ISSN 2348 – 9928
IJAICT Volume -1, Issue-7, November 2014 Doi:01.0401/ijaict.2014.01.29 Published Online 05 (05) 2014

IMAGE AUTHENTICATION: A FEW APPROACHES USING DIGITAL WATERMARKING

Ms. P. Sangeetha
Nehru Institute of Technology,
Coimbatore, Tamilnadu , India.

Ms. Preethi Chacko
Nehru Institute of Technology,
Coimbatore, Tamilnadu , India.

Abstract— We might think that the images that we pick are all ours. Images may be secure enough with a Watermark that could be very well traced down. A digital Watermark is a digital signal or pattern inserted into a digital image. Since this signal or pattern is present in each unaltered copy of the original image, the digital Watermark may also serve as a digital signature for the copies. The desirable characteristics of a Watermark are (1) Watermark should be resilient to standard manipulations of any nature. (2) It should be statistically irremovable. Every Watermarking system consists at least two different parts: Watermark Embedding Unit and Watermark Detection and Extraction Unit. In this paper, we discuss an algorithm for embedding and detecting the Watermark in a still image. A robust, secure, invisible Watermark is imprinted on the image I, and the Watermarked image WI, is distributed. The author keeps the original image I. To prove that an image WI' or a portion of it has been pirated, the author shows that W' contains his Watermark (to this purpose, he could but does not have to use his original image I). The best a pirate can do is to try to remove the original W Watermark (which is impossible if the Watermark is secure). There can be another way out for the pirate, as to embed his signature in the image. But this does not help him too much because both his "original" and his Watermarked Image will contain the author's Watermark (due to robustness property), while the author can present an image without pirate's Watermark. Thus, the ownership of the image can be resolved in the court of law. We have done the implementation in MATLAB and doing the simulation in C++.

Keywords— Watermark, Transform Domain, DCT, FFT, Picture Cropping.

I. INTRODUCTION

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.

A digital Watermark is a digital signal or pattern inserted into a digital image. Since this signal or pattern is present in each unaltered copy of the 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 recipient), or
- Be common to multiple copies (e.g., to identify the document source)

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 "best describes" the original file's content. As a simple example, the Checksum field for a disk sector would be a fingerprint of the preceding block of data. Similarly, Hash Algorithms produce fingerprint files.

Digital Watermarking is also to be contrasted with Public-Key Encryption, which also transforms original files to another form. It is a common practice nowadays to encrypt digital documents so that they become un-viewable without the decryption key. Unlike encryption, however, Digital Watermarking leaves the original image or basically intact and recognizable. In addition, Digital Watermarks, as signatures, may not be validated without special software. Further, decrypted documents are free of any residual effects of encryption, whereas Digital Watermarks are designed to be persistent in viewing, printing, or subsequent re-transmission or dissemination.

1.1 The purpose of digital watermarks

Two types of digital Watermarks may be distinguished, depending upon whether the watermark appears as:

- **Visible** Watermarks
- **Invisible** Watermarks

1.1.1 Visible watermarking

Visible Watermarks are used in much the same way as their bond paper ancestors, where the opacity of paper is altered by physically stamping it with an identifying pattern. This is done

© 2014 IJAICT **(www.ijaict.com)**

to mark the paper manufacturer or paper type. One might view digitally Watermarked documents and images as digitally "stamped".

1.1.2 Invisible watermarking

Invisible Watermarks are potentially useful as a means of identifying the source, author, creator, owner, and distributor or authorized consumer of a document or image. For this purpose, the objective is to permanently and unalterably mark the image so that the credit or assignment is beyond dispute. In the event of illicit usage, the Watermark would facilitate the claim of ownership, the receipt of copyright revenues, or the success of prosecution.

Watermarking has also been proposed to trace images in the event of their illicit redistribution. Whereas past infringement with copyrighted documents was often limited by the unfeasibility of large-scale photocopying and distribution, modern digital networks make large-scale dissemination simple and inexpensive. Digital Watermarking makes it possible to uniquely mark each image for every buyer. If that buyer then makes an illicit copy, the illicit duplication may be convincingly demonstrated.

1.2 Requirements of watermarks

To be effective in the protection of the ownership of intellectual property, the invisibly Watermarked document should satisfy the following criteria:

- The Watermark must be difficult or impossible to remove, at least without visibly degrading the original image
- The Watermark must survive image modifications that are common to typical image-processing applications (e.g., Scaling, colour requantization, dithering, cropping, and image compression)
- An invisible Watermark should be imperceptible so as not to affect the experience of viewing the image
- For some invisible Watermarking applications, Watermarks should be readily detectable by the proper authorities, if imperceptible to the average observer. Such decodability without requiring the original, un-Watermarked image would be necessary for efficient recovery of property and subsequent prosecution.

One can understand the challenge of researchers in this field since the above requirements compete, each with the others. None of the digital techniques have yet to meet these tests.

1.3 Watermarking a still image

The important steps in watermarking an image are:

- Embedding the Watermark
- Attacking the Watermarked image to test efficiency
- Extraction of the Watermark

II. TECHNIQUES FOR WATERMARKING

Watermarking techniques tend to divide into two categories, text and image, according to the type of document to be watermarked. Techniques for images:

The Watermarks can be included in two domains:

- **Spatial** Domain
- **Frequency** Domain

2.1 Spatial domain

Several different methods enable Watermarking in the spatial - domain. The simplest (too simple for many applications) is to just flip the lowest-order bit of chosen pixels in a gray scale or color image. This will work well only if the image will not be subject to any human or noisy modification. A more robust Watermark can be embedded in an image in the same way that a Watermark is added to paper. Such techniques may superimpose a Watermark symbol over an area of the picture and then add some fixed intensity value for the Watermark to the varied pixel values of the image.

The resulting Watermark may be visible or invisible depending upon the value (large or small, respectively) of the Watermark intensity. One disadvantage of spatial domain Watermarks is that picture cropping (a common operation of image editors) can be used to eliminate the Watermark. Spatial Watermarking can also be applied using color separation. In this way, the Watermark appears in only one of the color bands. This renders the Watermark visibly subtle such that it is difficult to detect under regular viewing. However, the Watermark appears immediately when the colors are separated for printing or xerography. This renders the document useless to the printer unless the Watermark can be removed from the color band. This approach is used commercially for journalists to inspect digital pictures from a photo-stock house before buying un-Watermarked versions.

2.1.1 The process

- The Spatial method involves the 2D array of pixels in the container image to hold hidden data.
- Most common method is known as **Least Significant Bit method (LSB).**

This technique involves replacing the N least-significant bits of each pixel of the container image with the data of the hidden message.

© 2014 IJAICT **(www.ijaict.com)**

- The pixels for gray scale images are encoded with 8 bits.
- We swap the higher resolution bits of the container image for the lower resolution bits of the hidden image.
- The key used by the sender and the receiver is the number of bits N of hidden data imbedded in each container pixel.

2.1.2 Advantages

- It is a well-rounded method and lends itself to a variety of information hiding applications.
- A large quantity of embedded information can be included in even the most modestly sized images.
- LSB can also allow for the hiding of photographic images and even audio recordings.
- Calculation complexity is relatively low.

2.1.3 Disadvantages

- Any attack or noise distortion of the composite image will seriously damage the imbedded data.
- Cropping or translation of the composite image will destroy an equal portion of the imbedded image.
- Robustness limits the overall effectiveness.

2.2 Frequency domain

Watermarking can be applied in the frequency domain (and other transform domains) by first applying a transforms like the Fast Fourier Transform (FFT), Discrete Cosine Transforms (DCT), Wavelet Transforms etc. Since high frequencies will be lost by compression or scaling, the Watermark signal is applied to lower frequencies, or better yet, applied adaptively to frequencies that contain important information of the original picture (feature-based schemes). Since Watermarks applied to the frequency domain will be dispersed over the entirety of the spatial image upon inverse transformation, this method is not as susceptible to defeat by cropping as the spatial technique.

2.2.1 The process sequence

- Frequency methods encode the data across the global frequencies of the image.
- This method enables to achieve greater robustness to attack.
- Two types of information hiding methods are
  - Fast Fourier Transform (FFT)
  - Discrete Cosine Transform (DCT)

We focus our attention in FFT.

2.2.2 The FFT watermarking

This transformation is a one that converts the time domain signal into a signal of the frequency domain. The watermarking is now performed over the transformed values instead of the spatial domain values of the image. The steps in a nutshell are:

- 2D FFT of the original image.
- Isolate the coefficients with the maximum information – similar to denoising
- Then the watermark is embedded
- The inverse transform is applied to get the watermarked image

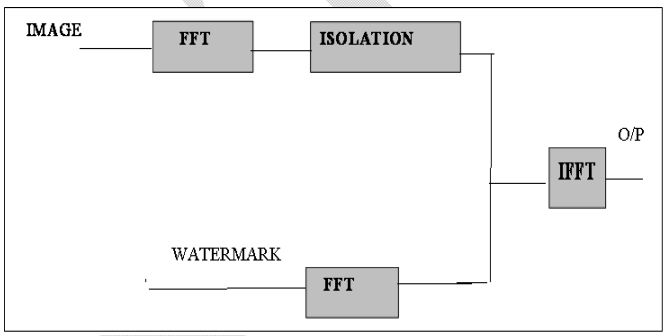

Fig 1 : The FFT Watermarking

III. IMPLEMENTATION

3.1 Algorithm for embedding the watermark

1. Start the process.
2. Get the text data (eg. your college name), the original image.
3. Convert the text data to a binary row vector.
4. Scale the binary vector.
5. Create the data mark.
6. Compute the FFT and decompose into the magnitude and phase
7. Create the ring of the data mark (using loops)
8. Add the ring to the magnitude of the image
9. Reduce the magnitude points where the data bit is zero.
10. Convert the matrix into an image.(i.e. watermarked image)
11. Output the watermarked image.
12. Stop the process.

3.2 Algorithm for extraction of watermark

1. Start the process.
2. Get the watermarked image.
3. Initialize the matrix used in storing the

© 2014 IJAICT **(www.ijaict.com)**

Extracted magnitude coefficients.

4. Compute the magnitude of the FFT of the image.
5. Calculate the size of the image.
6. Extract the magnitude coefficients along the circle.
7. Thresholding.
8. Convert to estimated data bits.
9. Convert the bits to a text message.
10. Output the watermark (text).
11. Stop the process.

Fig 2 : Original Image

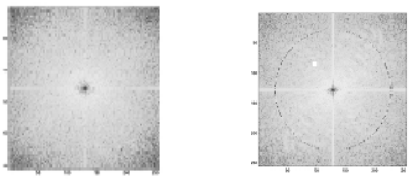

Fig 3: FFT of the original image

FFT – image embedded with watermark (ring format)

3.3 For High Level Security

- The watermark embedding process should occur on the spot (eg.the images in your website should be converted in to watermarked image immediately before the image gets downloaded in to the user's machine).
- The owner should have a database of watermarks and there should be a key in selection of the watermarks.
- There should be a ***MOBILE AGENT*** to watch which user has been accessing your website and that address should be added in the database.

So the image he downloaded last minute and this minute will be same for Human Visual System, but not actually same. So hacking is 99.9999% impossible.

3.4 Advantages of our paper

- Since we are making use of frequency domain, it takes much time for a hacker to find the particular frequency that we used in embedding.
- Even if he is making a trial and error method to find the frequency with the downloaded images of same picture at different times, he can't - since the frequency and watermarks vary each time for same image.
- Since the owner is having a mobile agent, he can easily identify the wrong person.
- This is a technique that does not allow the intruder to attack the image by JPEG compression, scaling or other methods.

3.5 Applications

- Copyright ownerships.
- Secret messaging.
- Mobile agencies eg. If the persons having windows XP pirated version, when he connects to net his system gets crashed without his knowledge.

IV. CONCLUSION

A robust and transparent Digital Watermarking for image copyright protection has been developed in this work. By embedding the Watermark in the most significant components, i.e. by the methods explained in this paper and by considering the texture of the image, two possible schemes are proposed. These methods are robust and provide high imperceptibility.
The implementation of the same has been done using MATLAB and the figures shown here are outputs of the same. This technique of image authentication is a one that is not easily imperceptible. We dedicate this paper to the proposition that "hackers already know our algorithm". As a final word to say "Security (success) is a journey, never a destination".

References

[1] R.L.Lajendijk, Langelaar and G.C.Setvawa "Watermarking Digital Image and Video Data", IEEE Transaction in Signal Processing, April 2013.

[2] Ingmer Cox, Jeffrey Bloom, Mathew Miller, "Digital Watermarking", IEEE Transactions on Circuits And Systems for Video Technology, March 2011.

[3] Gonzalez ,"Digital Image Processing", Electronics Letters Vol. 48 No. 8, 12th April 2012.

[4] Katzenbeissse, r Stefan, Fabien A.P.Petitcolas, "Information Hiding Techniques for Steganography and Digital Watermarking", Signal Processing Applications ,Vol. 2,Issue 2,pp. 102-107,April 2012.

[5] Jae Kyu Suhr, Ho Gi Jung, Gen Li, and Jaihie Kim "Mixture of Gaussians-Based Background Subtraction for Bayer-Pattern Image Sequences" IEEE Transactions on Circuits And Systems for Video Technology, Vol. 21, NO. 3, pp.365-370, March 2011.

© 2014 IJAICT **(www.ijaict.com)**