TELEMATIQUE Volume 22 Issue 1, 2023
ISSN: 1856-4194 2909– 2916

Dynamic Image Watermarking using Hybrid DWT Compression and Decompression Techniques

Dr.Shaik Javed Parvez[1], Mannepuli Srujana[2], Dr. N. Venkatesh[3], Syed Abdul Haq[4]

[1]Associate Professor, Department of CSE - AI & ML, Malla Reddy Engineering College (A), Maisammaguda,Hyderabad,Telangana-500100.
[2]Assistant Professor, Department of Computer Science and Engineering, Malla Reddy Engineering College (A), Maisammaguda,Hyderabad,Telangana-500100.
[3]Asst. Professor, School of CS&AI, S R University, Warangal-506371
[4]Assistant Professor, Department of CSE -DS, Malla Reddy Engineering College (A), Maisammaguda, Hyderabad, Telangana-500100

Email: [1]shaikjavedparvez@gmail.com, [2]srujanamannepuli@gmail.com, [3]naramulavenkatesh@gmail.com, [4]abdulhaq007@gmail.com

Received 04/11/2023; **Accepted** 08/12/2023

Abstract

This study presents an innovative information hiding approach that utilizes lifting schemes to seamlessly embed data in color images. The efficacy of this technique lies in achieving successful extraction of concealed data with a high level of integrity. Current preferences favor the use of digital image files as cover files for concealing additional digital content containing secret messages or information. Different digital media streams can function as cover streams for secret messages, with watermarking emerging as a prominent technique for copyright protection. The paper introduces a novel method for encoding secret messages using wavelets. The wavelet technique dissects the stream into high and low-frequency components, referred to as details and trends.

Keywords: FPGA, LSB, Watermarking, Hybrid, Compression technique

1. INTRODUCTION

Watermarking represents a sophisticated method of covert communication, entailing the concealment of information within data, reminiscent of steganography or "covered writing." The exponential growth in the utilization and distribution of digital multimedia data in recent years underscores the critical need to safeguard such content, spanning images, videos, audio, and text, each vulnerable to seamless copying and efficient distribution. However, this widespread accessibility has concurrently given rise to challenges related to copyright infringement, prompting the development of innovative approaches for the protection of digital data.

Within the array of techniques for safeguarding digital multimedia data, watermarking emerges as a prominent player. It involves the embedding of concealed information within multimedia elements, such as images, videos, audio, or text. Notably, there are two primary categories of watermarking techniques: visible and invisible. Visible watermarking incorporates discernible semi-transparent text or images overlaid onto original content, often employed for logos or maps. In contrast, invisible watermarking entails the embedding of imperceptible information in an image, detectable solely by electronic devices or specialized software, enhancing security and resilience against transformations.

A watermarking system comprises three essential components: the cover objects (which conceals the secret message), the secret message itself, and the stego-object (the cover object with the embedded message). Given the ubiquity of digital images, they have become the preferred cover objects for watermarking. Digital images are represented as 2-D matrices of color intensities at each pixel, with gray-scale images using 8 bits and colored ones utilizing 24 bits in models like RGB. Various techniques exist to conceal information within cover images, categorized into spatial domain and transform domain methods. Spatial domain techniques manipulate pixel bit values directly, with the Least Significant Bit (LSB) standing out as a prominent approach.

Conversely, transform domain techniques embed messages in the frequency domain, proving more robust against attacks like compression and filtering. While transform domain methods offer higher security and peak signal-to-noise ratio (PSNR), they hide messages in significant areas, enhancing resistance against diverse attacks. Spatial domain techniques, though simpler and easily implementable, tend to be more detectable and sensitive to noise. In contrast, frequency-based watermarking methods provide heightened security and robustness against various attacks. The article also delves into specific implementations, including FPGA implementations of spatial-domain steganography designs and watermarking techniques employing wavelets. Notably, the approach discussed involves the implementation of the LSB technique to strike a balance between secret data size and system imperceptibility.

The other sectors of the suggested paper have been given in the following way, section 2 demonstrates the related work, section 3 describes the suggested approach and the conclusion of the paper has been presented in section 4.

2. Related work

The authors of [1, 2] suggested an approach, in which the authors describe various watermarking and steganography approaches to hide the information. However the methods not applicable to real time application, because the suggested approach is having complex mathematical design ad introduces a delay. In [3, 4} the authors describes an overview and comparative analysis of watermarking and steganography. Walia [5] et al described an approach to analyze LSB and DCT. Hernández et al [6] proposed an approach using StenographicContext Technique with an application of FPGA hardware; however the arrangement is too complex to apply on real time applications. Prasad et al [7] provided High Secure Image Watermarkingin BCBS using DCT and Fractal Compression, but the mathematical design introduces an unacceptable delay and may not be the optimum solution in real time applications. The authors of [8, 9] suggested a watermarking image processing technique using normalized circular image in DWTand simple wavelet transform technique, but didn’t obtain the optimum results to apply on real time applications. Pavan, A.C. and Somashekara presented a paper in which the authors described the

issues and challenges of watermarking in image processing. Saber, Mohamed, et al [11] proposed an approach in which the researchers apply watermarking to medical applications.
Imperceptible digital watermarking technology [12, 13] is a crucial tool for enhancing PDF fortification [14]. This expertise contains the supplement of hidden material into PDF archives, version it untraceable by humanoid awareness systems. Only dedicated watermark indicators have the competence to recognize or excerpt the unseen evidence, contribution various applications such as proclaiming tenure of PDF files through watermarks, outlining the illegitimate spreading of delicate pamphlets using impressions, and confirming the article's origin from additional gathering through verification [15]. Given that PDF is a file arrangement, the digital watermark working in PDFs can be categorized as a file watermark. Even with current progressions, the field of PDF file watermarking algorithms is silent in its initial stages, with researchers actively exploring and proposing various techniques in recent years

3. PROPOSED APPROACH

3.1.LSB BASED IMAGE WATERMARKING

The Least Significant Bit (LSB) refers to the lowest significant bit in the byte value of an image pixel. LSB-based image watermarking involves embedding a secret message in the least significant bits of pixel values in the cover image (CVR). To illustrate the LSB technique, consider the following example with two pixel values in the CVR:

Original Pixel Values:

(0000 1010 0011 0010 0111 0100)
(1111 0101 1100 0011 1100 0111)

Assuming secret bits: 1011012, after embedding, the resulting pixel values become:
Modified Pixel Values:

(0000 1011 0011 0010 0111 0101)
(1111 0101 1100 0010 1100 0111)

The underlined bits indicate the modifications from their original values, with only three bits altered in the cover image. On average, approximately half of the bits in the cover image undergo modification during the secret image embedding. The presented LSB method limits the size of the secret data to one-eighth of the size of the CVR. Additionally, LSB watermarking can extend to embedding secret information in the least n-bits, thereby increasing the capacity to n/8 of the CVR size.

However, an increase in n leads to distortion in the stego-image. To demonstrate the impact of the value of n on the stego-image, we conducted several experimental runs on a test image (Figure 1a). Each run involved embedding random data in the n least significant bits, where $1 \leq n \leq 7$. It is essential to introduce methods for measuring the quality and distortion in images for a comprehensive evaluation of the watermarking process.

3.1.1. The Discrete Wavelet Transform

The Wavelet Series is essentially a sampled version of the Continuous Wavelet Transform (CWT), and its computation can be demanding in terms of resources, particularly dependent on the desired resolution. As a response to this computational challenge, the Discrete Wavelet Transform (DWT), rooted in sub-band coding principles, has emerged as a more efficient alternative. This method not only reduces computation time but also minimizes the overall resource requirements. The inception of DWT can be traced back to 1976 when techniques for decomposing discrete time signals were initially introduced [5]. Notably, this approach shares similarity with sub-band coding, a concept initially explored in the domain of speech signal coding. A crucial milestone in the evolution of this technique was reached in 1983 with the introduction of pyramidal coding, which is akin to sub-band coding. Over time, continuous refinements and enhancements to these coding schemes have paved the way for the development of efficient multi-resolution analysis techniques.

In the Continuous Wavelet Transform (CWT), signals undergo analysis via a sequence of fundamental functions connected through uncomplicated scaling and translation. Conversely, the Discrete Wavelet Transform (DWT) accomplishes the representation of a digital signal in the time-scale domain by employing digital filtering techniques. This involves passing the signal through filters with defined cutoff frequencies corresponding to different scales. The use of these filters facilitates a comprehensive examination of the signal's characteristics across various scales, offering a detailed perspective on its unique feature

3.1.2. Multi-Resolution Analysis using Filter Banks

Filters represent a fundamental component in signal processing, widely employed for various applications. The realization of wavelets involves the iterative application of filters with rescaling. The resolution of a signal, indicating the level of detail within it, is influenced by filtering operations, while scale is determined through up sampling and down sampling (sub sampling) operations

The Discrete Wavelet Transform (DWT) is computed through successive low-pass and high-pass filtering of the discrete time-domain signal, as depicted in Figure 2.2. This process, known as the Mallat algorithm or Mallat-tree decomposition, is significant for its ability to connect continuous-time multi-resolution to discrete-time filters. In the figure, the signal is represented by the sequence x[n], where n is an integer. The low-pass filter is denoted by G0, and the high-pass filter is denoted by H0. At each level, the high-pass filter generates detail information, denoted as d[n], while the low-pass filter, associated with the scaling function, produces coarse approximations, denoted as a[n]

This paper introduces an invisible watermarking design utilizing the Least Significant Bit (LSB) algorithm. The paper focuses on creating and implementing watermarking specifically tailored for the Spartan-3 FPGA kit. The coding aspect of the project is executed in System C, and the FPGA synthesis and logic simulation are carried out using Xilinx ISE Design Suite 10.1.

The Spartan-3 Starter Board, chosen for this project, serves as a robust, self-contained development platform catering to designs aimed at the Spartan-3 FPGA by Xilinx. With features such as a 200K or 1000K gate Spartan-3, on-board I/O devices, and 1MB fast asynchronous SRAM, it offers an ideal environment for experimenting with a spectrum of designs—from simple logic circuits to embedded processor cores. Notably, the board includes a Platform Flash JTAG-programmable ROM, ensuring that designs can be easily rendered non-volatile.

The compatibility of the Spartan-3 Starter Board extends to all versions of the Xilinx ISE tools, including the free Web Pack. Figure 1 illustrates the distinctive features of the Spartan-3 FPGA, encapsulating the technological essence of this innovative platform

a) Xilinx Spartan-3 FPGA w/ twelve 18-bit multipliers, 216Kbits of block RAM, and up to 500MHz internal clock speeds
b) -200 and -1000 versions available
c) On-board 2Mbit Platform Flash (XCF02S)
d) 8 slide switches, 4 pushbuttons, 9 LEDs, and 4 digit seven-segment display
e) Serial port, VGA port, and PS/2 mouse /key board port
f) Three 40-pin expansion connectors
g) Three high-current voltage regulators (3.3V, 2.5V, and 1.2V)
h) 1Mbyte on-board 10ns SRAM (256Kb x 32)

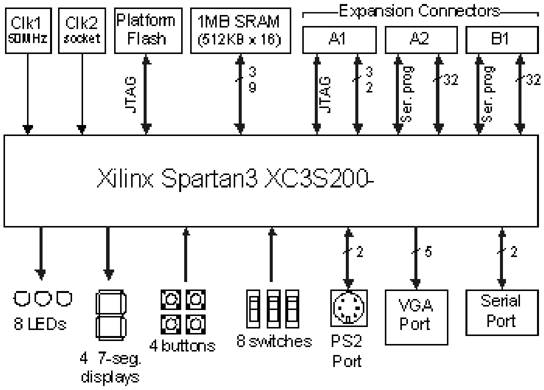


Fig1: spartarn3 functional block diagram

3.1.3. SYSTEM DESCRIPTION

The fundamental components of the system encompass the Watermarking unit, MicroBlaze processor, SRAM, and UART & JTAG interface. The integration of both the watermarking block and MicroBlaze processor is realized within the FPGA chip Spartan 3EDK. The watermarking block employs the Least Significant Bit (LSB) method to conceal secret information within the Cover Image (CVR) using a hybrid 2-bit and 3-bit LSB watermarking technique known as 2/3-LSB. Each CVR pixel is composed of three bytes, with a single byte of secret information concealed within these three bytes of a CVR pixel, as illustrated in Figure 2. This approach yields several advantages.

i) The mapping of one secret byte to one CVR pixel significantly streamlines memory access, simplifying hardware design and reducing both design area and power consumption.
j) The secret size is reduced

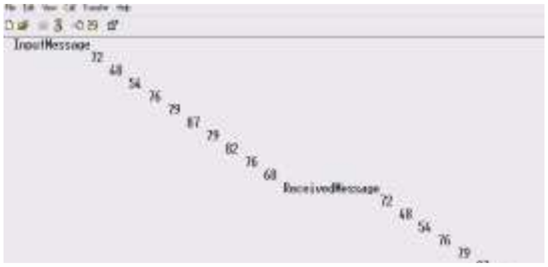
Fig 2: GUI window to create header file

The LSB block receives the three bytes of CVR and one byte of the secret, combines them, and then returns them to the processor. The watermarking block is implemented in the System C language

In the paper, we initiate by creating a header file for the images using MATLAB. Within MATLAB, the header files are generated through a GUI window. These header files, serving as supporting files, are then used to fuse two images using the Discrete Wavelet Transform (DWT) technique.

3.1.4. Results

This section presents the performance analysis of the proposed image watermarking technique based on the Least Significant Bit (LSB). The resultant figures (see figures 3, 4, 5 and 6) illustrate the application of invisible watermarking employing DWT compression.



```
InputMessage
            72
              48
                54
                  76
                    79
                      87
                        79
                          82
                            76
                              68
                                ReceivedMessage
                                               72
                                                 48
                                                   54
                                                     76
                                                       79
```

Fig 4: input image

Fig 5: Watermarking image

Fig6: Output image

4. CONCLUSION

This paper introduces an image watermarking technique based on the Least Significant Bit (LSB). The implementation involves invisible watermarking through the utilization of the LSB algorithm on FPGA. The results are subsequently validated by applying discrete wavelet transform (DWT) to the stego image, aiming to enhance the overall outcome. DWT based watermarking methods, known for their speed and robustness, offer protection against various forms of manipulation, making them a staple in the watermarking domain due to their substantial information capacity. The proposed method has demonstrated compliance with the essential characteristics of an ideal watermarking scheme, including imperceptibility, robustness, and ample capacity. Its applicability extends to authentication and data hiding purposes.

Future endeavors will explore the extension of this technique to encompass other categories and formats of images, such as DICOM images and videos.

5. REFERENCES

[1] Neil F.Johnson, ZoranDuric and SushilJajodia, "*Information Hiding, Steganography and Watermarking-Attacks and Counter Measures*," Kluwer academic publisher, pp. 15-29, 2003.

[2] Stefan Katzenbeisser and Fabien A. P. Petitcolas, "I*nformation Hiding Techniques for Steganography and Digital Watermarking*," Artech house, Computer security series, pp.15-23, 97-109, 2000.

[3] T. Morkel, J. Eloff and M. Olivier, "An Overview of Image Steganography," The Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa, July 2005

[4] H. Wang, S. Wang, “Cyber warfare: Watermarkingvs. Steganalysis”, Communications of the ACM, October 2004, Vol. 47, No. 10, pp. 76-82

[5] E. Walia, P. Jain, Navdeep, “An Analysis of LSB & DCT based Steganography”, Global Journal of Computer Science and Technology, April, 2010, Vol. 10, pp. 4-8.

[6] E. Hernández, C. Uribe, R. Cumplido . “FPGA Hardware Architecture of the StenographicContext Technique”, 18th International Conference on Electronics, Communications and Computers, pp. 123- 128, Puebla, Mexico, March, 2008.

[7] K. Prasad, V. Jyothsna, S Raju and S. Indraneel, “High Secure Image Watermarkingin BCBS Using DCT and Fractal Compression, International Journal of Computer Science and Network Security, vol. 10 No.4, April 2010.

[8] Nasir, F. Khelifi, Jianmin Jiang and S. Ipson, "A robust image watermarking scheme based on normalized circular image in DWT domain," *10th International Conference on Information Science, Signal Processing and their Applications (ISSPA 2010)*, Kuala Lumpur, Malaysia, 2010, pp. 33-36, doi: 10.1109/ISSPA.2010.5605562.

[9] Tay R., Havlicek, J.P*.,” image watermarking*.*Using wavelets”,* circuits and systems,pp.258-261, MWSCAS-2002.

[10] Pavan, A.C. and Somashekara, M.T., 2023. An Overview on Research Trends, Challenges, Applications and Future Direction in Digital Image Watermarking. *International Research Journal on Advanced Science Hub*, *5*(01).

[11] Saber, Mohamed, et al. "Watermarking System for Medical Images Using Optimization Algorithm." *Fusion: Practice & Applications* 10.1 (2023).

[12] Parah, S.A.; Sheikh, J.A.; Loan, N.A.; Bhat, G.M. Robust and blind watermarking technique in DCT domain using inter-block coefficient differencing. *Digit. Signal Process* 2016, *53*, 11–24.

[13] Kamili, A.; Hurrah, N.N.; Parah, S.A.; Bhat, G.M.; Muhammad, K. DWFCAT: Dual watermarking framework for industrial image authentication and tamper localization. *IEEE Trans. Ind. Inform.* 2020, *17*, 5108–5117.

[14] Chen, Q.; Hu, Q.W.; Feng, S.K.; Fu, Z. A Blind Digital Watermarking for Pdf Document. *Appl. Mech. Mater.* 2013, *392*, 1006–1009.

[15] Lin, H.F.; Lu, L.W.; Gun, C.Y.; Chen, C.Y. A Copyright Protection Scheme Based on PDF. *Int. J. Innov. Comput. Inf. Control* **2013**, *9*, 1–6.