is freely available on the World Wide Web to protect the originator's rights. It also serves as a means of advertising within digital imagery. For instance, a user may download and view a digital image, use a watermark reader to extract the digital signature, and then access a web-based directory to find the company's name and up-to-date address, phone number, and web and e-mail addresses.

8. FUTURE SCOPE

Images are used in every field ranging from security to art and culture. This process of protecting the image can be used in various fields where the integrity of an image is to be maintained. It provides the security to the highest level. In future, it can be used to ensure security of the image where it is accessible to many personalities e.g. on internet. It can also be used at the places where a digital image is to be transferred in a network which is not secure. The attacks like packet sniffing because of which information can be stolen can severely damage the private information. This method can help in protecting the digital images.

9. REFERENCES

[1] Braudaway, G.W., K.A. Magerlein and F.C. Mintzer, 1996. Protecting publicly available images with a visible image watermark. Proceedings of the SPIE Conference on Optical Security and Counterfeit Deterrence Technique, Feb. 1-2, San Jose, CA, USA., pp: 126-133.

[2] Kankanhalli, M.S. and R.K.R. Rajmohan, 1999. Adaptive visible watermarking of images. Proceedings of the IEEE International Conference on Multimedia Computing and Systems, July 7-11, Florence, Italy, pp: 568-573.

[3] Mohanty, S.P. and K.R. Ramakrishna, 2000. A DCT domain visible watermarking technique for images. Proceedings of the IEEE International Conference on Multimedia and Expo, July 30-Aug. 2, New York City, USA., pp: 1029-1032.

[4] Yong, L., C. Li-Zhi, X. Zhi-Hong and W. Yi, 2004. A visible digital watermark based on integer wavelet transform with parameters. J. Software, 15: 238-249.

[5] Yang, Y., X. Sun, H. Yang, C. Li and R. Xiao, 2009. A contrast-sensitive reversible visible image watermarking technique. IEEE Trans. Circuits Syst. Video Technol., 19: 659-667.

[6] In order to achieve reversibility, a new reconstruction/recovery scheme is devised. Tsaia and Chang (2010) proposed a secure reversible visible watermarking approach

[7] Wenfei Zeng and Yanpeng Wu, 2010. A Visible Watermarking Scheme in Spatial Domain Using HVS Model. Information Technology Journal, 9: 1622-1628

[8] Yang, H., X. Sun, G. Sun and Z. Tian, 2010. Lossless authentication watermarking based on adaptive modular arithmetic. Radioengineering, 19: 52-61.

[9] Yang, H., X. Sun and G. Sun, 2010. A semi-fragile watermarking algorithm using adaptive least significant Bit substitution. Inform. Technol. J., 9: 20-26.