www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 5 Issue 8 August 2016 Page No. 17633-17637

Implementation Of Encryption And Watermarking Algorithm For Remote Sensing Image.

Faruk Ahmed., Dr. E.N Ganesh
B.E., M.E(VLSI).
Saveetha Engineering college
B.E.,M.Tech.,Ph.D .
Principal., Saveetha Engineering College

Abstract—

This paper presents the processing of remote sensing image using water marking and encryption algorithm. Earth observation missions have recently attracted rowing interest form the scientific and industrial communities, mainly due to the large number of possible applications capable to exploit remotely sensed data and images. Along with the increase of market potential, the need arises for the protection of the image products from non-authorized use. Such a need is a very crucial one even because the Internet and other public/private networks have become preferred means of data exchange. A crucial issue arising when dealing with digital image distribution is copyright protection. Such a problem has been largely addressed by resorting to watermarking technology. A question that obviously arises is whether the requirements imposed by remote sensing imagery are compatible with existing watermarking techniques. On the basis of these motivations, the contribution of this work is twofold: i) assessment of the requirements imposed by the characteristics of remotely sensed images on watermark-based copyright protection ii) analysis of the state-of-the-art, and performance evaluation of existing algorithms in terms of the requirements at the previous point. so in this method we are going to propose the Double-Density Wavelet Transform for remote sensing image

Keywords—watermarking; Double density wavelet transform; remote sensing image

I.INTRODUCTION

Watermarking is a branch of information hiding which is used to hide proprietary information in digital media like photographs, digital music, or digital video. The ease with which digital content can be exchanged over the Internet has created copyright infringement issues. Copyrighted material can be easily exchanged over peer-to-peer networks, and this has caused major concerns to those content
providers who produce these digital contents. In order to protect the interest of the content providers, these digital contents can be watermarked.

II. PERFORMING DWT TRANSFORM OF THE WATERMARK IMAGE

Image watermarking techniques can be applied to digital videos as well. Digital watermarking techniques can be classified into two categories: spatial domain methods and transform domain methods. Spatial domain methods usually provide simple embedding schemes with inefficiency and low robustness. By contrast, watermarking techniques based on transform domain such as DFT, DCT , DWT can take full advantage of human perception and have a good robustness and invisibility. Several algorithms in mixed transform domain are recently presented to obtain high robustness and transparency. Algorithms in DWT and DCT transforms are for audio and image watermarking respectively, which combines the advantages of multiresolution and the energy compression properties of the DWT and DCT. Performing DWT transform of the watermark image In numerical analysis and functional analysis, a discrete wavelet transform (dwt) is any wavelet transform for which the wavelets are discretely sampled. As with other wavelet transforms, a key advantage it has over fourier transforms is temporal resolution: it captures both frequency and location information .To use the wavelet transform for image processing we must implement a 2d version of the analysis and synthesis filter banks. In the 2d case, the 1d analysis filter bank is first applied to the columns of the image and then applied to the rows. if the image has n1 rows and n2 columns, then after applying the 1d analysis filter bank to each column we have two subband images, each having n1/2 rows and n2 columns; after applying the 1d analysis filter bank to each row of both of the two subband images, we have four subband images, each having n1/2 rows and n2/2 columns. this is illustrated in the diagram below. The 2d synthesis filter bank combines the four subband images to ob in numerical analysis and functional analysis, a discrete wavelet transform(dwt) is any wavelet transform for which the wavelets are discretely sampled. 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 first dwt was invented by the hungarian mathematician alfréd haar. For an input represented by a list of 2^n numbers, the haar wavelet transform may be considered to simply pair up input values, storing the difference and passing the sum.

The inherent time-scale locality characteristics of the Discrete Wavelet Transforms has established them as powerful tools for numerous applications such as signal analysis, signal compression, and numerical analysis. This has lead numerous research groups to develop algorithms and hardware architectures to implement the DWT. In VLSI architectures for the 1D and 2D DWT have been proposed. Additionally, comparisons among the architectures and

scheduling algorithms for the DWT, regarding their efficiency when the DWT is mapped in custom VLSI architectures, has been performed in . Although the comparisons presented in [5] and [6] are enlightening, the related analysis is performed in an abstract level ignoring implementation platform parameters (e.g. memories' latency, number of ports, type of filters etc) that can heavily affect the results of such a comparison. Additionally, no direct comparison in terms of energy efficiency has been attempted so far. Furthermore the possible optimizations and their effect in the design parameters are not discussed by prior work. However, what prior work has pointed out, is that none of the alternative architectures has a clear lead in terms of either memory requirements or throughput or energy dissipation for all possible sets of parameters. Hence, the researcher or designer has not yet been provided with the an analytical comparison that will enable the early and secure selection of one among the alternative architectures for the 2D-DWT. In this paper we attempt to fill this gap. Specifically, the main VLSI architectures for the 2D-DWT are analytically described. Additionally throughput and memory minimization optimizations are presented and their effect is analyzed. The main contribution of this paper is the comparative study of the alternative architectures, which is based on the development of analytical equations for memory requirements, throughput, and energy. Analysis focuses on the forward 2D-DWT. Energy Model For the energy characterization of the alternative hardware architectures for the 2D-DWT, only energy consumed due to data storage and transfers is taken into account. This suffices for the purposes of this paper for two reasons: 1. In hardware implementation of data-intensive algorithms, such as the 2D-DWT, the energy dissipation due to data storage and transfers forms the dominant component (up to 80%) of the total power budget . It is indicative that a transfer to/from an on-chip memory consumes 4 10 times more power than one addition, while an off-chip accesses requires 10 100 times more power than an on-chip access . 2. The different hardware architectures, perform exactly the same number of filtering operations. Thus it can be said that energy consumed to arithmetic operations is a common cost for all architectures. The energy dissipated on the memory hierarchy is approximated by the energy dissipation due to on-chip memory accesses plus the energy dissipation due to off-chip memory accesses.

A. Double density discrete wavelet transform

To implement the double-density DWT, we must first select an appropriate filter bank structure. The filter bank proposed in Figure 1 illustrates the basic design of the double-density DWT. The analysis filter bank consists of three analysis filters—one low pass filter denoted by $h_0(-n)$ and two distinct high pass filters denoted by $h_1(-n)$ and $h_2(-n)$. As the input signal x(n) travels through the system, the analysis filter bank decomposes it into three sub bands, each of which is then down-sampled by 2. From this process we obtain the signals c(n), $d_1(n)$, and $d_2(n)$, which represent the low frequency (or coarse) sub band, and the two high frequency (or detail) sub bands, respectively.

The synthesis filter bank consists of three synthesis filters—one low pass filter denoted by $h_0(n)$ and two distinct high pass filters denoted by $h_1(n)$ and $h_2(n)$—which are essentially the inverse of the analysis filters. As the three sub band signals travel through the system, they are up-sampled by two, filtered, and then combined to form the output signal y(n).One of the main concerns in filter bank design is to ensure the perfect reconstruction (PR) condition. That is, to design $h_0(n)$, $h_1(n)$, and $h_2(n)$ such that y(n)=x(n).

B. Dual tree complex

The dual-tree complex DWT of a signal x is implemented using two critically-sampled DWTs in parallel on the same data, as shown in the figure.The transform is 2-times expansive because for an N-point signal it gives 2N DWT coefficients. If the filters in the upper and lower DWTs are the same, then no advantage is gained. However, if the filters are designed is a specific way, then the subband signals of the upper DWT can be interpreted as the real part of a complex wavelet transform, and subband signals of the lower DWT can be interpreted as the imaginary part.

C. Equation

The energy dissipated on the memory hierarchy is approximated by the energy dissipation due to on-chip memory accesses plus the energy dissipation due to off-chip memory accesses.

$$E_{MEM} = X \cdot E_{ON\ CHIP}\ M_{EMI} + X \cdot E_{OFF\ CHIP}\ M_{EMI}$$

III. AES ENCRYPTION OF THE ORIGINAL IMAGE

This paper discusses a Matlab implementation of the Advanced Encryption Standard (AES) . AES is based on the block cipher Rijndael and became the designated successor of the Data Encryption Standard (DES) which has been implemented in a tremendous number of cryptographic modules worldwide since 1977. Matlab is a matrix-oriented programming language, perfectly suited for the matrix-based data structure of AES. Even though this implementation is fully operational, (i. e. it can be utilized to encrypt arbitrarily chosen plaintext into ciphertext and vice versa), the main optimization parameter of this implementation has not been execution speed but understandability. Assembler programmers might throw their hands up in horror, looking at shifting or substitution functions that have been coded algorithmically step-by-step instead of using a simple predefined lookup table; the primary goal of this "educational" paper is to explain in greater detail what has to be done, rather than how it could be done for speed optimization reasons. Also the question why certain algorithms have been chosen, e. g. with respect to the resistance against differential and linear cryptanalysis, is far beyond the scope of this paper. Interested readers are referred to the annex of the AES proposal or a good book on cryptography . Even Galois fields, the workhorse of modern cryptography, are introduced in a very pragmatic, engineer-friendly way, touching only as much mathematical background as necessary.

Furthermore, in order to minimize the number of if-then-else-conditions, a key length of 128 bits (16 bytes) has been implemented only; the extension to 24 or 32 bytes key lengths, as defined in , can easily be realized by altering the corresponding constants.

IV.WATERMARK EMBEDDING

The process of watermark embedding is using a watermarking key and watermarking algorithm to produce watermarked digital image.The embedding methodvary based on which image domain is being processed e.g the space , frequency domain or the wavelets.Depending on

embedding method detectable(single bit) or readable bit watermarks are being incorporated to digital image.

In case of two-dimensional image, after a DWT transform, the image is divided into four corners, upper left corner of the original image, lower left corner of the vertical details, upper right corner of the horizontal details, lower right corner of the component of the original image detail (high frequency). You can then continue to the low frequency components of the same upper left corner of the 2nd, 3rd inferior wavelet transform.

The extraction algorithm process is the inverse of the embedding process. It is assumed that the watermark as well as the see value is available at the receiver end to the authorized users.

The operation of channel separation is applied on the watermarked color image to generate its sub images, and then 2-level discrete wavelet transform is applied on the sub images to generate the approximate coefficients and detail coefficients.

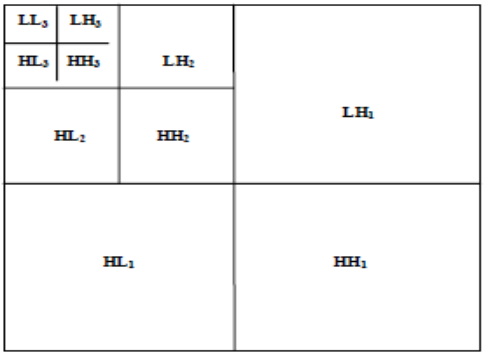

Fig1: DWT decomposition model

On the basis of such considerations, the algorithm uses a different color image multiplied by the weighting coefficients of different ways to solve the visual distortion, and by embedding the watermark, wavelet coefficients of many ways, enhance the robustness of the watermark.

Pictures, music, cinemas and other forms of art are traditionally stored in the physical media, such as CD disks, photo paper or films. With the advance of computer technology, these works are digitized as a sequence of 0s and 1s for easy storage and distribution. However, the technology has also brought us a new dilemma: on the one hand, it offers us the great convenience of storage and duplication; on the other hand, it also makes easier the unauthorized copying and redistribution. Copying in the digital world is exact, and no technology available can differentiate between the originals and the duplicates. The great popularity of Internet even makes things worse. Internet provides us with the great ease of

exchanging ideas and sharing resources between and among its users. Publishers can sale over Internet to save the high cost of transportation and delivery, while at the same time the purchasers can gain quick access to the published works. This simple rule works over Internet if all the subscribers are honest not to resale the digital works for commercial benefits. However, there are always dishonest people complicating the whole business. With the help of Internet, the pirates can redistribute the authorized copies more efficiently and effectively. The huge losses suffered by the media companies call urgently on a technology for copyright protection. Traditional cryptography fails to meet this need since when decrypted, the content data will be fully exposed to the pirates who have also purchased the contents. The decrypted contents can thus be easily copied and redistributed. Can any further protection be provided to combat this problem? Luckily, the watermarking technology is born to meet this growing demand. It embeds perceptibly or imperceptibly the copyright or the ownership information into the digital work itself. The embedded information is supposed to be permanently coupled with the original work and copied into the duplicated work, and could be detected even after any severe removal or confusing attacks.

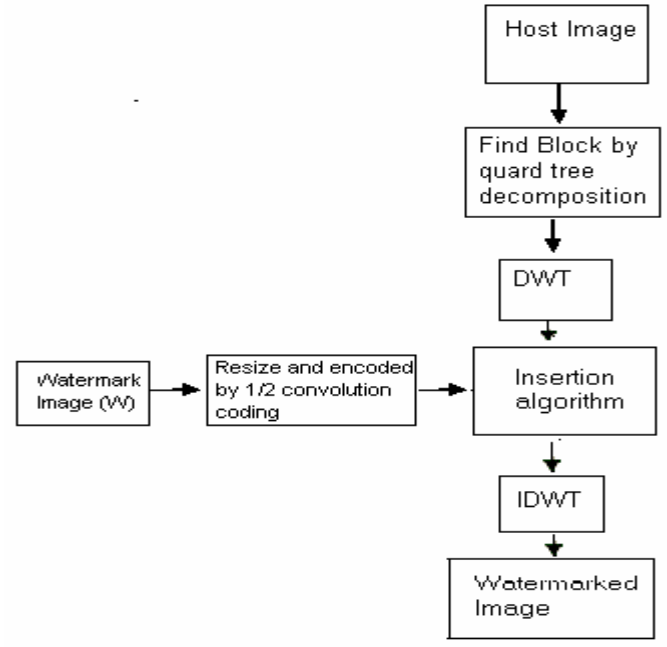

Fig2:watermark insertion

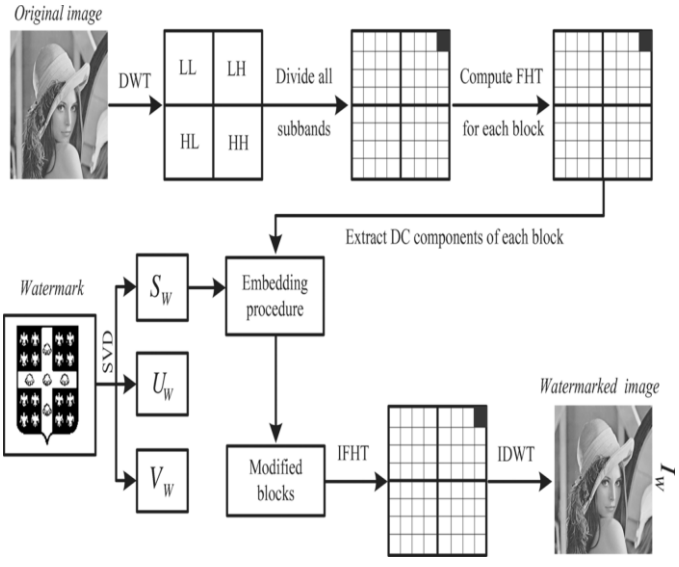

Fig3:watermarking of digital images based on singular valued dicomposition

V.FPGA IMPLEMENTATION OF THE WATERMARKED IMAGE

The watermarked image obtained by embedding watermark image with the remote sensing image is then converted to

binary and taken as an input for the VHDL code for implementing this image in the FPGA kit .This is obtained by taking the binary image in the VHDL program of constant ROM. The pixel bits are stored in the data address constantly and can be visualized using VGA monitor.

The block diagram for the proposed system is shown in the figure below

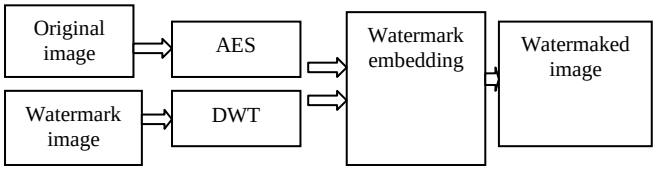

Fig4:proposed system

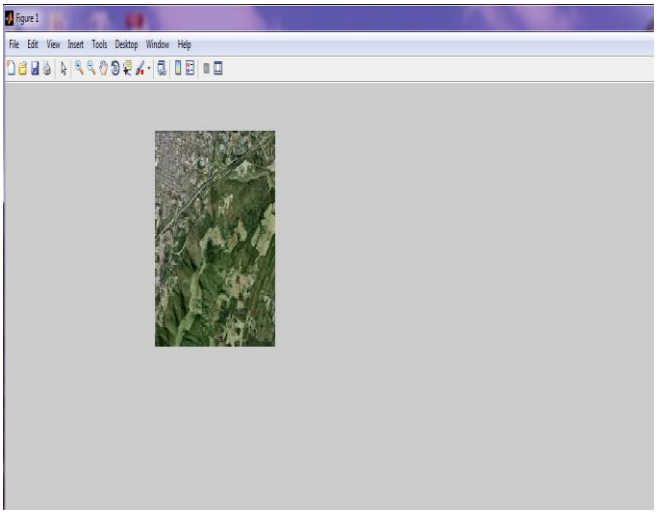

Fig5:original image

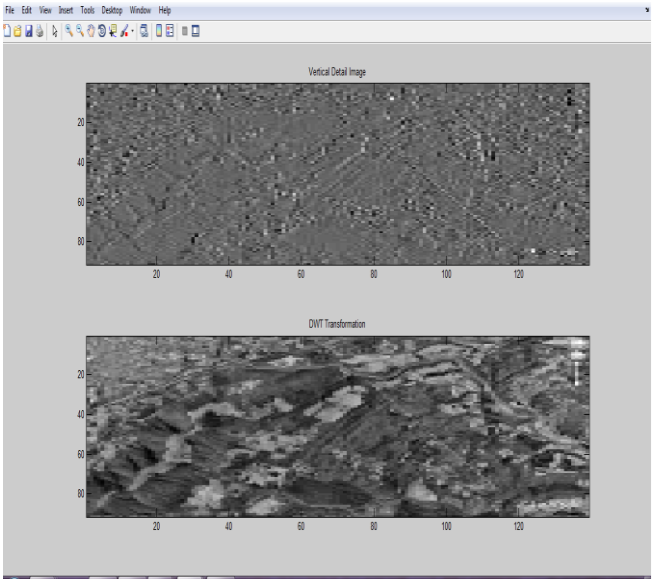

Fig6:DWT transformed image

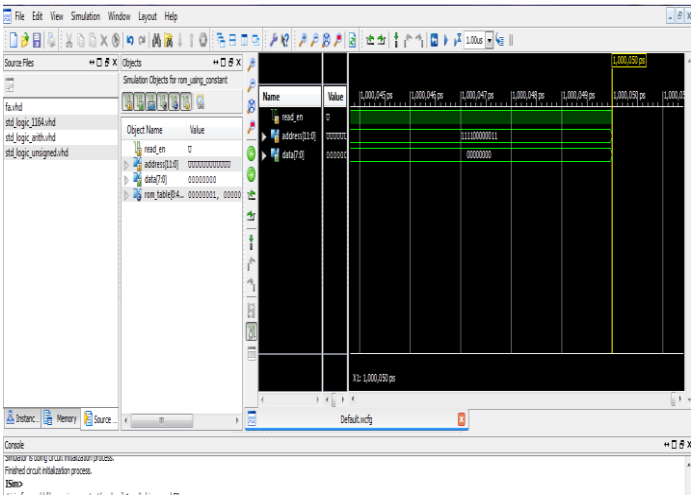

Fig7:FPGA implementation of the binary image

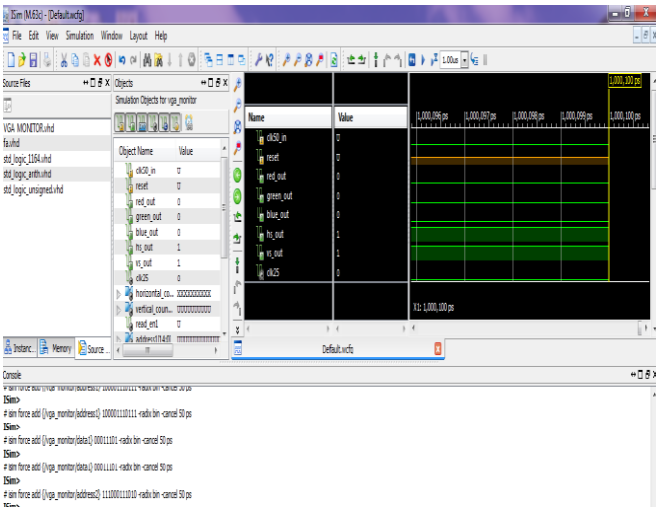

Fig8:Data ROM constant

Marking invisibility means that the nondegradation of carrier after mark embedding. As mentioned above, greater PSNR denotes better image quality, then better marking invisibility. The PSNRs of the 10 decrypted-marked images are all around

35 dB. is the decrypted-marked square under the proposed scheme, whose PSNR = 38.86 dB. Robustness experiments: (a) second JPEG compression and (b) AGWN. the original image, there is little difference and the proposed algorithm satisfies the marking invisibility constraint. Marking robustness is the ability of embedding mark against normal signal processing. The robustness experiments are conducted by the second JPEG compression and additive Gaussian white noise (AGWN). With the same experimental parameters, the dither modulation marking algorithm under the proposed scheme is compared with the common dither modulation marking algorithm. From Fig., it can be seen that, in a not so strong attack, the robustness of the marking algorithm under the proposed scheme is not outstanding and even weaker than the common algorithm, but it does not affect the mark extracting; however, with the increase of the attack intensity, the advantage of the marking algorithm under the proposed scheme becomes more clear: its correlation value of extracting mark is much bigger than the common algorithm.

Table lists the PSNR between original host image and watermarked image for various value of λ

λ	11	12	13	14	15	16
MSC	2.1753	2.3194	2.4751	2.6424	2.8212	3.0117
RMS	1.4749	1.5230	1.5732	1.6255	1.6797	1.7354
PSNR	44.7557	44.4771	44.1949	43.9108	43.6264	43.3427

Conclusion:

As a kind of sensitive information, remote sensing image requires not only security during storage and transmission butalso security during usage. However, there is no ideal practical security protection for remote sensing image.

In this paper thus we have general definition of digital image watermarking, our own work in watermarking start on chapter two using DWT first we decompose the host image into four bands LL, LH, HL and HH and we embedding the watermark in each band and with different values of quality factor and embedding factor.

Under the proposed scheme, during the storage or transmission of remote sensing image, encryption can be used to prevent information leakage actively, and in the same time, mark can be extracted from ciphertext for copyright protection.

This research was taken up with an objective of developing watermarking algorithms for images. We felt that it is essential to first ensure that all the developed watermarking schemes are resistant to at least one attack having the most financial implications to establish a high demand in the commercial market

References

[1] L. Jiang and Z. Xu, "Commutative encryption and watermarking for remote sensing image," *Int. J. Digit. Content Technol. Appl.*, vol. 6, no. 4, pp. 197–205, Jul. 2012.

[2] G. Strang, *Introduction to Linear Algebra*, 4th ed. Cambridge,MA, USA:
Wellesley-Cambridge, 2009, pp. 203–213.

[3] R. C. Gonzales and R. E. Woods, *Digital Image Processing*, 3rd ed. Englewood Cliffs, NJ, USA: Prentice-Hall, 2007, pp. 558–563.

[4] S. He and M. Wu, "Joint coding and embedding techniques for multimedia
fingerprint," *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 2, pp. 231–247, Jun. 2006.

[5] P. Sweeney, *Error Control Coding From Theory to Practice*, 2nd ed. Hoboken, NJ, USA: Wiley, 2002, pp. 155–176.

[6] B. Chen and G. W. Womell, "Quantization index modulation: A class of provably good methods for digital watermarking and information embedding,"
IEEE Trans. Inf. Theory, vol. 47, no. 4, pp. 1423–1443, May 2001.

[7] S. Lian, *Multimedia Content Encryption: Techniques and Applications*, 1st ed. New York, NY, USA: Auerbach, 2008.

[8] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data,"
IEEE Trans. Inf. Theory, vol. 44, no. 5, pp. 1897–1905, Sep. 1998.

[9] H. V. Zhao, M. Wu, Z. J. Wang, and K. J. R. Liu, "Forensic analysis of nonlinear collusion attacks for multimedia fingerprinting," *IEEE Trans. Image Process.*, vol. 14, no. 5, pp. 646–661, May 2005.

[10] R. W. Conners and C. A. Harlow, "A theoretical comparison of texture algorithms," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 2, no. 3, pp. 204–222, May 1980.

[11] R. C. Gonzales and R. E. Woods, *Digital Image Processing*, 3rd ed. Englewood Cliffs, NJ, USA: Prentice-Hall, 2007, pp. 850–858.

[12] M. Barni, F. Bartolini, V. Cappellini, E. Magli, and G. Olmo, "Nearlossless
digital watermarking for copyright protection of remotely sensed images," in *Proc. IEEE Int. Geosci. Remote Sens. Symp. (IGARSS)*, 2002, vol. 3, pp. 1447–1449.