Study of DCT Watermarking Methods

V. Buchaillet and M.A. Ambroze

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

Abstract

In digital watermarking, information are hiding into audio, image and video files with the main goal to be invisible at the human visual or hearing system and robust to some piracy attacks. Nowadays many technics of watermarking has been developed and are based on spatial domain (Least Significant Bit (LSB)) and transform domain (Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT)). The basic DCT watermarking technics has been implemented in this project to study its strength and weaknesses and moreover how it is possible to improve a watermarking process and what does it cost.

Keywords

Digital watermarking, Discrete Cosine Transform, Improve a watermark process, Invisible.

1 Introduction

Since the creation of internet the availability of digital data has rapidly increase. Nevertheless, with this increasing of data, problem of protection and piracy appeared and protecting these data with copyright started to be a really important point for searchers. Indeed, to maintain the availability of digital files online and respect the owners of these files, a way to protect these files and their creators efficiently had to be finding.

One of method which is the most used to protect digital data as video, image or audio files is based on the steganography process and is named watermarking. The main goal of this method is to embed information data into the digital file to protect with an insensible form for human perception but in a way to protect it against some possible attacks against this information. Indeed, at the end of this process the data which has been protected will have to be exactly the same than the original one for the human perception but still offer the possibility of identification for the owner of the encrypting key.

In this paper, the method which has been studied is the DCT watermark method on images. This method is applied in the transform domain which is the most efficient domain to realise an invisible watermark (Mistry, 2010). Furthermore, this method has been applied to images to see easily the impact of the watermarking.

This study will only be focus on the performance of the DCT watermarking technic and study the factors which could affect the invisibility of the watermark. Nevertheless, by doing some amelioration in the second part of the research the watermark process developed will be protect against some attack even if creating a robust watermarking process is not the main goal of this research.

2 Discrete Cosine Transform Watermarking Studied

The principle of the DCT process is to break an image into different frequency bands (Mistry, 2010) in order to embed information into the middle frequency bands of the image to be invisible to the human perception which is sensible to the low frequencies. Furthermore, image compression systems affect more high frequencies so choosing the medium frequencies avoid a part of this problem.

A. Step of The DCT embedding method studied

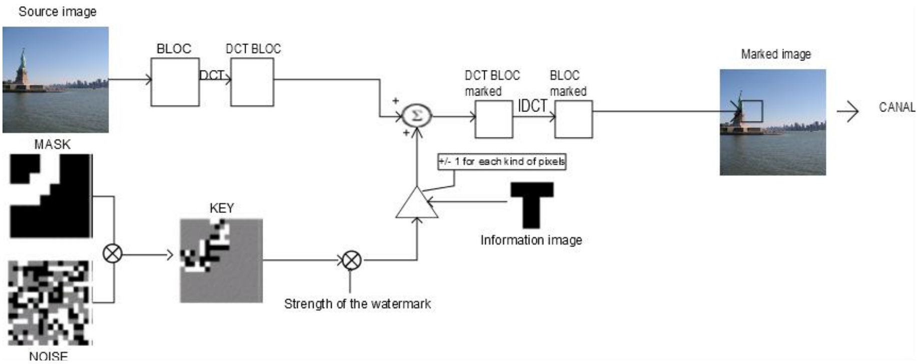

Figure 1: Scheme of the system studied

1) Isolate the blue component of the RGB colour of the original image because working on the blue component will increase the invisibility of the mark. Indeed, the human perception is less sensible to blue component that any other.

2) Divide the original image onto blocs of pixels which have a size proportional to the original and information image.

3) Transforms each bloc by using the DCT algorithm.

4) Encryption of the information using an encrypting key which will embed the information only on the medium frequencies.

5) Inversion of the DCT process and reassembling of each pixel blocs to have an image back which carry the mark.

B. Step of The DCT decoding method

To decode the information which has been encode the user will need the image where the information has been encoded and the encrypting key to decode this information. Then, if all the information is given to the receiver this one is able to decode it by following the scheme on figure 2.

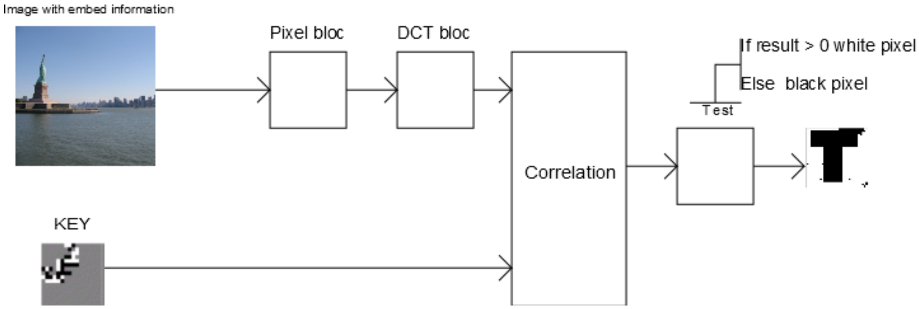

Figure 2: Scheme of the system studied

Indeed, the decoder will first take a bloc of pixels of the same size than the one which was taken by the encoder. Then, the DCT algorithm is applied to this bloc. Then, the DCT bloc and the encrypting key are comparing by a correlation system which will send back a value which will tell the dependency between this two blocs. The value sending back by the correlation system will be between -1 and 1.So, if the correlation system send a value superior to zero that's mean that the correlation is high so a black pixel will be encode however a white one will be encoded. So, at the end by adding all this pixels together it will rebuild the information image.

C. Experiences applied to the DCT watermarking method

In the watermark process there is few things which can affect the visibility and the quality of the mark, like the strength of the watermark or the frequencies of a bloc. To analyses the efficiency of the method implemented three parameters have been test.

The first one is the difference between the original image and the mark image which is called distortion. Indeed, this allow us to see if the watermark is hide enough or if just by doing this simple manipulation a user can see which information has been mark. In the case of this study the following result has been finding.

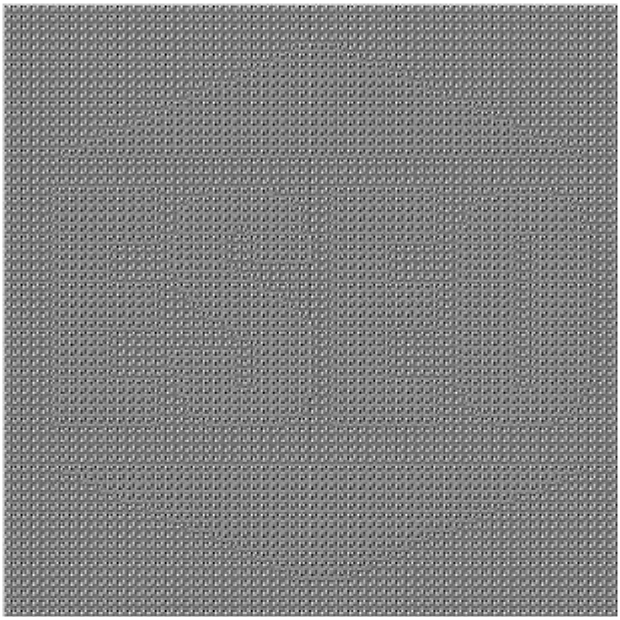

Figure 3: Distortion applied on images after applying the DCT watermarking

By analysing the result, it is possible to see that the mark can be seen. So the way to mark the information could be improved by for example find a way to scramble the information to be sure that the information will not be seen.

In a second analysis it has appeared that in some cases the retrieve information after the decoding process was noisy.

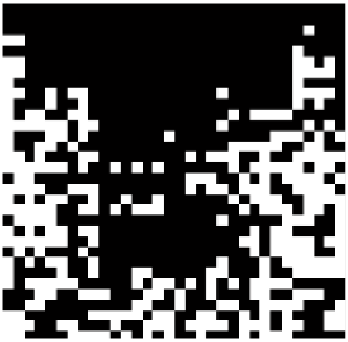

Figure 4: Example of noisy retrieved image

This noise was detected most of the time when the strength of the watermarking process was setting too low. To analyse how the strength was influencing the watermarking process a test has been done to show the influence that this parameter has on the error between the original image and the mark image and the peak signal to noise ratio.

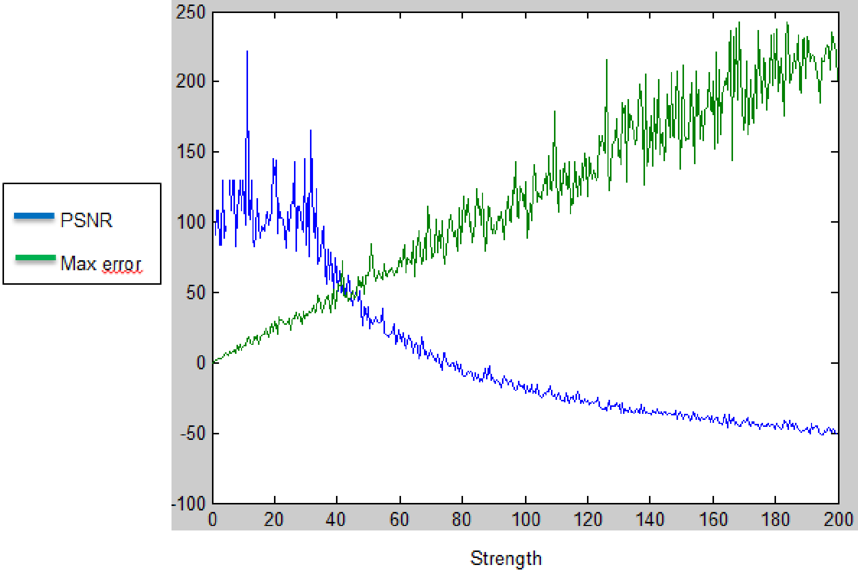

Figure 5: Influence of the watermarking strength on the peak signal to noise ratio and the error between the original image and the mark one.

So this experiment as shown that the strength of the process must be chosen well if the user want to retrieve the image without noise. Nevertheless, by testing on some images to use the best strength to embed the image another parameter has been finding. Indeed, when the watermarking process is applied to image with light colours the zones of the image will bring noise has it is possible to see on the following figure.

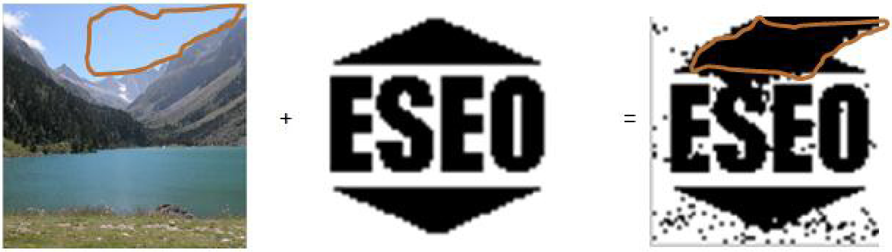

Figure 6: Influence of light colours on the watermarking process.

To conclude, the DCT watermarking which was studied was efficient to mark an image but not so efficient for hiding it or caring information without deteriorate it.

D. Improvement of the system

By doing the previous analysis an idea has come to deal with the light colours problem. Indeed, if a threshold value can be set on the DCT coefficient that have to be mark on each bloc, then the blocs which are not goodwill be dropped and the efficiency and the robustness of the watermark process will be increase.

To realise this improvement some step of the method has been modified. Indeed, each bloc taken from the original image will be 8X8 pixels bloc. This change has been made to be sure that even by dropping some blocs all the information to mark will fit in the source image. Furthermore, by dropping some blocs and taking some others this will scramble the mark during the process and increase the robustness of the mark.

The biggest modification of the process has been the bloc selection process. This step analyse DCT coefficients of the frequencies selected by the encrypting key and if there is less than half of them which are higher or equal to the threshold then the bloc will be dropped and the information will be marked in the next valuable bloc.

3 Conclusion

Digital watermarking can protect image from unauthorized modification done on an image by some noise or some person. The DCT system studied is better than a spatial domain watermark by the fact by the fact that it is more robust against compression or noise. Nevertheless, it can be improve to be more robust or even be secure but this can of improvement will take a long time to implement and will add some cost to the watermark process as computational or information cost.

4 References

Cox, I.J, Miller M, Bloom J, Fridrich J and Kalker T(2008), ‘Digital Watermarking and Steganography (second edition)’, Burlington: Morgan Kaufmann Publishers, ISBN: 978-0-12-372585-1.

Mistry, d., *comparison of digital watermarking methods*, International journal of computer science and engineering, vol.2, India: Gandhibagar, 2010.