International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-3, Issue-5)

Research Article | **May 2014**

Improved Data Embedding into Images Using Histogram Shifting

Sapana Saini,
Master of Computer Applications,
School of Information Technology,
VIT University, Vellore, India

Brindha K.
Assistant Professor (Senior)
School of Information Technology,
VIT University, Vellore, India

Abstract:

This paper is proposed for improved security and integrity of image type data. Watermarking is one of the techniques which we are studying in this paper. In watermarking we hide digital information in carrier signal for authentication and copyright. Watermarking can be of two type visible and invisible watermarking. In this paper we are researching more about invisible watermarking. The main objective of this paper is to provide a better mechanism for invisible watermarking technique with less image distortion. We are using histogram shifting method in this paper. We will be emphasizing on reversible watermarking where we can update and extract the existing watermark. The proposed method will provide a enhanced system for reversible watermarking technique with less image distortion. Main aim of watermarking is to secure the imperceptibility of a data file and to guarantee the authorized use of data file.

Keywords: Carrier Pixel, Histogram Shifting, Image Classification, Reversible Watermarking, Watermarking

I. INTRODUCTION

Today, when everything is becoming digital and is available on network, security is a major issue. Today data security is a basic requirement in every organization. It is necessary to secure the data and to provide authenticate and authorized form of data. Today all kind of applications are using digital information from network. It is difficult to track all the users who are using the information in an unauthorized way. [14, 15] There are various types of methods available for securing the data such as cryptography, steganography, watermarking etc. Watermarking is the technique for copyrighting and authorization. We also use watermarking for tracking the data over the network. Watermarking provide us the facility for a secure and reliable use of information. Watermarking is a technique where we add a small form of data called watermark in the carrier file. This watermark can be visible or invisible. This watermark can be extracted or removed from the original image as per the need. The base file or the carrier file can be of any media type such as image, audio and video. Here we are working on image type of data which are commonly used.

Watermarking technique can be divided into two parts: 1) visible watermarking and 2) invisible watermarking. Visible watermarking is most commonly used for copyrighting. [2] Generally visible watermarking consists of a visible logo or signature of the owner and gives information about the authorized person directly. Visible watermarking involves the authority person and the end user for proper utilization of the information as it is clearly visible to the user. Invisible watermarking consists of the information in a hidden way. In this kind of watermarking the carrier file appear the same as the original image. [1,5,8] Invisible watermarking is mostly used for tracking the use of data file. Invisible watermarking is also used for comparing the data file after any kind of attack. We can also measure the image quality using invisible watermarking. In this paper we are working on invisible watermarking. Watermarking can also be divided into two types such as reversible watermarking and permanent watermarking. We use permanent watermarking when the watermark information or the authorized information has to be eternally. This provides more authorization power and protection. But this type (robust) of watermarking is very strict for use. Reversible watermarking is comparatively more useful as authorized person always have the rights of changing the watermark. Reversible watermarking is used when we have to modify the watermark information in a continuous basis. Reversible watermark can provide us the original image after extracting the watermark information. Our paper focuses on invisible-reversible watermarking. The combination of these two techniques will provide a better mechanism for watermarking with great reliability and security. In present reversible watermarking techniques user can bring back the original carrier image from its watermarked version by extracting the watermark. This makes the modification process achievable with respect to watermark information. [6] The reversible property of watermark can affect the data protection and can begin discontinuity in data. We can also say that image is not secure properly if we remove the watermark. In reversible watermarking even if watermark removal is possible, its imperceptibility has to be guaranteed. Watermark removal can distort the image quality hence we need a reversible watermarking technique with less distortion and increased capacity.

Histogram is the graphical representation of an image. Histogram represents the pixel value and density at a particular pixel. Histogram plots the pixel for each part of the image. We can easily identify pixel distribution and density of colors and tonal distribution with a histogram. There are various algorithm which supports histogram functionality in order to manipulate original image. A histogram gives us the highest and lowest pixel values in graph. A user can dynamically adjust the image brightness and can adjust image display according his need. Histogram shifting is one of the techniques which we use to modify or to extract a certain group of pixel from a image.

II. WATERMARKING AND STEGANOGRAPHY

Watermarking and steganography both techniques are used for security purpose. These both techniques are major part of information hiding. These techniques offer the different methods for hiding sensitive information in an undetectable and/or irremovable way in audio, video or image type of data. Watermarking and steganography both are hiding techniques in which the digital image file is changed in a way that one can see the background image or the text without any kind of corruption or distortion in the image quality.

In secret government communication or defense services information is really sensitive. While transmitting this information from one point to another point it is really essential that no one else should access this information except only two sides of communication. In this kind of scenario we use steganography and cryptography. Steganography is the act of hiding the information into the carrier object such that only the receiver and sender should be aware of the hidden message. The main object of steganography is to hide the information in the carrier object such that the message should not be detectable. Steganography is used for confidential data storage and secret communication. Compare to cryptography steganography is better in one context as it does not seek attacker's attention. Steganography can be implemented using different techniques such as permutation steganography, least significant bits (LSB), bit-plane complexity segmentation (BPCS) and chaos based spread spectrum image steganography (CSSIS).

Today in some applications which use digital information, it is necessary to maintain the original information without any distortion and disturbance. The main aim of watermarking is to provide the authorized access and copyrights. In watermarking we do not focus on security of hidden message but to keep the original image secure. Watermarking focuses on that no one except the authorized person should be able to remove or replace the hidden watermark information. [2, 3] Watermarking methods need to be very robust to attempts to remove or modify a hidden message. Source tracking is one of the applications of digital watermarking. A watermark can be inserted into a digital signal at any point of circulation. If a data file is found in use without proper authorization then the watermark may be retrieved from the copy and the source of the distribution is known. This facilitates prevention of illegal use of data object. [4] Watermarking provides a proof ownership of digital data as we embed copyright information into image or video file. Watermark includes information about the author and copyrights of the respected person. Watermarking can be implemented using various algorithms and techniques such as least significant bit algorithm, frequency domain, spatial domain etc. while applying watermark we also consider objective of the same as we have blind watermarking, semi-blind watermarking and non blind watermarking. Steganography and watermarking both are security enhancement techniques with hiding methodology. The main difference between watermarking and steganography is that the first one secures the carrier object with copyright information and the later one secures the hidden message into the carrier object.

III. METHODOLOGY

In this paper we are researching on reversible- invisible watermarking. We have divided this process in different sequential modules. These modules are interconnected and flow of data is in both ways. Here we are using image type of data as carrier object and text file as invisible watermark. We are not using the whole image for watermarking but only a part of image will be used for embedding process. In reversible watermarking if we use whole image as watermark object it may affect the image quality. Dividing the image into parts will minimize quality distortion. The very first module is to get the textured image from the original image. Here with textured image we are referring original image with background and front image object. In an image we have different pixel values.

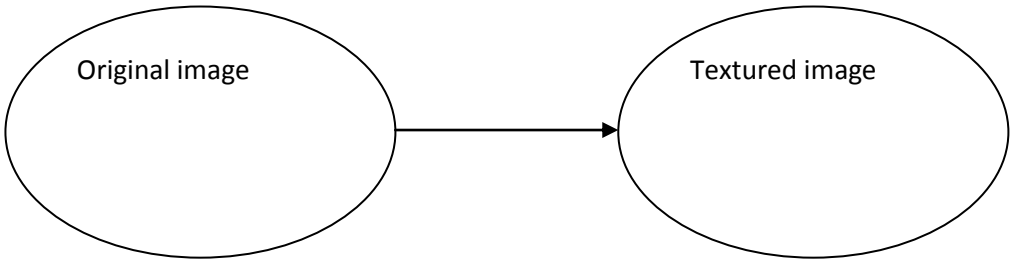

Figure 3.1 Module 1

For dividing image into two parts as background and front object we calculate the pixel value. Pixel value of background will be lesser compare to front image object. We are also using background detector and grouping segment modules. Once we get the textured image we will perform histogram shifting process for finding suitable pixel values for watermark embedding. Histogram calculation gives us pixel values and we can decide appropriate pixel for watermarking. In a histogram we have one highest value called maxima and one lowest value called minima. All other pixel value comes under these two values. We consider pixel values between these values as suitable for watermark. When we modify pixel value for embedding process it should not cross the minima and maxima limit, this is called underflow and overflow of pixel. We are using local specification of image.

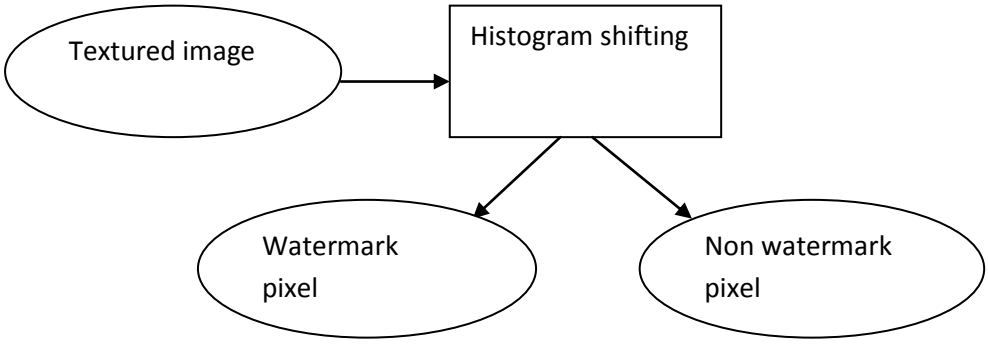

Figure 3.2 Module 2

In next module we are embedding watermark in suitable pixels. This process will minimize image distortion as we are not using whole image instead a part of it. It increases the image value and quality. This process makes the data embedding more effective and reliable. For embedding the watermark content we are using least significant bit algorithm which is simple and reliable.

We are implementing reversible watermarking algorithm. After embedding watermark into image last module is to update or extract watermark information from the image. Extracting process should be in a manner that image quality should be unchanged. The pixel should get their original values so that the final image remains same as original image. We perform watermark extraction operation from authorized person who wants to remove or update watermark information from the image. This performs reverse operation from process of embedding. This module gives original image and watermark information as result.

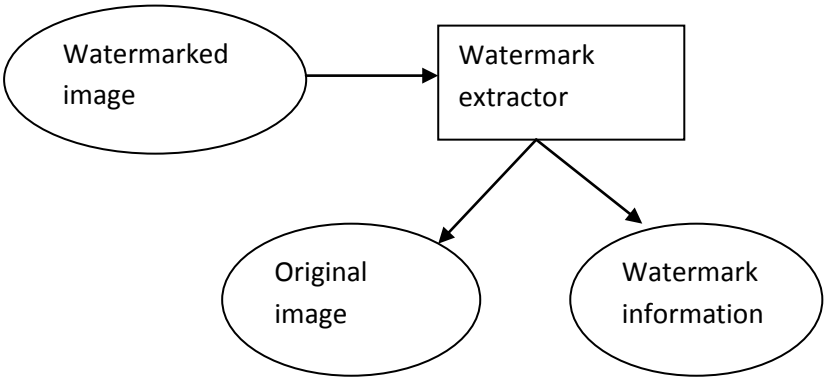

Figure 3.3 watermark extractor

1V. RESULT AND FUTURE WORK

Our project is working successfully as achieving the requirements. We are able to successfully embed and extract the image and text file from the carrier file. Watermarking process is able to function by itself. Reversible function of watermark is also reliable. We have tested all the modules as individual and integrated form. We have also compared the results from different images and also between original image and watermarked image

Figure 4.1 (a) original image (b) watermarked image

We can see both the images given here are same and image distortion is on minimum level. Histogram shifting and our new method of dividing the whole image into suitable carriers is a successful story. Watermark embedding and extracting process is synchronized. Our proposed system is providing better reversible watermarking technique with minimum image distortion and maintaining image quality. This system is reliable and secure and gives better copyright permission. In future we will be improving watermark robustness in security and image quality way. We will also try to increase embedding capacity. Watermarking is a modern technique for tracking and authenticate digital data.

REFERENCES

1. Sang-Kwang Lee, Hyang-Mi Yoo, Jae-Won Suh, "Reversible data hiding employing histogram shifting using a rotated even–odd difference image", 2013
2. R. chandramouli, Nasir menon, Majid rabbani, "watermarking"
3. Navnath narawade, Rajendra kanphade, "Reverssible watermarking:a complete review", [Volume 2, Issue 3, June 2011];
4. Matthew Elliott and Brian Schuette, "Digital Image Watermarking", December 21, 2006
5. Coatrieux, G., Le Guillou, Cauvin, Roux, C,"Reversible Watermarking for Knowledge Digest Embedding and Reliability Control in Medical Images", March 2009
6. F. Bao, R. H. Deng,B.C.Ooi, andY. Yang, "Tailored reversible watermarking schemes for authentication of electronic clinical atlas," December 2005.
7. Che-Wei Lee1 and Wen-Hsiang Tsai, "A Lossless Data Hiding Method by Histogram Shifting Based on an Adaptive Block Division Scheme", 2010
8. Zhi-Hui Wang, Chin-Feng Lee, Ching-Yun Chang, "histogram-shifting-imitated reversible data hiding", 2013
9. Rosziati Ibrahim and Teoh Suk Kuan, "Steganography Algorithm to Hide Secret Message inside an Image", February 25, 2011.
10. http://www.datahide.com/BPCSe/applications-e.html, 2014
11. Fadoua DRIRA, Florence DENIS, Atilla BASKURT, "Image watermarking technique based on the steerable pyramid transform"
12. http://www.differencebetween.net/business/product-services
13. http://en.wikipedia.org/wiki/Steganography
14. Minewa M. Yeung and Fred Mintzer, "An Invisible Watermarking Technique For Image Verification " 1997
15. http://en.wikipedia.org/wiki/Digital_watermarking