International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 02 Issue: 02 | May-2015 www.irjet.net p-ISSN: 2395-0072

Digital Watermarking Encryption and Decryption Using DWT

Arisudan Tiwari[1], Anoopa Arya[2], Shubham Shukla[3]

[1]*M.Tech Scholar, Department of Computer Science & Engineering, Maharishi Ved Vyas Engineering College Jagadhri, Yamuna Nagar, India*

[2]*Assistant Professor, Department of Computer Science & Engineering, Maharishi Ved Vyas Engineering College Jagadhri, Yamuna Nagar, India*

[3]*Assistant Professor, Department of Computer Science & Engineering, Neelkanth Institute of Technology, Meerut, India*

Abstract: *Watermarking is a technique in which pattern bits are inserted into digital image; video or audio files have copyright information such as rights authors etc. The aim of digital watermarks is to provide secured or copyright protection for intellectual property that's in digital format. Digital watermarks are completely invisible and inaudible in case of audio clips unlike printed watermarks. Apart from it, the actual bits representing the watermark must be scattered throughout the file in such a way that they cannot be identified and manipulated. The goal of watermarking is not to restrict access to the original image but to ensure the embedded data remain recoverable. The paper focuses on the MATLAB simulation of watermark decoding scheme using Discrete Wavelet Transform (DWT). The work is carried out on MATLAB 13.0, image processing tool.*

Keywords: Discrete Wavelet Transform (DWT), Matrix Laboratory, Digital Watermarking

1. Introduction

Owing to the usage of Internet, concerns about protecting and enforcing intellectual property (IP) rights of the digital content are mounting. Unauthorized replication and manipulation of digital content is relatively easy and can be achieved with inexpensive tools. Digital rights management (DRM) systems [1], [2] address issues related to ownership rights of digital content. Various aspects of content management–namely, content identification, storage, representation, and distribution and IP rights management are highlighted in DRM. Although unauthorized access of digital content is being prevented by implementing encryption technologies, these approaches do not prevent an authorized user from illegally replicating the decrypted content. Digital watermarking is one of the key technologies that can be used in DRM systems for establishing ownership rights, tracking usage, ensuring authorized access, preventing illegal replication, and facilitating content authentication. Therefore, a two layer protection mechanism utilizing both watermarking and encryption is needed to build effective DRM systems that can address IP rights a copyright issue [3].

Watermarking and cryptography are closely related but watermarking is distinct from encryption. In the digital watermarking system, information carrying the watermark is embedded in an original image. The watermarked image is transmitted or stored and then decoded to be resolved by the receiver. Cryptography scrambles the image, so that it cannot be understood. Internet based multimedia technologies such as images, video and audio require network security to create, transmit and distribute the data over long distance. There are three basics to protect the data over internet namely, cryptography Steganography and watermarking [1]. In cryptography we can transmit and receive secured text and image using encryption and decryption technique. Steganography is the technique to hide and extract the information using a carrier signal. The third one, watermarking is a technique for hiding proprietary information in the perceptual data. Watermarking involves the content authentication, copyright protection, detection of duplication and alteration. In the original message watermarks are used to protect the data and at the receiving end these watermarks are extracted. So watermarks are used with the secret information to protect it.

Watermarking requires 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.

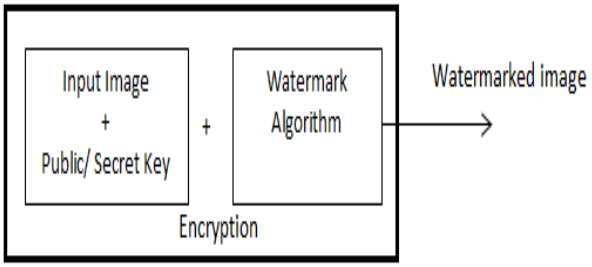

Fig. 1 Watermark embedding process

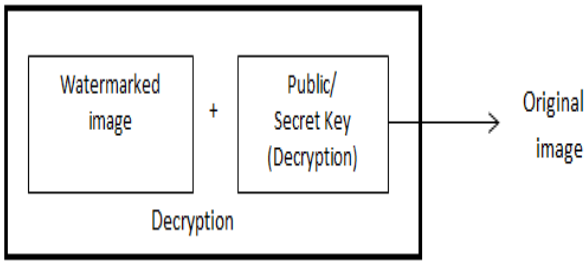

Fig. 2 Watermark Decryption process

The success of the Internet, cost-effective and popular digital recording and storage devices, and the promise of higher bandwidth and quality of service (QoS) for both wired and wireless networks has made it possible to create, replicate, transmit, and distribute digital contents in an effortless way. 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 for multimedia data such as MPEG-2/4 and JPEG standards, and increase in the network data transmission speed have allowed wide spread use of applications, which rely on digital data. In other words, digital multimedia data are rapidly spreading everywhere. On the other hand, this situation has brought about the possibility of duplicating and/or manipulating the data. To keep on with the transmission of data over the internet the reliability and originality of the transmitted data should be verifiable. 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. There are many techniques for information hiding, which can be divided into different categories such as convert channels, steganography, anonymity, and watermarking. Convert channels techniques were defined in the context of multilevel secure systems. Convert channels usually handle 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. Steganography is about preventing the detection of an encrypted data, which has been protected by cryptography algorithms. Anonymity is a technique to find the ways to hide the meta content of transmitted messages such as sender and the recipients. Digital watermarking has an extra requirement of robustness compared to steganography algorithms against possible attacks. It should be also noted that watermarking is not intended for protecting of the content of a message, and hence it is different from cryptography.

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. Techniques and Algorithm

There are different techniques that can be used to embed the watermark, but since using the spatial domain gives us fragile watermarks that are not robust against the attacks, we decided to work on the frequency domain because we are searching for watermarking algorithms that are robust against different kinds of attacks such the Geometrical and Removal attacks, without affecting the quality of the watermarked image, so we were trying to solve the conflict between robustness and imperceptibility. Fig.3 shows the sequence of the techniques we used in our algorithm.

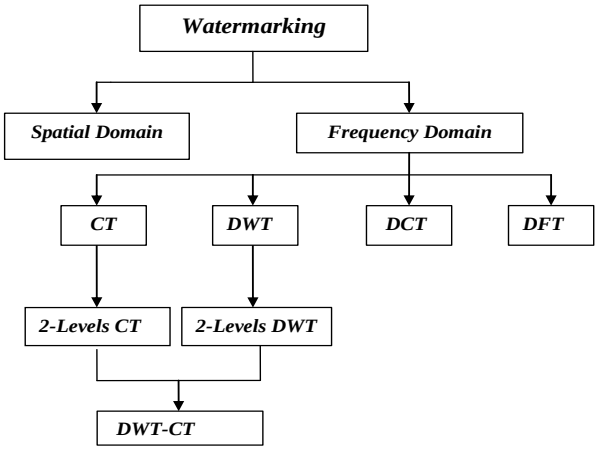

Fig.3 watermarking techniques

A new image watermarking algorithm will be presented by combining DWT and CT to develop a blind image watermarking algorithm to provide better imperceptibility and higher robustness against variety of attacks. First, we applied a 2-level DWT to the image by choosing mid-mid sub-band. The selection to the mid-mid sub-band shored better results in imperceptibility. Second, we applied CT to the chosen sub-band to study their effects.

The main reason of combing DWT and CT is to minimize the drawbacks of each of them separately. Most researchers in the field of digital watermarking focuses on using DWT, due to its excellent spatial localization and multi-resolution properties, which are similar to the theoretical models of human visual system. However, there are two drawbacks associated with DWT. First, it lacks shift invariance, which means small shift in input signal that can cause big changes in the energy distribution of the wavelet coefficients. The discrete wavelet transform 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 figure 4. In image processing, the multi-resolution of 2-D DWT has been employed to detect edges of an original image

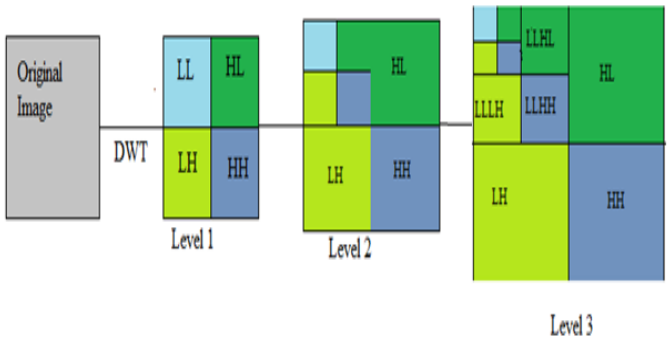

Fig. 4 Decomposition of wavelet transforms

The two-dimensional extension of DWT is essential for transformation of two-dimensional signals, such as a digital image. A two-dimensional digital signal can be represented by a two-dimensional array $\mathbf{X}[M,N]$ with M rows and N columns, where M and N are nonnegative integers of 2D image array. The simple approach for two-dimensional implementation of the DWT is to perform the one-dimensional DWT row-wise to produce an intermediate result and then perform the same one-dimensional DWT column-wise on this intermediate result to produce the final result. This is shown in Fig. 5.. This is possible because the two-dimensional scaling functions can be expressed as separable functions which is the product of two-dimensional scaling function such as $\Phi_2(x,y) = \Phi_1(x)\Phi_1(y)$. The same is true for the wavelet function $\Psi(x,y)$as well. Applying the one-dimensional transform in each row of image, two sub-bands are produced in each row. When the low-frequency sub-bands of all the rows (L) are put together, it looks like a thin version (of size $\mathrm{M} \times \frac{\mathrm{N}}{2}$of the input signal as shown in Fig. 5.7(a). Similarly put together the high-frequency sub-

bands of all the rows to produce the H sub-band of size $M = \frac{N}{2}$, which contains mainly the high-frequency information around discontinuities (edges in an image) in the input signal. So that applying a one-dimensional DWT column-wise on these L and H sub-bands (intermediate result), four sub-bands LL, LH, HL, and HH of size $\frac{M}{2} \times \frac{N}{2}$ are generated as shown in Fig.5 LL is a coarser version of the original input signal. LH, HL, and HH are the high frequency sub-band containing the detail information of the image. It is also possible to apply one-dimensional DWT column-wise first and then row-wise to achieve the same result. Fig..5 comprehends the idea describe above.

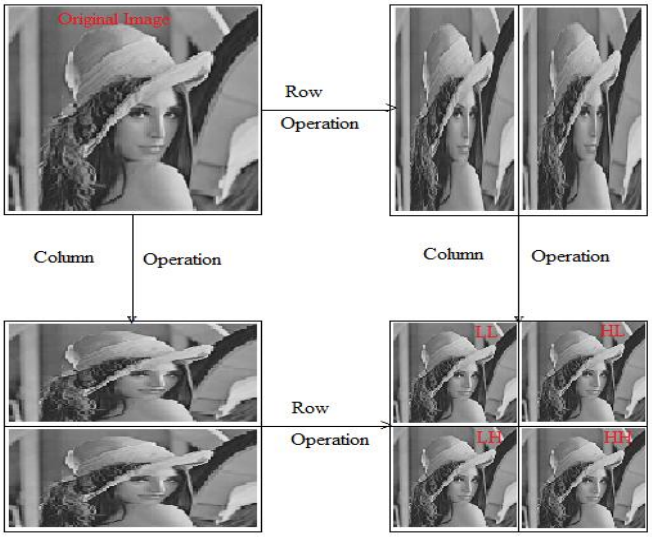

Fig. 5 Extension of DWT in two - dimensional signals

The multi-resolution decomposition approach in the two-dimensional signal is demonstrated in Fig.5. After the first level of decomposition, it generates four sub-bands LL1, HL1, LH1, and HH1 as shown in Fig. 5. 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. These spatially oriented (horizontal, vertical or diagonal) sub-bands mostly contain information of local discontinuities in the image and the bulk of the energy in each of these three sub-bands is concentrated in the vicinity of areas corresponding to edge activities in the original image.

3. 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 multi core processors, GPUs, and C-code generation. Image Processing Toolbox supports a diverse set of image types, including high dynamic range, giga-pixel 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 enhancement, filtering, and deblurring
- Image analysis, including segmentation, morphology, statistics, and measurement
- Image transforms, including FFT, DCT, Radon, and fan-beam projection
- Geometric transformations and intensity-based image registration methods
- 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.

4. MATLAB Simulation Results

The MATLAB simulation is carried out in MATLAB 2013 with the help of MATLAB image processing tool. Figure 6 to 7 shows the input image with key and extracted watermark as output. The images are extracted from the MATLAB software directly.

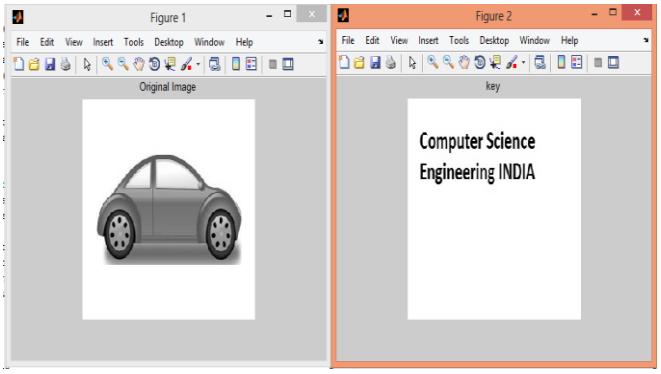

Fig. 6(a) Original Image (b) Key

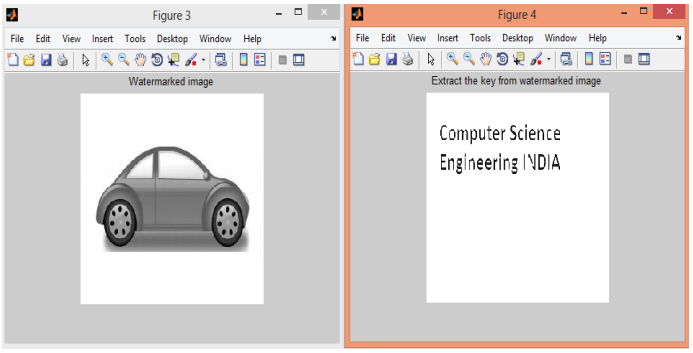

Fig.6 (c) Watermarked image (d) extracted watermark

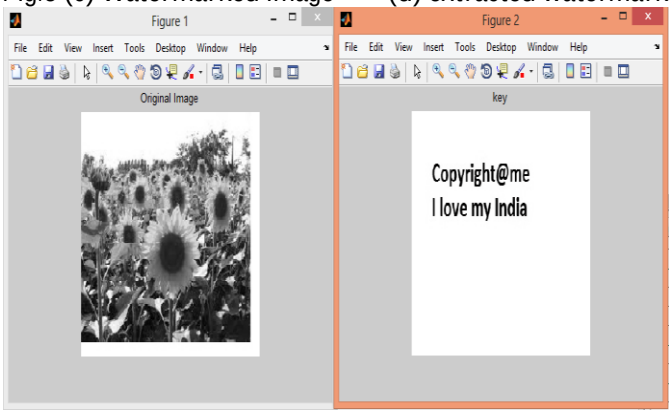

Fig. 7(a) Original Image (b) Key

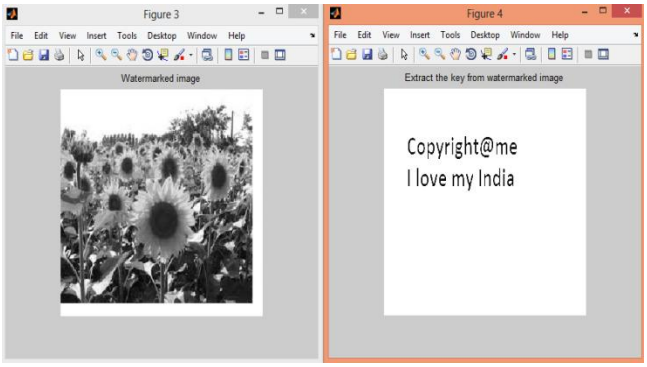

Fig.7 (c) Watermarked image (d) extracted watermark

5. CONCLUSIONS

Digital watermarking is one of the key technologies that can be used in Digital Rights management systems for establishing ownership rights, tracking usage, ensuring authorized access, preventing illegal replication, and facilitating content authentication. Therefore, a two layer protection mechanism utilizing both watermarking and encryption is needed to build effective DRM systems that can address IP rights a copyright issue, 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. The limitation of the watermarking algorithms implemented is that the processing needs to be done pixel-by-pixel. In future, we are aiming to investigate block-by-block processing.

REFERENCES

[1] A. Kejariwal, S. Gupta, A. Nicolau, N. D. Dutt, and R. Gupta, Energy Efficient Watermarking on Mobile Devices Using Proxy-Based Partitioning, IEEE Trans. On Very Large Scale Integration (VLSI) Systems 14 (2006), no. 6, 625–636.

[2] A. Shahbahrami and B. Juurlink, A Comparison of Two SIMD Implementations of the 2D Discrete Wavelet Transform, Proc. 18th Annual Workshop on Circuits, Systems and Signal Processing (ProRISC2007), November 2007.

[3] 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.

[4] A. Singh, S. Tiwari and S. Kumar Singh, "Face Tampering Detection from Single Face Image using Gradient Method", International Journal of Security and its Applications, http://www.sersc.org/journals/IJSIA/vol7_no1_2013/3.pdf, vol. 7, no. 1, (2013)

[5] Chan-Il Woo and Seung-Dae Lee "Digital Watermarking for Image Tamper Detection using Block-Wise Technique" International Journal of Smart Home Vol.7, No.5 (2013), pp(115-124).

[6] Dr. Neeraj Bhargava, Manish Mathuria "Color Image Digital Watermarking" Springer Proceeding of International Conference ICERECT Series: Lecture Notess in Electrical Engineering, Vol. 248, in press, 2012.

[7] Kesavan Gopal, Dr. M. Madhavi Latha, "Watermarking of Digital Video Stream for Source Authentication, IJCSI International Journal of Computer Science Issues, Vol. 7,

Issue 4, No 1, July 2010 ISSN (Online): 1694-0784 ISSN (Print) pp(18-26)

[8] Kanchan H. Wagh, Pravin K. Dakhole, Vinod G. Adhau.: Design & Implementation of JPEG2000 Encoder using VHDL. Proceedings of the World Congress on Engineering 2008 Vol I, WCE 2008, , London, U.K July 2 - 4, 2008.,

[9] 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.

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

[11] 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.

[12] Namrata Vaswani, Yogesh Rathi, Anthony Yezzi, and Allen Tannenbaum "Deform PF-MT: Particle Filter With Mode Tracker for Tracking Nonaffine Contour Deformations" IEEE Transactions On Image Processing, VOL. 19 ,NO .4, April 2010 page (841 - 857)

[13] Y. C. Fan, L. D. Van, C. M. Huang, and H. W. Tsao, "Hardware-Efficient Architecture Design of Wavelet-based Adaptive Visible Watermarking," in Proceedings of 9th IEEE International Symposium on Consumer Electronics, 2005, pp. 399–403.

[14] Yang Qianli and Cai Yanhong," A Digital Image Watermarking Algorithm Based on Discrete Wavelet Transform and Discrete Cosine Transform," IEEE international symposium on information technology in Medicine and Education, 2012.

[15] Zhong, Yu.,Karu, K., and Jain, A.K. (1995), "Locating text in complex color images". Proceedings of the Third International Conference on Document Analysis and Recognition, 1, 14-16: 146-149.

BIOGRAPHIES

Arisudan Tiwari, M. Tech Scholar, Department of Computer Science & Engineering, Maharishi Ved Vyas Engineering College , Jagadhri Yamuna Nagar, India. I Completed my B.Tech (Information Technology) in 2011. I am having good Interest in image processing and analysis.

Shubham Shukla working as a Assistant Professor in the Department of Computer Science & Engineering, Neelkanth Institute of Technology, Meerut, India. He has good knowledge in Digital Image Processing and published various papers.

