Graphical Interface for Watermarking

R.R.N.Eeshan and M.A.Ambroze

Centre for Security, Communications and Network Research,
Plymouth University, Plymouth, UK
e-mail: info@cscan.org

Abstract

Watermarking is a method which is use to hide the data or identifying the data within in the digital multimedia such as Images, Videos, and audios. In this paper the discussion is focused on the watermarking of digital images. Digital watermarking is becoming more popular mainly for embedding undetectable and detectable identifying the marks such as author and copyright information. This research aim is to represent the graphical interface for watermarking techniques. . In this project, the digital watermark is using visible and invisible watermarking technique is designed and discussed. Invisible watermarking using least significant bit (LSB) technique is implemented; the image is to be watermarked has number of pixels, each pixel is represents with the binary system, which is structured to create a digital plane. LSB bits of pixels shows randomness and will not affect the original image even after the bit is changed. We can replace a bit with watermarking metadata. Visible watermarking is visible even after the image is embedded on the original image. This process is implemented in java for graphical interface, where GUI was implemented to provide an easy to use interface that allows easy comparisons of images, and reliable on watermarking techniques.

Keywords

Least Significant bit, Graphical user Interface (GUI), digital watermarking

1 Introduction

In recent years, Multimedia technologies have become increasingly sophisticated with in the rapidly growing internet which allows Images, audio and videos. According to this there are several problems that are related with security, copyright, and so on. Especially the important factor was to protect the rights of the owners with different watermarking techniques in multimedia distribution. The copyright define for copyright protecting and secure the intellectual property rights. In this, if copyright have some problems where the other persons claimed that they own the multimedia objects like images, audio and videos. So to solve this kind of problems copyright had been adapted to digital watermarking techniques which embed the hidden metadata, information, or secret information in a host image (Kutter and Hartung, 2000). Where this allows someone to identify the original owner rights or in case of illicit duplication of purchased materials in which the buyer is involved. Digital watermarking is an effective technique for protecting these rights. There are several domains in the digital watermarking techniques one of which is frequency domain and spatial domain. Spatial domain is the earliest watermarking techniques the simplest example is to embed the watermark into the least Significant bit (LSB) of the image pixels, this technique has a relatively low capacity of information hiding. And in frequency domain approach can be embed more information bits and it is relatively robust to attacks. This technique inserts the direct watermarks in a host image by changing the pixels values and increasing the bits information (Hanjalic et al., 2000). Our goal was to design and implement the watermarking methods and determining the process of adding/ embedding, extracting the watermarks. In this we have proposed one of the methods with a GUI for watermarking by using visible and invisible watermarking technique is designed and discussed. Invisible watermarking using least significant bit (LSB) technique is implemented; the image is to be watermarked has number of pixels, each pixel is represents with the binary system, which is structured to create a digital plane. LSB bits of pixels shows randomness and will not affect the original image even after the bit is changed. We can replace a bit with watermarking metadata. Visible watermarking is visible even after the image is embedded on the original image. So additionally we have created a graphical interface (GUI) that would allow the users unfamiliar with java which is JDK 1.6 used for adding different features as well as extract watermarks and evaluate their respective robustness based on a few morphological image attacks. Where GUI was implemented to provide an easy to use graphical interface that allows simple comparisons of images, and reliable on watermarking techniques.

2 Related works

Generally, copyright will present the ownership of the multimedia object. It uses the watermarking technique, which is use to protect its copyright of the digital media (Hy et.al., 2006) In order to achieve the purpose of watermarking techniques for protecting the rights of the owner and also the technique should meet the following requirements:

- Robustness: Depending upon the applications the digital watermarking can support different levels of robustness towards the changes that has made to the watermarked content. If digital watermarking is used for the ownership rights identification then the watermark should be robust against any modification. In the real world environment, no such perfect watermarking method is implemented and it is not clear yet whether a perfectly secure watermarking method exist (cox *et.al, 1997,* Fridrich *et.al, 1998)*. The watermarks should not be degraded or destroyed with the respective robustness based on a few morphological image attacks.

- Imperceptibility: The embedded watermark is invisible by both statistically and perceptually and does not alter the aesthetics of the content that is watermarked. It is very difficult to distinguish the difference between the original image/medium and the embedded one for human eye. The basic concept of the visible watermarking is simpler when it is compared with the invisible watermarking. The main advantage of using the invisible watermark is that in does not lower the quality on the content.

- Inseparability: Even after the digital material (it can be text or an image) is embedded with watermark separating the content that is used for the watermark to retrieve the original content is not possible.

3 Implementation

The implementation is divided into two approaches, visible watermarking using basic watermarking techniques, and invisible watermarking using least significant bit (LSB) in spatial domain.

The implementation of visible watermarking, a visible watermark means that it is visible to the user and the information could be anything like text, logo or image. It is a process that can add/embed secret message on to the image; the secret message could be anything like text or an image over an original image. In this process the embed text can be placed anywhere on the original image from any position, in this we can change the visibility of the embedded text or image, and also has the process of changing the font and size of the text, it has different features of scaling the text or an image. In the above figure A, we can see the actual process of embedding the text or an image in to the original image to get the watermark image. These types of image will have the 8 bit image as a cover image and the input of the file to be embedded is the actual image could be colour image. While in visible watermarking is not that sure for watermarking for different application like copy writer because the algorithm cannot be kept covert. The goal was to design and implement the watermarking methods and evaluate the process of displaying and scaling and determining the right flow of events for watermark embedding, adding the covert message So additionally graphical interface (GI) that would allow the users unfamiliar with java to add evaluate their respective robustness based on a few structured images. The output using GI will be explained in result part. Figure 1 is a pictorial representation which shows the flow of visible watermarking.

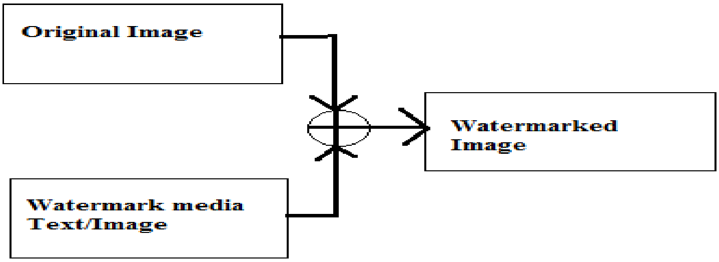


Figure 1: For embedding/adding the watermark on to the image.

Secondly, invisible watermarking using least significant bit, least significant bit is used for visible watermarks; it is the simplest method in hiding the covert message in the original image. Least significant bit is based on the substitution method. The LSBs of pixel of a cover image to the covert image from watermark noise. It embeds the watermark into the least significant bit (LSB) of the image pixel. Adding/embedding and extraction is done by using correlation of both the images. The main advantage of using this technique is, it has a relevant low information hiding capacity, and the disadvantage is that it can be erased by lossy image compression.

3.1 Spatial domain technique

Spatial method analyses the information from the spatial can be viewed from the point of information, where it scatters the information in such a way that the data cannot be easily detected in spatial domain watermarking. The spatial technique has different methods of using pixel, by changing the value of the pixel or alters the lower level bit of the pixel so that the image should not lose the quality (Wolfgang et.al., 1996). One of the methods of data hiding exploits least significant bit (LSB) plane, it has a direct replacement between the cover images. The message and LSB watermark bits will adopt the logical and arithmetic combinations. The image is watermarked in such a way that by selecting the randomly 8x8 blocks of the pixels of the image, it is the earliest watermarking techniques are of this kind, and the simplest example is to embed or add the watermark into LSB of the image pixels. The other features using pixel is adding a positive number to the one of the sub group where the image is grouped into two sub groups (pitas, 1996).

3.2 Watermark Insertion

Embedding the process of the LSB watermarking process, the original image is in vecterized form, this means that it is converted into the matrix form. Then each byte of the image is taken and replaces with the last bit of LSB to the secret information that is watermark image of the each bit. Then the secret image also access the each pixel to convert into the matrix form, then they convert into arrays of bits in binary's of 0s and 1s, and replaces with the least significant of the bit, the output is the watermarked image. It shows that the original image is embedded in to the covert/ secret image that is shown in the figure 2. Figure 2 shows the overall flow of the watermark insertion.

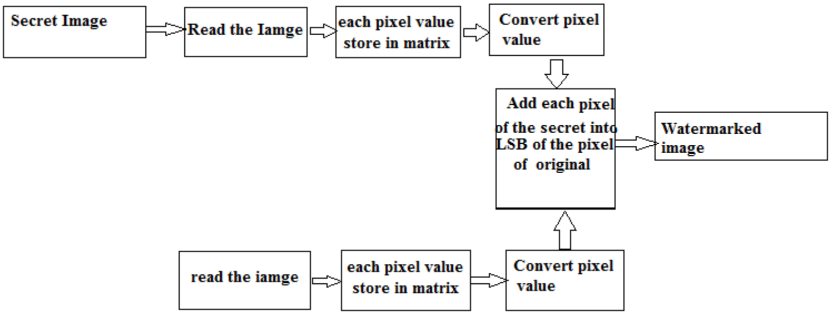

Secret Image
Read the Iamge
each pixel value store in matrix
Convert pixel value
Add each pixel of the secret into LSB of the pixel of original
Watermarked image
read the iamge
each pixel value store in matrix
Convert pixel value

Figure 2: Watermark Insertion

3.3 Watermark extraction using LSB.

It is the similar way of extracting the watermark but in reverse way of doing it. It is the process of finding and extracting the similar bits for both the image like, original and the watermarked image. In this process, after the least significant bit is extracted from both the images, the output is in the form of bytes, and then they are grouped to obtain the watermarked information. This is the process of extraction this can be found from the figure3.

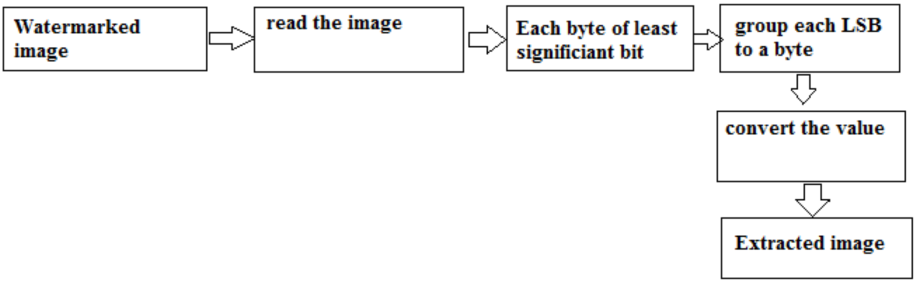
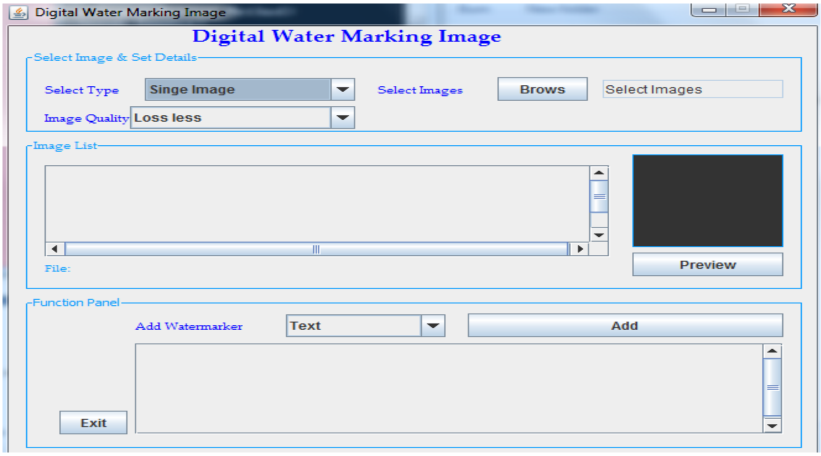


Figure 3: Watermark Extraction

4 Implementation Results

Based on the investigation and implementation we have obtained some results which are discussed in detail as follows.

As mentioned earlier, visible watermark interfaces with the image and can be annoying. It can be easily removable, but the quality will be affected. This was designed to show how the interface is happening between the embedded processing like text and image onto the original image. This is a basic watermarking process that is been implemented using the graphical interface for watermarking. It will show how the interface take the input and process it or in other way adds the covert data in to original image. It has different functionalities that will be explained using Figures. In figure 4, we can select the image by clicking on the browser. We can preview the selected original image. In the functional panel we can select the type of secret message to add/embed on the original image the message could be text or an image.



Digital Water Marking Image

Select Type: Singe Image

Image Quality: Loss less

Add Watermarker: Text

Figure 4: GUI for visible water marking

There are some options for setting the size, font, pixel position, image position, and also can change the visibility options like maximum visibility to minimum. This is the basic implementation using basic visible watermarking technique. The main reason using this technique was to explain the visible watermarking process, how the text or image is embedded on the original image. These images cannot be extracted; there is no software for the extraction process in this method.

In this process a text is embedded in the original image which is visible. In figure 4.8, we can see the text to embed. The difference can be seen from Figures 5 and 6. This is to show the actual process of watermarking technique for visible watermarks. The changes can be made on the written text like increase the size, change the font, change the colour, position of the text to be placed, and the visibility of the text.

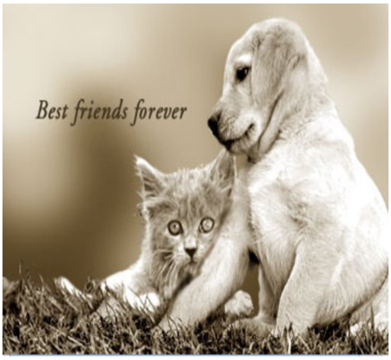


Figure 5: Original image

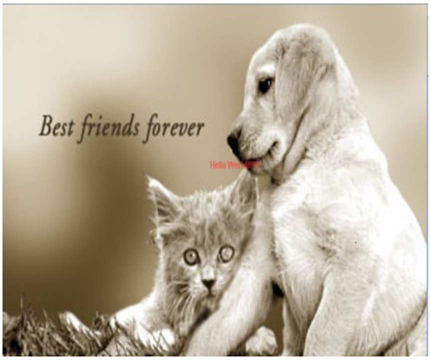


Figure 6: Embed text

From Figures 7 and 8 we can see that how an image is embedded on to the original image. In this we can change the visibility of the embedded image, set the positions of the image. This is to show where the image is been embedded visibly.

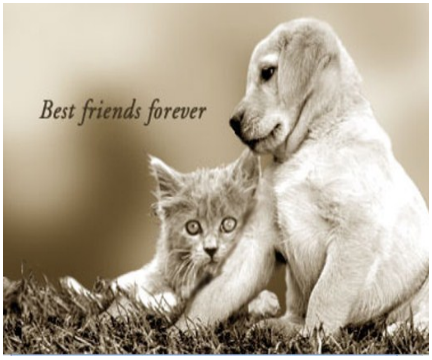


Figure 7: Original image

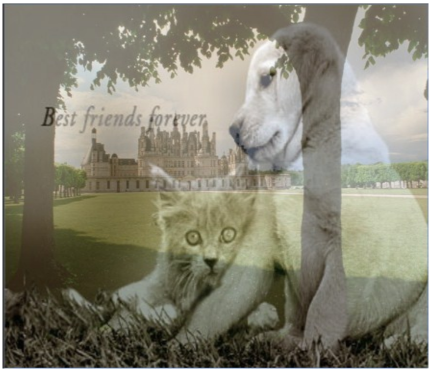


Figure 8: Embed image

5 Results for invisible watermarking

This section will show the results that grained for the LSB watermarking that was implemented. Here JPEG file are used for the cover image as well as watermarked image. The size of the file taken here was 24bit 256*256 colour versions for the original image, 8bit figure the watermark image is been added/ embedded in the original image, it's like adding original image + watermark. This watermarked bit is not visible to the human eye, this process of watermark is called invisible watermark. The image looks same as the original image even 16*16 for the secret image for the least significant bit. The output of the file is resized to the 8bit 16*16 which is very small.

In figure 9, we can see the original image that was selected. And in this the watermark is a predefined image is (J) that is been added to the original image. On clicking the button, insert watermark into the image, the watermark gets embedded into the original image. In this process 24bit 256*256 original image is used. And the water image is smaller size 8bit 16*16. This is mainly used for inserting the logos of the organisations so that it should be secret. In Figure 10, we can see that embedded watermark, in this the main part of interface is that it takes the input process it and sends back the output to the user. In this when the covert image is added to the image.

In figure 11, this is the extraction of the watermark, when we click the extract watermark form the image in figure 10, we can see the covert image is been extracted from the original image is been shown in figure 11.In this we can see the extracted image which was (J), this was extracted from the figure 10 to get the same results, which was embed in figure 9. We can see that extracted image and watermark image was same.

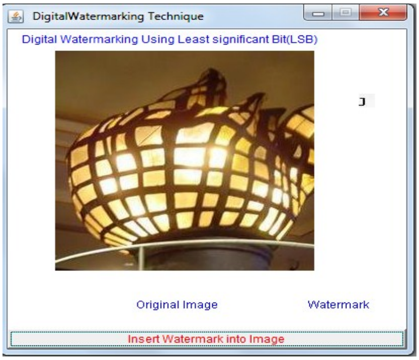

DigitalWatermarking Technique
Digital Watermarking Using Least significant Bit(LSB)
J
Original Image
Watermark
Insert Watermark into Image

Figure 9: Original image

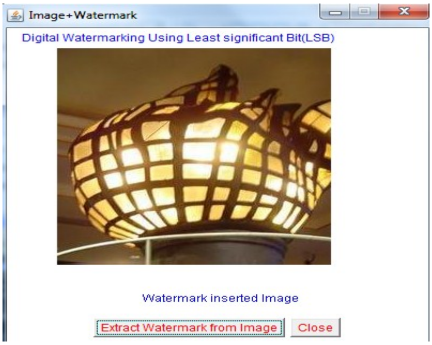
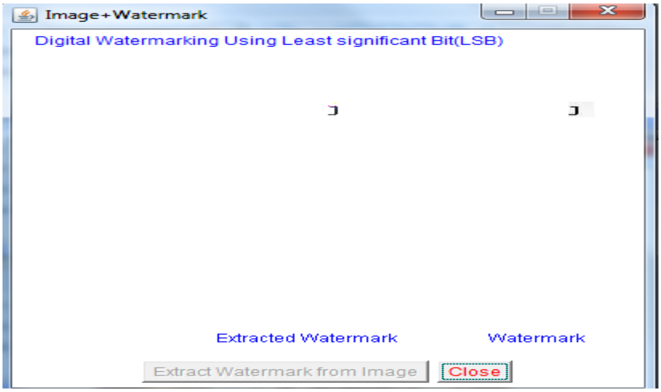

Image+Watermark
Digital Watermarking Using Least significant Bit(LSB)
Watermark inserted Image
Extract Watermark from Image
Close

Figure 10: Hidden image same as original



Image+Watermark
Digital Watermarking Using Least significant Bit(LSB)
Extracted Watermark
Watermark
Extract Watermark from Image
Close

Figure 11: Extracted image

6 Conclusion and future work.

Form the above analysis and discussion for watermarking techniques that are visible and invisible. These techniques perform adaptive measures in embedding the covert message in to the original image where they can be easily achieved. When dealing with the images, it is more useful to approach the matter form the visual position, where the GUI makes visual application much easier. As GI allows us to compare and contrast the original image and the embedded one this is easier to compare the image, and also monitors the illegitimate user by make copies. These methods are successful watermarking in the perspective of reliability and cost. Watermarking is a powerful technique of hiding the data in other files without altering the cover image noticeably. In future this work can be improved by extracting the visible watermarks, and can also introduce the lossy, and lossless visibility watermarking for the quality levels. And there is another important transformation called as Fast hadamard transformation which was not discussed in depth. This is found to be more robust and efficient approach for digital watermarking of digital images; this is used to scale the watermark coefficients in the similar range to the coefficient form hadamard coefficient of the sub blocks of the container image. This research work can be further be improved by improving the security and the robustness.

7 Reference

Cox I. J, Kilian J Leighton F.T and Shamoon T. “Secure spread spectrum watermarking for multimedia,” *IEEE Transactions on Image Processing*, vol. 6, no. 12, pp. 1673-1687, December, 1997

Fridrich.J, “Robust digital watermarking based on key,” In Proc. of the International Information hiding Workshop, 1998.

Hartung, F. (2000). Introduction to watermarking techniques. In S. Katzenbeisser & F.A.P. Petitcolas (Eds.), Information hiding techniques for steganography and digital watermarking. Boston: Artech House

Hanjalic, A., Langelaar, G.C., van Roosmalen, P.M.G., Biemond, J., &Langendijk, R.L. (2000). Image and video databases: Restauration,watermarking and retrieval. Amsterdam: Elsevier

Hy.M,Lou.D, and Chang.M. Dual-wrapped digital watermarking scheme for image copyright protection. Computers& Security, 26:319–330, October 2006.

Pitas, "A method for Signature Casting on Digital Image," Proc. Of ICIP, Vol. 3, pp.2 15-2 18, 1996.

Wolfgang.R and E. J. Delp, "A watermark for digital images," *Proceedings of the 1996 International Conference on Image Processing*, Lausanne, Switzerland, Sept. 16-19, 1996, vol. 3, pp. 219-222