Quick Response Decomposition Watermarking Algorithm based on Discrete Wavelet Transform Techniques

T.R.Ganesh Babu[1], R.Praveena[1], M.Lakshmi[2], Balachandra Pattanaik[3]

[1]Muthayammal Engineering College, Salem, Tamil Nadu, India
[2]S.A. Engineering College, Chennai, Tamil Nadu, India
[3]College of Engineering and Technology Wallaga University, Ethiopia
ganeshbabutr@gmail.com,

Abstract. Now a days, Image compression schemes and water marking is widely performed in signal processing with the help of wavelet transform. In comparison with approaches based on DCT and wavelet-based watermarking in some cases wavelet based Watermarking schemes are used better. In the literatures hardware realization was diverse for watermarking digitally. Design and implementation of a Field Programmable Gate Array (FPGA) based architecture discrete wavelet transform (DWT) invisible watermarking algorithm using QR decomposition will be focused in this paper. When using Reversible Watermarking techniques some image losses occurs and compression ratio is about 1.6. But while using discrete wavelet transform (DWT) invisible watermarking fragile algorithm using QR decomposition image compression ratio can be increased to 1.9 . We chose MATLAB and Xilinx 14.1 4Spartan 3E FPGA for VLSI architecture implementation and schematic based design

Keywords: Wavelet transform, Water marking, DCT, FPGA, VLSI

1 Introduction

Digital water marking is one of the techniques which can be used to identify the illegally distributed images. It can be done by two methods one is spatial domain and another one is frequency domain [1]. Commonly, the main limitation is available in watermarking techniques that is size, so, in order to establish the combined techniques of spatial and frequency domains which is used to achieve the huge number of watermark data and to reduce the noise of the watermark image. After, the frequency domain of host image is embedded with watermarks and to perform the translation operation of image from frequency domain to spatial domain by using inverse transform. Though, the transformed image of the pixel value to be in real numbers. During the process of transforming that the image is transformed from frequency domain into spatial domain in that the data is somewhat troubled because of converting real numbers into integers in the spatial domain and to reduce this type of trouble in rounding process by using GA-based watermarking algorithm. Hence, to improve the security by using GA-based watermarking and this is one of the techniques is used to rounding the errors for both robust and fragile watermarks.

R. Murugan et al. (eds.), *Proceedings of the International Conference on Signal Processing and Computer Vision (SIPCOV 2023)*, Advances in Engineering Research 239,
https://doi.org/10.2991/978-94-6463-529-4_37

The main aim of this work to develop the DWT invisible watermarking algorithm and to implement in FPGA related architecture using QR decomposition [2].

In watermarking System consists of two processes, one is insertion and another one is detection. The combined process is used to attack the watermarked images.

The insertion step is given by,

$$P_i = P_{ori} + \left(q_i(C) + W_i\right) * \alpha \quad (1)$$

q = Key generator

C= Binary Random Sequence

i = i^{th} iteration

α = Visibility factor

P_i= i^{th} watermarked coefficient

P_{ori} = i^{th} original coefficient

W_i = i^{th} bit of the watermark

The extraction step is given by,

$$W'(i) = \left[\frac{[LHt(i) - LH0(i)]}{\alpha} + C(i)\right] \quad (2)$$

With LHt : Watermarked sub-band
LHo : Original sub-band

$$\begin{cases} P_{al}(i) \geq S \rightarrow W(i) = 1 \\ else \rightarrow W(i) = 0 \end{cases} \quad \begin{cases} P_{al}(i) \geq S \rightarrow W(i) = 1 \\ else \rightarrow W(i) = 0 \end{cases}$$

with $P_{al}(i)$: i^{th} is the coefficient between watermarked and original coefficient
S : Threshold value

2 Existing System

Database watermarking, video watermarking, image watermarking and audio watermarking etc. these were the classification of digital signals based on the signal type. fragile watermarking or robust is also a category of watermark based on the robustness. By the embedding process the distortion inflicted on the host media is one such drawback of watermarking-based authentication schemes. In military applications and medical imaging, it may not acceptable even this distortion is often insignificant, Hence, for recovering the original media, removing distortion the watermarking scheme should be efficient so we can get desired authentication.

Reversible watermarking schemes [3] indicates schemes with capability. With different type of algorithm Various Reversible Watermarking techniques has been proposed. Popular reversible watermarking techniques are: i) Integer Discrete Cosine Transform, ii) Contrast Mapping, iii) Histogram bin Shifting, iv) Data hiding using Integer Wavelet Transform, and v) Difference Expansion. Usually, reversible scheme performs some type of lossless compression operation on host media in order to make space for hiding, compressed data and the Message Authentication Code (MAC) hash, signature, or other feature derived from the media were used as the watermark.

These were done to authenticate the media which is received, information hidden is extracted and it will decompress the compressed data for obtaining possible original media as possible. the possible original media is used to obtain the MAC [4]. If the extracted one and the newly derived MAC matches, then it is deemed authentic/original. However, a specific transform is done with the implementation of the reversible watermarking technique. The reason behind choosing this technique is because for it robust and has less computational complexity. Accomplishing the high-speed hardware efficient VLSI architecture is the primary goal of the proposed design. The Discrete Cosine Transform (DCT) technique has been used in the proposed scheme [5].

In that the water marking is used DCT coefficients of all 128-bit hash [6]. Then for verification it uses the compressed bit-stream which is extracted; with no local information signature of the image is alone in the hash. Hence, this technique is unable to locate the position where the tampering has been done although it is simple and has the ability to detect authenticity, this technique is unable to locate the position where the tampering has been done [7-10].

3 Proposed System

In watermarking application, fragile watermarking approach is used for content authentication. In watermarking algorithm, the content authentication system provides a high level of brittleness and digital watermarking are also acknowledged a new attention which is comparatively new technology [11].

For analysis and betterment of a watermarking technique for particular application few recognized tools and metrics were used, which can be evaluate the performance by researchers. Because of this insufficient tool and metric need to motivate and develop a web based digital watermark evaluation method called watermark evaluation test bed or WET [12]. It is a web which is designed to be absorbed from still image digital watermarking [13].

This watermark evaluation test bed method includes a reference software which contains both watermark embedders and detectors, attacks, evaluation modules, and a large image database. The aim of this work is to develop a platform which is not only used to test but also used for performance of own techniques. Figure 1 and 2 shows the block diagram of fragile watermarking and detection process [14].

In figure 1 indicates the diagram of fragile water marking algorithm, first select watermark algorithm and relevant parameters. Based on this parameter select the input

images and that images are embedded into the system and detection operation is performed. Figure 2 represents the detailed flow of fragile water marking algorithm. In that diagram based on the secret key insertion, distortion and detection process is selected.

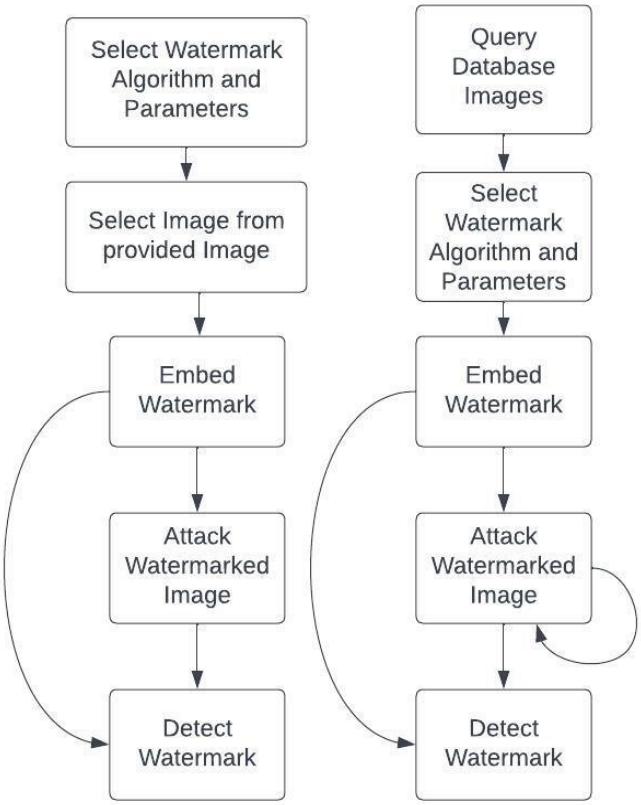

Fig. 1. Block diagram of fragile water marking algorithm

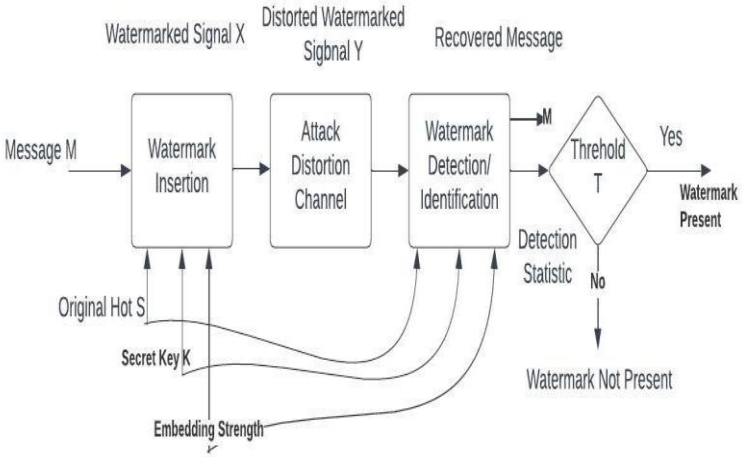

Fig. 2. Block diagram of fragile water marking algorithm for detection process

In this paper, the system is categorized into two stages which is watermark embedding is first stage followed by watermark extraction is second stage shown in fig 3 and 4[15].

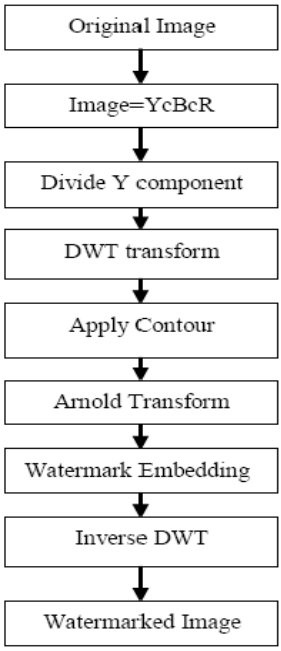

Fig. 3. Watermark Embedding Process

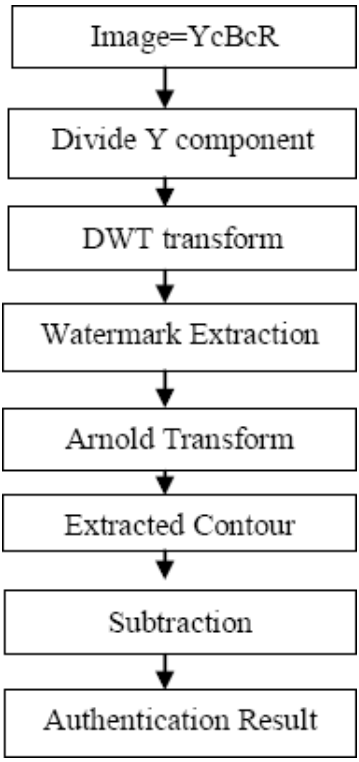

Fig. 4. Watermark Extraction Process

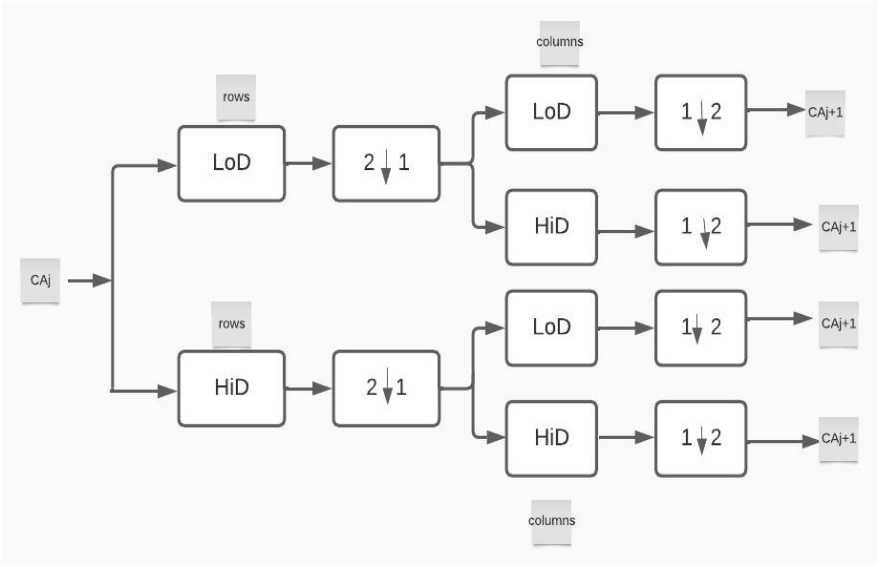

Fig. 5. Block Diagram of Wavelet Decomposition

In the figure 5 represents two-dimensional wavelet transform. The following parameters indicates the rows and columns of the above diagram.

Where,

$2 \downarrow 1$ represents down sample columns

$1 \downarrow 2$ represents down sample rows

CA indicates decomposition initialization

The following equation [3-7] represents one level wavelet transform

$$\phi(x1,x2)=\sum n1 \sum n2 h0(n1,n2)\phi(2x1-n1,2x2-n2) \quad (3)$$

$$\phi(x1,x2)=\sum n1 \sum n2 h(n1)h(n2)\phi(2x1-n1,2x2-n2) \quad (4)$$

$$\psi hg(x1,x2)=\sum n1 \sum n2 h(n1)g(n2)\phi(2x1-n1,2x2-n2) \quad (5)$$

$$\psi gh(x1,x2)=\sum n1 \sum n2 g(n1)h(n2)\phi(2x1-n1,2x2-n2) \quad (6)$$

$$\psi gg(x1,x2)=\sum n1 \sum n2 g(n1)g(n2)\phi(2x1-n1,2x2-n2) \quad (7)$$

The following equation[8-11] represents the two level wavelet transform.

$$Sj,v=2l2\sum khh(l-2v)Sj+l,l \quad [8]$$

$$Wlj,v=2l2\sum khg(l-2v)Sj+l,l \quad [9]$$

$$W2j,v=2l2\sum kgh(l-2v)Sj+l,l \quad [10]$$

$$W3j,v=2l2\sum kgg(l-2v)Sj+l,l \quad [11]$$

The extraction procedure follows the Decryption of a chaotic map, Inverse of Arnold, and Inverse of Fast Fourier transform algorithms.
In this the system will read the input host image and the YCbCr color space is created from RGB image. In the Y, Cb, Cr components of watermarking apply the 4 level DWT and sub-band components LL, HL, LH, and HH are accomplished. Apply Singular value decomposition to hl sub-band of the fourth DWT.

Extract watermark information with host components of y, Cb, Cr. Calculate encoded bits with chaotic map, apply channel decoding, Embed watermark information with host components Y, Cb, Cr. Reshape them according to decoded bits, Apply the inverse of the Arnold transform. Perform decryption of a chaotic map and achieve the extracted watermark image.

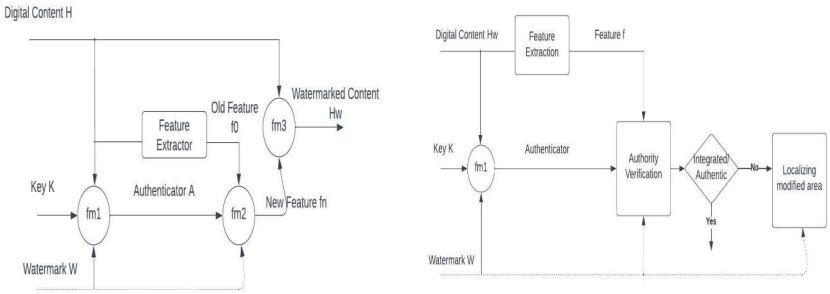

Fig. 6. Watermarking model

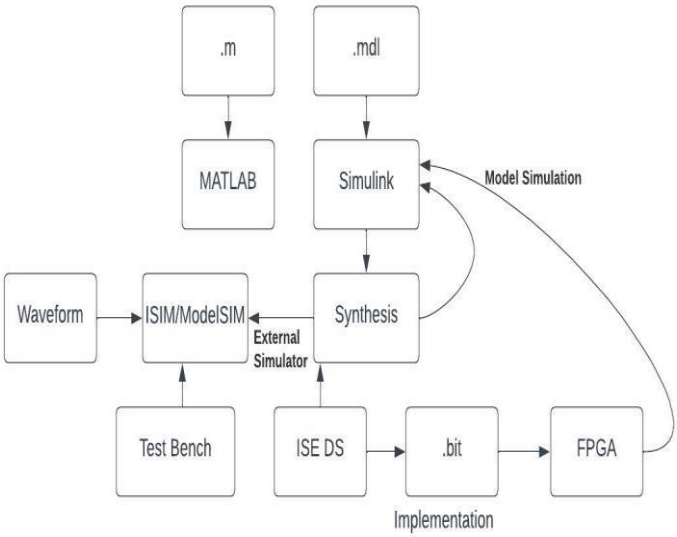

Fig. 7. Design Flow of Proposed System

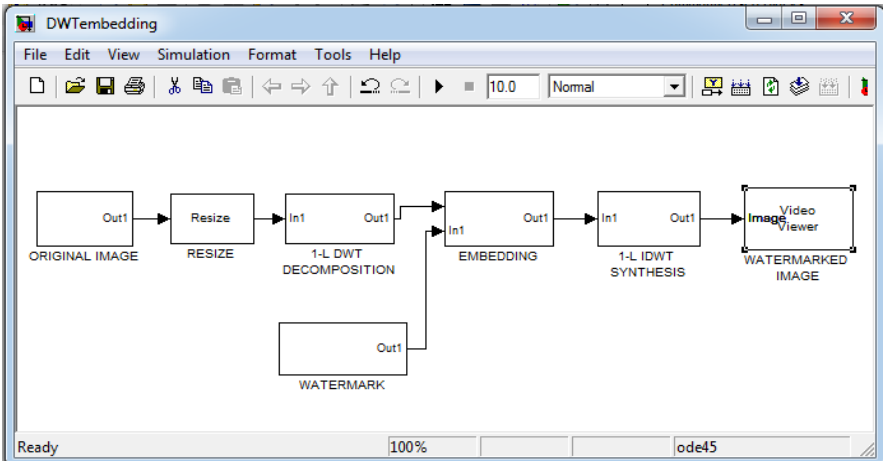

Fig. 8. Watermark Embedding Model in Simulink

Feature to generate a new feature fn with fn = fun2(fo,A,W). Finally, watermarked image HW is produced by function fun3 on the new feature fn substituting the old feature fo shown in Fig. 6. Figure 7 represents the design flow of proposed diagram. It should be noted that function fun3 is a general function, generally speaking, which can embed the new feature fn into the given image using a watermark algorithm or other algorithms.

A cryptographic hash or message authentication code (MAC) function can be used in this process without loss of generality. The extracting process is shown in Fig.8 and 9. First function fun1 is used to generate the same authenticator A as in the embedding procedure, and then feature extraction algorithm outputs feature f, into which the authenticator. A in embedding 5procedure is embedded. Once the feature has been extracted, the inverse function of function fun2 can extracts the embedded authenticator from feature f. Then we compare this extracted authenticator with the authenticator A to determine whether the received digital content is authentic or not. If both are the same that prove the source.

4 Results and Discussion

The following steps represents the watermark embedded process

1. The actual image is reconstructed into 512x512. The DWT is applied to the input image, then the output of decomposed image is 256x256 size image.
2. The watermark image size is 32x32, 256x256 is the correct dimension to embedded with 32x32 pixels on 8x8 sub-blocks.
3. A one level DWT has applied.
4. After, watermark embedded image obtained Low-high frequency components.
5. Then the IDWT is applied to this image to get watermark image.

The watermarking process is same but in the reverse order. Watermark extraction process is same as the watermarking process but the order of process is reversed.

1. The output image is resized into 512x512 pixels.
2. A 1-level DWT is applied to watermarked resized image.
3. The comparison operation is done for extraction according to the embedding process.

In this work, after completion of decomposition process to increase the speed of the operation, we need to implement in FPGA design. After the implementation process, MATLAB Simulink file embedded with FPGA board by using DSP builder software and this Simulink file converting into HDL code.

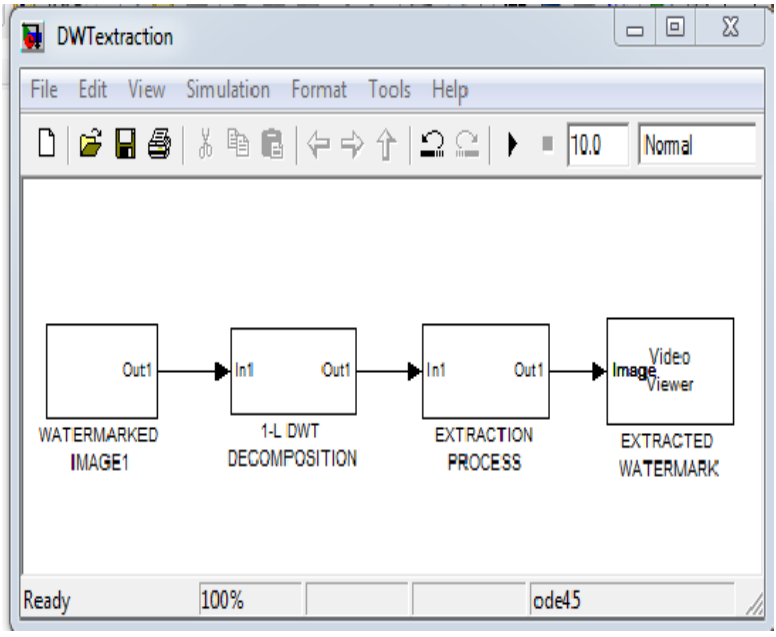

Fig. 9. Watermark extraction model

5 Conclusion

A watermarking is one of the emerging technique in current research field for many applications The digital watermarking is used to cryptography management and protection applications. In our work, to analysis frequency domain image processing and implement in FPGA board. In this work, discrete wavelength transform used for embedding and extraction process. The developed algorithm is implemented in FPGA architecture to increase the speed of the operation. In this developed algorithm, so image losses will occur due to the compression ratio that value is 1.6. But while using discrete wavelet transform (DWT) invisible watermarking fragile algorithm using QR decomposition image compression ratio can be increased to 1.9. In this work, encoding method is used for invisible fragile watermarking process.

References

1. S. Emmanuel and M. S. Kankanhalli, "A Digital Rights Management Scheme for Broadcast Video," ACM-Springer Verlag Multimedia Systems Journal, vol. 8, no. 6, pp. 444–458, June 2003.
2. D. Kundur and K. Karthik, "Digital Fingerprinting and Encryption Principles for Digital Rights Management," IEEE Signal Processing, vol. 52, 2004.
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. N. M. Kosaraju, M. Varanasi, and S. P. Mohanty, "A High Performance VLSI Architecture for Advanced Encryption Standard (AES) Algorithm," in Proceedings of 19th IEEE International Conference on VLSI Design, 2006, pp. 481–484.
5. S. Katzenbeisser and F. A. P. Petitcolas, Information Hiding techniques for steganography and digital watermarking, Artech House, Inc., MA, USA, 2000.
6. S. P. Mohanty, "Digital Watamerking of Images," M.S. thesis, Department of Electrical Engineering, Indian Institute of Science, Bangalore, India, 1999
7. N. Memon and P. W. Wong, "Protecting Digital Media Content," Communications of the ACM, vol. 41, no. 7, pp. 35–43, July 1998.
8. F. Mintzer, G. Braudaway, and M. Yeung, "Effective and Ineffective Digital Watermarks," in IEEE International Conference on Image Processing (ICIP-97), 1997, vol. 3, pp. 9–12.
9. S. P. Mohanty, K. R. Ramakrishnan, and M. S. Kankanhalli, "A Dual Watermarking Technique for Images," in Proceedings of the 7th ACM International Multimedia Conference (Vol. 2), 1999, pp. 49–51.
10. I. J. Cox, J. Kilian, T. Shamoon, and T. Leighton, "Secure Spread Spectrum Watermarking of Images, Audio and Video," in Proceedings IEEE International Conf on Image Processing, 1996, vol. 3, pp. 243–246.
11. I. J. Cox, J. Kilian, T. Shamoon, and T. Leighton, "A Secure Robust Watermarking for Multimedia," in Proceedings of First International Workshop on Information Hiding, 1996, vol. 1174, pp. 185–206.
12. I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," IEEE Transactions on Image Processing, vol. 6, no. 12, pp. 1673–1687, Dec 1997.
13. H. Berghel, "Watermarking Cyberspace," Communications of the ACM, vol. 40, no. 11, pp. 19–24, November 1997
14. Swanson, M. Kobayashi, and A. Tewfik, "Multimedia Data Embedding and Watermarking Technologies," Proceedings of the IEEE, vol. 86, no. 6, pp. 1064–1087, June 1998.
15. S. Craver, N. Memon, B. L. Yeo, and M. M. Yeung, "Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks and Implications," IEEE Journal on Selected Areas in Communications, vol. 16, no. 4, pp. 573–586, May 1998.