Digital Image Watermark Key Extraction with Encryption and Decryption Scheme in MATLAB

Isha Garg
M.Tech Scholar
Department of C.S.E
Uttrakhand Technical
University, Dehradun India

Anchit Bijalwan
Assistant Professor and HOD
Department of C.S.E
Uttaranchal Institute Of
Technology, Dehradun India

ABSTRACT

Digital watermarking and image processing is a rapidly evolving area of research and development. One key challenge in the research problem is that we are still facing today is the development of truly robust, secure and transparent watermarking technique for different digital media including video, documentary text, graphics, images, and audio. In digital image processing, detection and extraction of text from a documentary image is found a challenging task, especially for inclined, vertical and circular text. The paper focuses on the MATLAB simulation of watermark encryption and decryption scheme using Discrete Wavelet Transform (DWT). The goal of the work is not to restrict access to the original image, but to ensure that embedded data remain recoverable. The research work is carried out on MATLAB 2012, image processing tool.

General Terms

HAAR DWT, MATLAB Simulation

Keywords

Digital Image Processing, Digital Watermarking, Discrete Wavelet Transform (DWT)

1. INTRODUCTION

The revolutions and advent in internet technology has resulted in many new opportunities for creating and delivering the contents in digital form. The applications of internet include electronic advertising, information sharing such as real-time video and audio [2, 4], Web publishing, digital repositories and libraries. In the all applications, an important issue arises, for the protection of the rights of all participants. It has been recognized and analyzed for quite some time that current laws of copyright protections are inadequate for dealing with digital data. The problem has developed an interest towards developing new copy deterrence and protection mechanisms. The effort towards that has been attracting increasing technological interest is completely based on digital watermarking techniques. Digital watermarking is the technique of embedding information into digital multimedia content such as the information, which is also called watermark used to extract or detect for a variety of purposes including copy control and prevention. Right now, digital watermarking is an active and leading area of research, for the future development. Commercialization of watermarking techniques [3, 4] is being deemed necessary to help some of the challenges, addressed by the rapid proliferation of digital contents or data.

Digital contents are possible to create, transmit, develop, replicate, and distribute in an effortless way, with the success of the internet. It is cost-effective and the promise of higher bandwidth and quality of service (QoS) for both wired and wireless networks, with digital recording and storage devices.

The protection and enforcement of intellectual property rights for digital media has become an important issue. In1998, Congress passed the Digital Millennium Copyright Act (DMCA) which makes it illegal to circumvent any technological measure that protects an owner’s intellectual property rights of digital content. Development of compression algorithms are done for multimedia data such as MPEG-2/4, JPEG standards and multimedia support. It has increased network data transmission speed to allow wide spread use of applications, which rely on digital data. Moreover, digital multimedia data are rapidly spreading everywhere and all types of networks, also permits the possibility of duplicating and manipulating the data. The reliability and originality of the transmitted data should be verifiable to keep on with the transmission of data over the internet. Hence, It is necessary that multimedia data should be protected and secured. One way to address this problem involves embedding an invisible data into the original data to mark ownership of them. Information hiding is very important and many techniques are existing which can be used into different categories such as convert channels, anonymity, steganography, and watermarking. Multilevel secured systems are using convert channels techniques, used to handle the properties of the communication channels in an unexpected and unforeseen way in order to transfer data through the medium without detection by anyone other than the entities operating the covert channel. The prevention the detection of an encrypted data is possible using Steganography, which has been protected by cryptography algorithms. Anonymity is a technique to find different ways to hide the meta contents of transmitted messages such as sender and the recipients. Digital watermarking has an extra requirement of robustness compared to steganography algorithms against possible attacks.

Watermarking requires [5] two operations, embedding the watermarks with the information and extraction. Watermark may be an image, plain text data, password, serial number or authentication key. According to the type of document, watermarking techniques can be divided into four categories; they are (i) text watermarking (ii) image watermarking (ii) audio watermarking and (iv) video marketing. Image watermarking can be classified both in spatial domain and frequency domain. Visible watermarks appear visible to a casual viewer on careful inspection. Primary images are embedded with the invisible fragile watermark technique in such a way that modification or manipulation of the image would destroy or alter the watermark. The alteration made to the pixel value is perceptually not noticeable and it is possible to recover with appropriate decoding. Human perception classified watermarking as robust and fragile. In image processing, the watermarking techniques are classified into three types, visible watermark, Invisible fragile watermark and Invisible robust watermark. All watermarking techniques are compatible with hardware, software or both together. There is a close relationship of watermarking and cryptography but watermarking is distinct from encryption. An original image is embedded with the information carrying the watermark. The watermarked image is stored and transmitted and then decoded by the receiver.

Cryptography helps to resemble the image so that it cannot be understood. Cryptographic [14] mechanism forms a foundation on network security [7], which help in implementation of security system based networks. There are encryption and decryption cryptographic algorithms. These algorithms suggest the ways by which it is possible to transfer secured data over networks [1].Encryption is the process of converting plain text or unhidden text to a cipher text or hidden text, to secure against thieves under key management policy [14]. In encryption, [10] the data is locked at one end by the sender with the help of key and routed over network. Decryption is the process to retrieve the same text from the cipher text at another end. In decryption, same data is received, when the receiver is breaks the encrypted data with the help of key. The encryption and decryption process is shown in fig. 1.

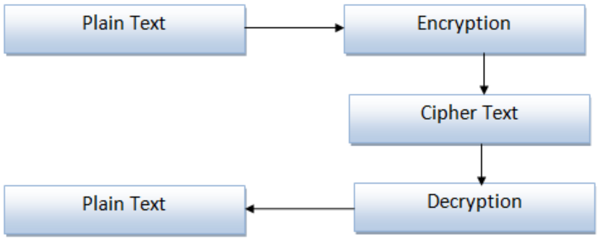


Fig.1 Encryption and decryption

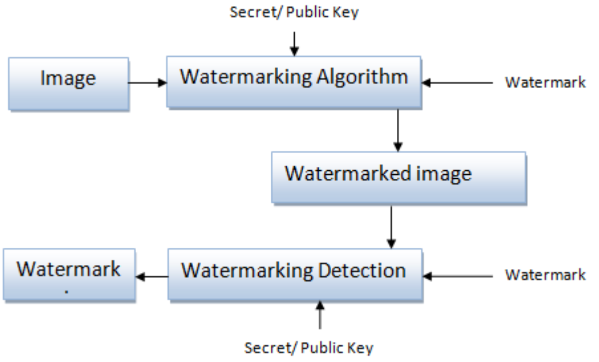


Fig. 2 Watermark embedding process and extraction process

A digital watermark could be used either source based or destination based. From the application point of view, source based watermarks are used for authentication or ownership identification. In this a unique watermark is identifying that the owner is introduced to all the parallel copies of a particular image being distributed and it also used to identify weather a received image has been tampered with. If the each distributed copy is getting a unique watermark, it could be a destination based watermark and it could be used to determine the buyer in case of illegal reselling. In real time, watermarking will solve the issues of source authentication. In the real time stream exchange, the parties involved to check the authenticity of the data received with the help of watermark extraction bits available in the embedded stream. This watermark can be used into the video stream at source, channel or at the receiver side. In the proposed system a simple video streaming authentication system is using watermarking at the source principle rather than at video delivery or at channel. The system is applicable for both unicast and multicasting application

2. TEXT EXTRACTION AND DWT

Recent advancement and research areas of image processing have much interest in content retrieval and derived in the perceptual and semantic content. Human perceptual includes color, shape pixel intensity and texture and semantic includes objects, events, interrupts and their relations. Contents of an image are described using texts, which are also easily and clearly describe the feature of an image. Since the text and characters data can be embedded in an image. Up to now it has been extracted by two basic techniques. These techniques are edge and connected component based technique. A text extraction system receives an input in the form of an image or a sequence of images. Text reorganization and extraction problem can be divided into the following parts. (i) Detection of text (ii) localization of text, (iii) tracking on text (iv)Extraction and enhancement of text, and (v) recognition of text. The meaning of text detection is to detect the text which is presences in image. In this, threshold values are needed for scene based change detection because the portion occupied by a text region relative to the entire image is usually small. It is based on the difference between two consecutive frames and then used this scene change information for text detection.

The methods of text localization are divided into two types: region and texture based. Regions defined methods use the properties of the color or gray scale in a text region or their differences with the corresponding properties of the background.

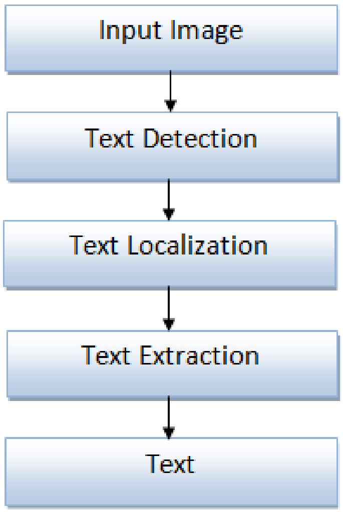


Fig. 3 Steps in text extraction

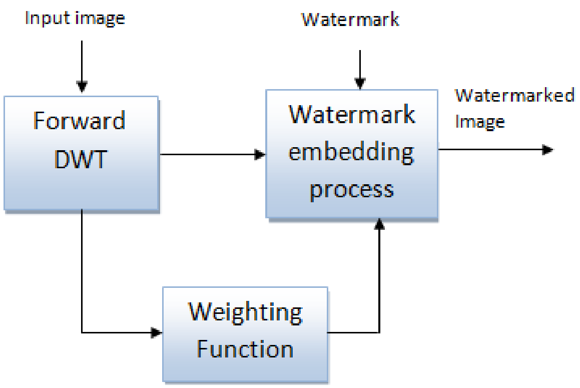


Fig. 4 Watermarking Scheme for key text extraction

In the watermarking scheme of input image, forward DWT is applied. In the watermark embedding process, the watermark is embedded with the weight function and watermarked image is gotten after applying encryption method at the input end of embedding image.

3. DISCRETE WAVELET TRANSFORM

The discrete wavelet transform (DWT) is a very useful tool for signal processing and image analysis especially in multi-resolution representation. In DWT signals are decomposed into different components in the frequency domain. 1-D DWT decomposes an input sequence into two components the average component and the detail component by calculations with a low-pass filter and a high-pass filter [9]. Two-dimensional discrete wavelet transform (2-D DWT) decomposes an input image into four sub-bands, one average component (LL) and three detail components (LH, HL,LH HH) as shown in fig. 5. In image processing, the multi-resolution of 2-D DWT has been employed to detect edges of an original image.

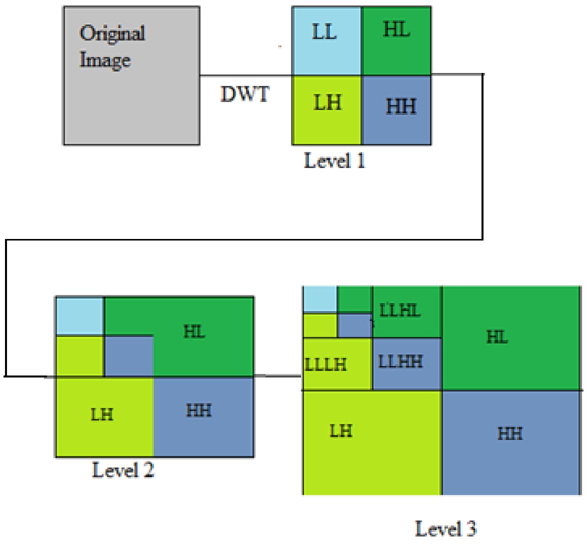


Fig.5. Decomposition of wavelet transforms

Haar Transform is a good method to transform the text from the colour images. A method of text extraction from images is proposed using the Haar Discrete Wavelet Transform. The multi-resolution decomposition approach in the two-dimensional image is demonstrated in fig. 5. After the first level of decomposition, it generates four sub-bands LL1, HL1, LH1, and HH1. Considering the input signal is an image, the LL1 sub-band can be considered as a 2:1 sub-sampled (both horizontally and vertically) version of image. The other three sub-bands HL1, LH1, and HH1 contain higher frequency detail information.

4. MATLAB IMAGE PROCESSING TOOL

Image Processing Toolbox provides a comprehensive set of reference-standard algorithms, functions, and apps for image processing, analysis, visualization, and algorithm development. You can perform image analysis, image segmentation, image enhancement, noise reduction, geometric transformations, and image registration. Many toolbox functions support multicore processors, GPUs, and C-code generation. Image Processing Toolbox supports a diverse set of image types, including high dynamic range, gigapixel resolution, embedded ICC profile, and tomographic. Visualization functions and apps let you explore images and videos, examine a region of pixels, adjust color and contrast, create contours or histograms, and manipulate regions of interest (ROIs). The toolbox supports workflows for processing, displaying, and navigating large images.

Key Features

- Image analysis, including segmentation, morphology, statistics, and measurement
- Image enhancement, filtering, and deblurring
- Geometric transformations and intensity-based image registration methods
- Image transforms, including FFT, DCT, Radon, and fan-beam projection
- Large image workflows, including block processing, tiling, and multiresolution display
- Visualization apps, including Image Viewer and Video Viewer
- Multicore- and GPU-enabled functions and C-code generation support.

A digital image can be synthesized from a micrograph of various cell organelles by assigning a light intensity value to each cell organelle [11]. The sensor signal is “digitized” converted to an array of numerical values, in which each value represents the light intensity of a small area of the cell. The discretized values of an image are called picture elements, or “pixels,” and are stored in computer memory as a digital image [1] [11]. A typical size for a digital image is an array of 512 by 512 pixels. Each pixel of image has value in the range of 0 to 255. The digital image can be processed by with the help of a computer to achieve the desired result.

5. MATLAB RESULTS

The MATLAB simulation is carried out in MATLAB 2012 with the help of MATLAB image processing tool. Fig. 6 to 9 shows the input image with key and extracted watermark as output. The images are extracted from the MATLAB software directly. The results are analyzed in a single window and extracted watermark is shown in another window.

The proposed method is also used to decompose the blocks including multi-line texts into single line text. According to the experimental results, the proposed method is proved to be efficient for extracting the watermark text regions from the image. In the fig. 6, Original image is of vehicle plate which has the number MX55NOB. The encrypted watermark is shown in fig. 7, which is *copyright@author India Do't. Copy*. After encryption watermark fig. 8 is approximately same because watermark is embedded with the image and under invisible watermarking technique.After MATLAB simulation and watermark extraction/ decryption , the same watermark key is extracted *copyright@author India Do't. Copy,* as shown in fig.9.

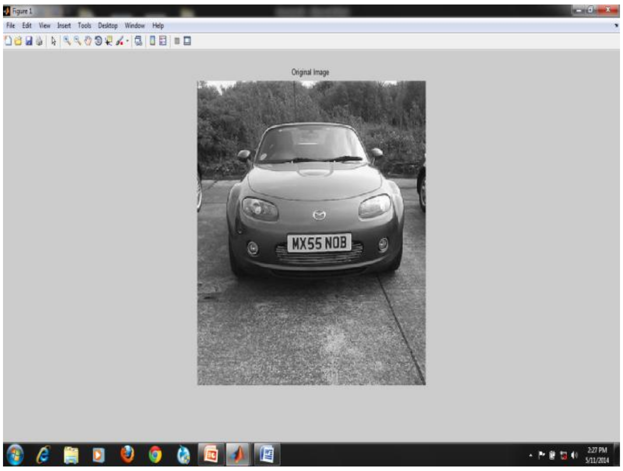
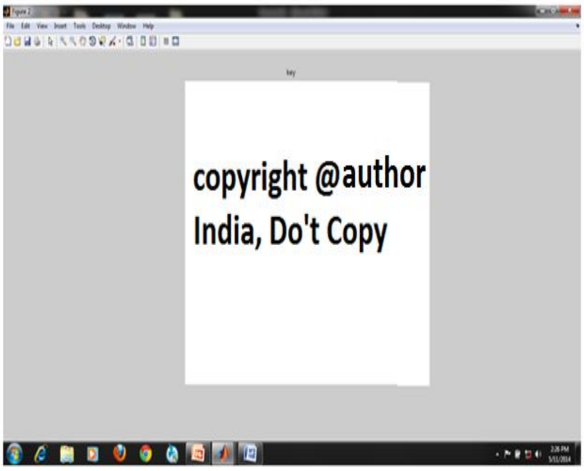


Fig. 6 Original Image



copyright @author
India, Do't Copy

Fig. 7 Watermarked key

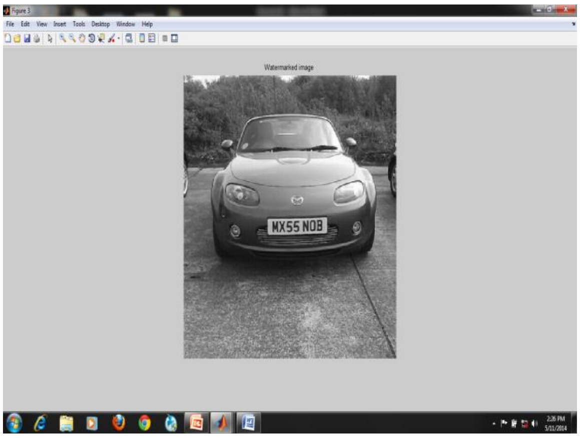


Fig. 8 Image with embedded watermark

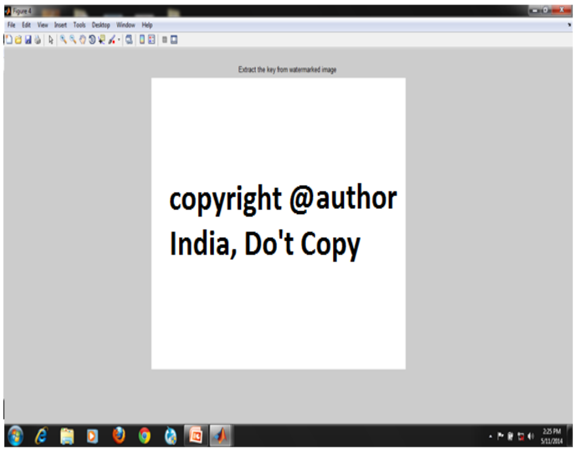


Figure 4
File Edit View Insert Tools Desktop Window Help
Extract the key from watermarked image

copyright @author
India, Do't Copy

Fig. 9 Extracted watermark

6. CONCLUSION

The watermark key text extraction on the colour images using mathematical morphology and Haar DWT is done successfully with the concept of encryption and decryption. Applications of text extraction are huge including the making of digital copies of the ancient scripture to everyday life bills etc. It may be required to be of digital form. Digital watermarks provide an efficient cost effective means of a digital image which may be used for copyright protection. In watermarking technology, the watermark key is unique and exhibits a one-to-one correspondence with every watermark. The key is private and known to only authorized parties, eliminating the possibility of illegal usage of digital content. The watermarking scheme is simulated successfully in MATLAB. The work is carried out for images. In the future work, further research can explore with the techniques to recognize the special characters from colour images. The limitation of the watermarking algorithms implemented is that the processing needs to be done pixel-by-pixel. In future development, we are aiming to investigate block-by-block processing. Digital watermarking find applications in the defense sector where it is must to transmit data secretly.

7. REFERENCES

[1] A. Tognetti, F. Lorussi, R. Bartalesi, S. Quaglini, M. Tesconi, G. Zupone, and D. De Rossi, "Wearable kinesthetic system for capturing and classifying upper limb gesture in post-stroke rehabilitation," *J. Neuroeng. Rehabil.*, vol. 2, no. 1, p. 8, Mar. 2005.

[2] A. M. Eskicioglu and E. J. Delp, "An Overview of Multimedia Content Protection in Consumer Electronics Devices," Elsevier Signal Processing: Image Communication, vol. 16, pp. 681–699, 2001.

[3] ArnabSinha and SumanaGupta,"A Fast Nonparametric Non causal MRF-Based Texture Synthesis Scheme Using a Novel FKDE Algorithm" IEEE Transactions on Image Processing, No.3, March 2010.

[4] D. Dhanasekaran and K. BoopathyBagan (2004) "HIGH SPEED PIPELINED ARCHITECTURE FOR ADAPTIVE MEDIAN FILTER," European Journal of Scientific Research ISSN 1450-216X Vol.29 No.4, pp. 454-460.

[5] JulindaGllavata, Ralph Ewerth and Bernd Freisleben, A Robust algorithm for Text detection in images, Proceedings of the 3rd international symposium on Image and Signal Processing and Analysis, 2003.

[6] J.D. Foley, A. van Dam, S.K. Feiner and J.F. Hughes, *Computer Graphics, Principles and Practice*, Addison-Wesley, Reading, 1990

[7] M. Hussain and M. Hussain, “Information Hiding Using Edge Boundaries of Objects”, International Journal of Security and its Applications, http://www.sersc.org/journals/IJSIA/vol5_ no3_ 2011/1.pdf, vol. 5, no. 3, (2011), pp. 1-10.

[8] Mohammad Nuruzzaman, “Digital Image Fundamentals in MATlAB,”Author House 08/23/05, ISBN 1-4208-6965-5 (sc), 2005.

[9] M. S. Hsieh, D. C. Tseng, and Y. H. Huang, Hiding Digital Watermarks using Multiresolution Wavelet Transform, IEEE Trans. on Industrial Electronics 48 (2006), no. 5, 875–882.

[10] Sunil Kumar, Rajat Gupta, NitinKhanna, *Student Member, IEEE*, SantanuChaudhury, and Shiv Dutt Joshi (2007) “Text Extraction and Document Image [23] Segmentation Using Matched Wavelets and MRF Model” IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 16, NO. 8, pp 2117-2129.

[11] T. Barbu, 2011, “An Automatic Face Detection System for RGB images”, in *Int. J. of Computers, Communications & Control ISSN*, 1841-9836, *E-ISSN*, 1841-9844, Vol No.1, pp.21-32

[12] Victor Wu, RaghavanManmatha, and Edward M.Riseman, Text Finder: An Automatic System to Detect and Recognize Text in Images, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 21, No. 11, November 1999.