DWT based Invisible Image Watermarking Algorithm for Color Images

Anumol T.J
II M.Tech, ECE Dept
Karunya University,
Coimbatore, India

P Karthigaikumar
Asst.Prof, (SG), ECE Dept.
Karunya University,
Coimbatore, India

ABSTRACT
In recent years, the applications about multimedia have been developed rapidly. Digital media brings about conveniences to the people, because it is easy to be processed. At the same time, it enables the illegal attackers to attack the works. For the protection of data there has been growing interest in developing effective techniques to discourage the unauthorized duplication of digital data. Digital watermarking is the process of embedding information into a digital signal in a way that is difficult to remove. The fragile and semi fragile watermarking techniques have some serious disadvantages like increased use of resources, larger area requirements, and high power consumption. In order to overcome this, robust watermarking technique is proposed. Robustness can be defined as resilience for a watermark to remain unaffected even when digital content is passed through various processes and attacks. Invisible robust watermarking is the most accurate method. Embed a watermark containing key information such as authentication or copyright codes.

Keywords
Digital watermarking, DWT, invisible watermarking, copyright protection

1. INTRODUCTION
The process of digital watermarking involves the modification of the original multimedia data to embed a watermark containing key information such as authentication or copyright codes. The embedding method must leave the original data perceptually unchanged[1]. The major technical challenge is to design a highly robust digital watermarking technique, which discourages copyright infringement by making the process of watermarking removal tedious and costly.

A watermarking algorithm consists of the watermark structure, an embedding algorithm, and an extraction, or a detection algorithm [2].In multimedia applications, embedded watermarks should be invisible, robust, and have a high capacity. Invisibility refers to the degree of distortion introduced by the watermark. The literature survey explain robustness is the resistance of an embedded watermark against intentional attacks such as noise. Capacity is the amount of data that can be represented by an embedded watermark [5].The most applicable and accurate method is invisible robust watermarking and that is used in this paper. Watermarking represents an efficient technology for ensuring data integrity and data-origin authenticity. Watermarking the process of embedding data into multimedia element can primarily for copyright protection. Because of its growing popularity, the Discrete Wavelet Transform (DWT) is commonly used in the proposed watermarking scheme increase, area increases so power consumption.

Watermarking is not a fully mature technology lot of research is going on this field, especially to increase security and capacity of watermark data. Most of researchers try to increase the watermark capacity by compromising image quality, because there is a trade off among data rate, security and imperceptibility. But with our scheme we will be able to embed more number of watermark bits without affecting the imperceptibility of the cover image The fragile and semi fragile watermarking techniques have some serious disadvantages like increased use of resources, larger area requirements, and high power consumption. In order to overcome this, robust watermarking technique is proposed . By incorporating parallel arrangement, significant reduction of power can be achieved. So, it is worth to solve this problem, because by solving it we will get a watermarking technique that will increase the robustness of watermarking. In numerical analysis and functional analysis, a discrete wavelet transform (DWT) is any wavelet transform for which the wavelets are discretely sampled. As with others wavelet transforms, a key advantage it has over Fourier transforms is temporal resolution: it captures both frequency and location information (location in time)

2. GENERAL WATERMARKING PROCEDURE

2.1 General Block Diagram

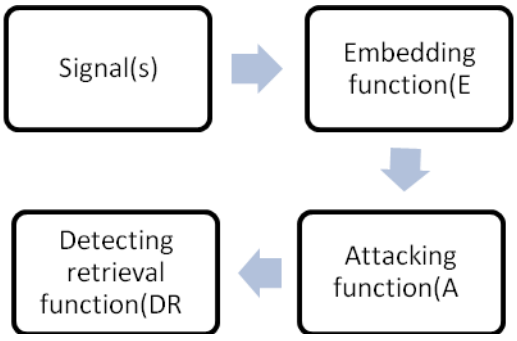

Figure 1 Basic block diagram

Digital watermarking is one of the proposed solutions for copyright protection of multimedia data. This technique is better than Digital Signatures and other methods because it does not increase overhead. In this paper plan to present a new image watermarking technique that can embed more number of watermark bits in the cover image without affecting the imperceptibility and increase the security of watermarks [4].Digital watermarking is the process of embedding information into a digital signal in a way that is difficult to remove [6]. The signal may be audio, pictures or video. In this paper image is the host signal and embedding the secret data and the extract the same. In this process enhancing the network security.

3. EMBEDING AND EXTRACTION STAGE

3.1 Embedding stage

Watermarking is not a fully mature technology lot of research is going on this field, especially to increase security and capacity of watermark data. Most of researchers try to increase the watermark capacity by compromising image quality, because there is a trade off among data rate, security and imperceptibility. But with our scheme we will be able to embed more number of watermark bits without affecting the imperceptibility of the cover image.

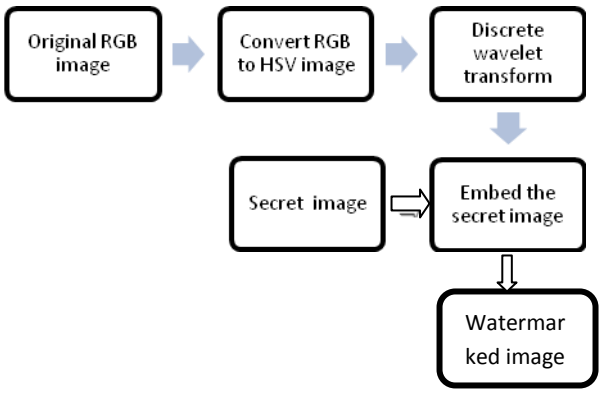

Figure 2 Embedding stage

One of the most important features that make the recognition of images possible by humans is color. Color is a property that depends on the reflection of light to the eye and the processing of that information in the brain. The color is used every day to tell the difference between objects, places, and the time of day. Usually colors are defined in three dimensional color spaces usually colors are defined in three dimensional color spaces. These could be RGB (Red, Green, and Blue), HSV (Hue, Saturation, and Value) or HSB (Hue, Saturation, and Brightness). The last two are dependent on the human perception of hue, saturation, and brightness [6]. Color represents the distribution of colors within the entire image. This distribution includes the amounts of each color, but not the locations of colors.

In numerical analysis and functional analysis, a discrete wavelet transform (DWT) is any wavelet transform for which the wavelets are discretely sampled [4]. As with other wavelet transforms, a key advantage it has over Fourier transforms is temporal resolution: it captures both frequency and location information (location in time). The discrete wavelet transform has a huge number of applications in science, engineering, mathematics and computer science [9]. Most notably, it is used for signal coding, to represent a discrete signal in a more redundant form, often as a preconditioning for compression. The DWT of a signal x is calculated by passing it through a series of filters [8]. First the samples are passed through a low pass filter with impulse response g resulting in a convolution of the two:

$$y[n] = (x * g)[n] = \sum_{k=-\infty}^{\infty} x[k]g[n-k]. \quad (1)$$

The signal is also decomposed simultaneously using a high-pass filter h. The outputs giving the detail coefficients (from the high-pass filter) and approximation coefficients (from the low-pass). The invisible watermarking techniques used for enhancing the network security. Fundamental role of watermarking is the reliable embedding and detection of information [3]. Digital watermark should be statistically invisible to prevent obstruction of the original image .The watermark should be robust to filtering ,additive noise, compression and other forms of image manipulation.

3.2 Extracting stage

In a digital watermarking scheme, it is not convenient to carry the original image all the time in order to detect the owner's signature from the watermarked image. Moreover, for those applications that require different watermarks for different copies, it is preferred to utilize some kind of watermark-independent algorithm for extraction process i.e. dewaters marking. Its robustness against many attacks including rotation, low pass filtering, salt n paper noise addition and compression.

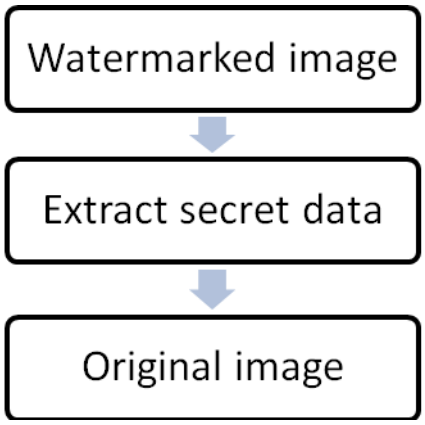

Figure 3 Extracting stage

The robustness evaluation is also carried out with respect to the spatial domain embedding and extraction. The extracted feature points can survive a variety of attacks and be used as reference

points for both watermark embedding and detection. The original content restoration information, a message authentication code, and additional data (which could be any data, such as date/time information, auxiliary data, etc.) will all be embedded into the difference values. Digital watermarks apply a similar method to digital content.

Watermarked content can prove its origin, thereby protecting copyright. A watermark also discourages piracy by silently and psychologically deterring criminals from making illegal copies. A robust watermarking scheme has to ensure the retrieved watermark is recognized, when the image quality does not get seriously harmed. Without robustness, an embedded watermark can be removed easily even in a legal procedure, and is unable to be proven. The watermark must be able to be easily and securely embedded and retrieved by the owner. Therefore, the overheads of embedding process and retrieving process should be limited in a reasonable range. The retrieved watermark can be used to determine the ownership by comparing the retrieved watermark with the assigned one. As in the definition, the goals of the reversible water- marking are to protect the copyrights and can recover the original image.

4. RESULT AND DISCUSSIONS

4.1 Input image

Fig 4: Input colour image

One of the most important features that makes the recognition of images possible by humans is color. . Color is a property that depends on the reflection of light to the eye and the processing of that information in the brain. Color represents the distribution of colors within the entire image. This distribution includes the amounts of each color, but not the locations of colors. The color is used every day to tell the difference between objects, places, and the time of day. Usually colors are defined in three dimensional color spaces. The Fig 4 green colour image is the input image.

4.2 HSV Image

Usually colors are defined in three dimensional color spaces. These could be RGB (Red, Green, and Blue), HSV (Hue, Saturation, and Value) or HSB (Hue, Saturation, and Brightness). The last two are dependent on the human perception of hue, saturation, and brightness.

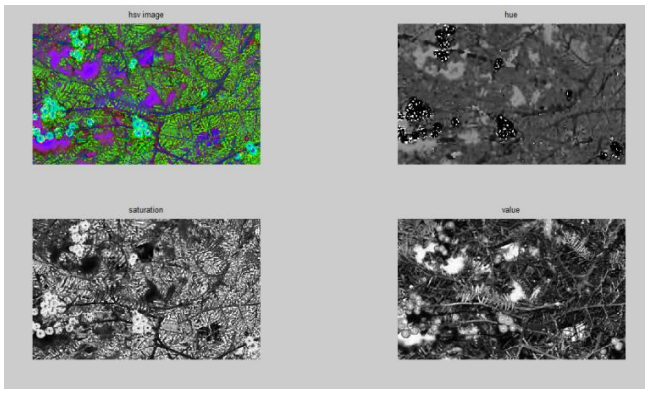

Figure 5 (a) HSV image, (b) Hue, (c) Saturation, (d) Value

Color searches will usually involve comparing color histograms, though this is not the only technique in practice. In this report Fig 5.a input RGB image converted to HSV image (Fig 5). HSL and HSV are the two most common cylindrical-coordinate representations of points in an RGB color model, which rearrange the geometry of RGB in an attempt to be more perceptually relevant than the Cartesian representation, computer applications, and are used for color pickers, in color-modification tools in image editing software, and less commonly for image analysis and computer vision. The Fig 5 split up in to three parts Hue (Fig 5a), Saturation (Fig 5b) and Value (Fig 5c). HSV stands for hue, saturation, and value, and is also often called HSB (B for brightness is and HSI, for hue, saturation, and intensity. Any of these abbreviations might be used for any of these three or several other related cylindrical models. A third model, common in computer vision applications, and value image (Fig 5c) used as input of water marking applications

4.3 Original value image and secret image

In multimedia applications, embedded watermarks should be invisible, robust, and have a high capacity. Invisibility refers to the degree of distortion introduced by the watermark .In this case Rabbit image (Fig 6b) used as secret image. Secret image (Fig 6b) will embed in to value part of the HSV image (Fig 6a).

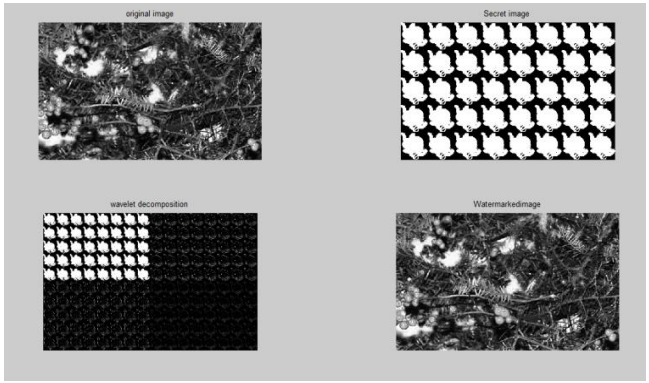

Figure 6 (a) Input value image (b) Secret image (c) DWT output (d) Watermarked image

The invisible watermarking techniques used for enhancing the network security. Fundamental role of watermarking is the reliable embedding and detection of information. In this report watermarking is done by embedded secret image (Fig 6b) in to the value part (Fig 6 a) of HSV image and we get the watermarked gray scale image like as same as the input image. Digital watermark should be statistically invisible to prevent obstruction of the original image. The watermark should be robust to filtering, additive noise, compression and other forms of image manipulation

4.4 Recovered input image and secret image

The extraction stage image watermarking we can see HSV watermarked image (Fig 7a) and RGB watermarked image (Fig 7b) and the embedded secret image is recovered back. The extracted image the secret image will recover back which is shown in Fig 7d and Fig 7c shows the recovered original image which will obtain after the extraction of secret image.

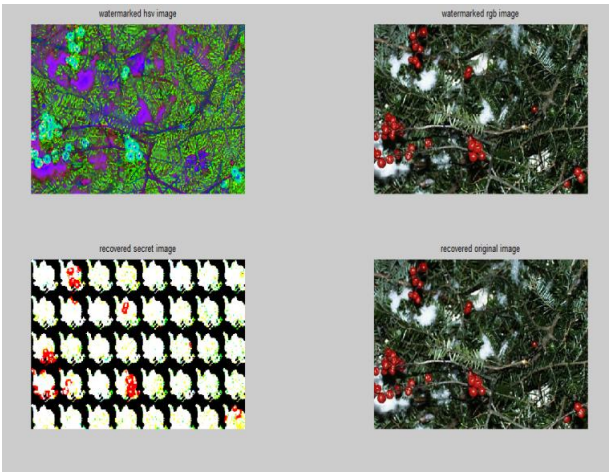

Figure 7 (a) Watermarked HSV image (b) Watermarked RGB image (c) Recovered secret image (d) Recovered original image

5. CONCLUSION

In this technique a new robust watermarking technique for color images was performed. The RGB image is converted to HSV and watermarked by using discrete wavelet transform. Watermarking embedded stage and extraction stage is designed using low power invisible watermarking algorithm. Here the host signal is an image and after embedding the secret data a watermarked image is obtained and then extracts secret image and original image separately. In future the resulted watermarked image was tested with several attackers to verify the robustness and VLSI implementation of invisible watermarking algorithm using VHDL code and check various performances like power, PSNR and tamper detection, area etc.

6. REFERENCE

[1]. P Karthigaikumar, K Baskaran," An ASIC implementation of a low power invisible robust watermarking processor"in proceedings of journal of system architecture,2010.

[2].Saraju P mohanty ,N Ranganathan,"VLSI architecture and chip for combined invisible robust and fragile watermarking", in proceedings of the IEEE workshop on signal processing system,19 June 2007.

[3]. A Mohamed Zuhair ,A Mohamed Yousef ,"FPGA based image securityauthentication in digital camera using invisible watermarking technique" International journal of engineering science and technology vol .2(6), ,1745-1751, 2010.

[4].DR .M A Dorairangaswamy,"A noval invisible and blind watermarking scheme for copyright protection of digital images" International journal of computer science and network security vol9 No.4 ,April 2009.

[5]. Christian Rey , Jean-Luc Dugelay," A surey of watermarking algorithams for image authentication", EURASIP Journal on applied signal processing, 6, 613-621, 2002

[6]. Afrin Zahra Husaini and M Nizamuddin,Challenges and approach for a robust image water marking algorithm, International journal of electronics engineering 2(1), pp 229-233, 2010.

[7].Raja' S Alomari and Ahmed Al Jaber, "A Fragile watermarking Algorithm for content authentication "International journal of computing and information science vol 2.No. 1 April 2004.

[8]. R. Schyndel, A. Tirkel, and C. Osborne, "A digital watermark," in IEEE,Proc. Int. Conf. Image Processing, vol. 2, pp. 86–90, 1994.

[9]. S. P. Mohanty, R. Kumara C., and S. Nayak, "FPGA Based Implementation of an Invisible-Robust Image Watermarking Encoder," Lecture Notes in Computer Science (LNCS), CIT 2004, Springer-Verlag, Vol. 3356, pp. 344-353, 2004.

[10]. S. P. Mohanty, N. Ranganathan, and R. K. Namballa, "VLSI Implementation of Invisible Digital Watermarking Algorithms Towards the Development of a Secure JPEG Encoder," in Proceedings of the IEEE Workshop on Signal Processing Systems (SIPS), pp. 183-188, 2003.

[11]. J. R. Kim, and Y. S. Moon, "A robust wavelet-based digital watermarking using level-adaptive thresholding," in IEEE Proc. Int. Conf. Image Processing, Japan, pp. 226-230,1999.