Hindawi Publishing Corporation
EURASIP Journal on Advances in Signal Processing
Volume 2009, Article ID 938515, 13 pages
doi:10.1155/2009/938515

Research Article

Joint Watermarking and Encryption of Color Images in the Fibonacci-Haar Domain

Federica Battisti,[1] Michela Cancellaro,[1] Giulia Boato,[2] Marco Carli,[1] and Alessandro Neri (EURASIP Member)[1]

[1] *Department of Applied Electronics, Universitá degli Studi Roma, TRE, 00146 Roma, Italy*
[2] *Department of Information Engineering and Computer Science, University of Trento, Trento 38123, Italy*

Correspondence should be addressed to Marco Carli, carli@uniroma3.it

Received 2 December 2008; Revised 6 March 2009; Accepted 23 July 2009

Recommended by Bulent Sankur

A novel method for watermarking and ciphering color images, based on the joint use of a key-dependent wavelet transform with a secure cryptographic scheme, is presented. The system allows to watermark encrypted data without requiring the knowledge of the original data and also to cipher watermarked data without damaging the embedded signal. Since different areas of the proposed transform domain are used for encryption and watermarking, the extraction of the hidden information can be performed without deciphering the cover data and it is also possible to decipher watermarked data without removing the watermark. Experimental results show the effectiveness of the proposed scheme.

Copyright © 2009 Federica Battisti et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

1. Introduction

Nowadays our life is becoming more and more permeated with Internet or widely-used communication systems (GSM, UMTS, CDMA2000, WLAN, etc.) and the technology allows an easy access to an almost unlimited amount of information. On one hand, the increased ease in sharing and transmitting data is an important goal and a basic need in our society; on the other hand the multimedia data need to be protected against reproduction and nonauthorized diffusion and modification. To satisfy these needs, several techniques have been developed, among them watermarking and cryptography.

Watermarking techniques are suitable for copyright protection: before distributing the data, the owner embeds an invisible signature, the watermark, into the host source (audio, text, image, or video) using a secret key (see Figure 1). In most applications, the existence of the signature is kept secret and the secret key, previously shared on a secure channel, is used to verify the presence of the embedded sequence in the detection phase. The design of a watermarking scheme is based on some important requirements: imperceptibility of the hidden data, robustness against data processing, capacity of hiding as many bits as needed, and granularity. As widely demonstrated in literature, such constraints are often in contrast to each other, forcing the designer to find a tradeoff among them. As far as robustness is concerned, the watermark must be detectable even after modifications, editing, or transmission of the cover data. Therefore, several techniques insert the watermark into the most significant portions of the digital data, so that it cannot be removed without impairing the original content.

A different approach for protecting data is given by cryptography, whose aim is to make the to-be-protected data not intelligible to any unauthorized user who might intercept the message. The digital data have to be decrypted in order to *extract* its information, being vulnerable to attacks, and manipulations. Obviously, protection vanishes after decryption. It is important to underline that the principle defined by Kerckhoffs [1, 2] for cryptography also stands for watermarking: the effectiveness of a cryptographic system should only depend on the secrecy of the key. The knowledge of the ciphering, or of the watermarking algorithm, should not allow an unauthorized user to decrypt the message or

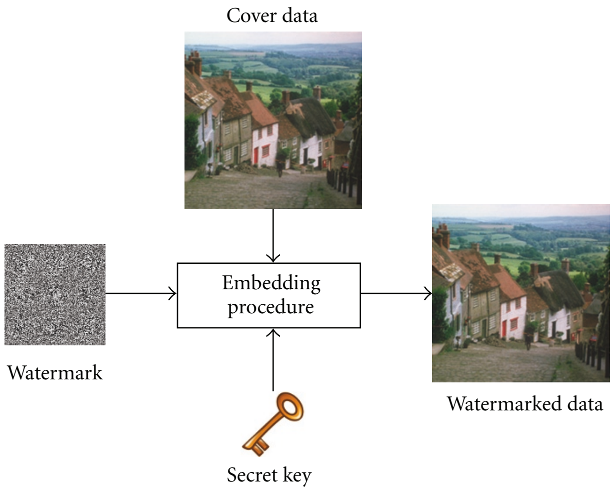


Figure 1: General watermarking scheme.

to have information about the existence of hidden data. Discovering a hidden message should only be possible with the knowledge of the secret key. Besides this analogy, the two techniques are complementary rather than overlapping and can be combined to increase protection of the message.

In this work we consider joint encryption and watermarking of color images, thus providing both levels of security. As described in [3], it is possible to increase the overall system security by utilizing a layered approach where watermarking and cryptography are simultaneously used as shown in Figure 2.

In the proposed scheme a key-dependent transform, the Fibonacci-Haar Transform, is employed to add an additional level of security. The main contribution of this paper is in the joint use of a key dependent wavelet transform with a secure cryptographic scheme. The intrinsic security of the method is in the adopted cryptographic scheme.

The rest of the paper is organized as follows. In Section 2 the state of the art on color watermarking and joint watermarking and encryption schemes is presented. In Section 3 the proposed method is described in details, while in Section 4 experimental results are reported. Finally, some conclusions are drawn in Section 5.

2. Previous Work

2.1. Color Image Watermarking. In literature several methods have been proposed to protect digital color images by using watermarking. However only few of them are considering the relation existing among the color components. Most of the proposed systems have been designed for gray scale images and then independently applied on the color components.

Singular Value Decomposition (SVD) has been proposed as a tool for watermarking color images in [4, 5]. Xing and Tan in [4] propose to partition each color component of the cover image (the image to be protected) in nonoverlapping blocks and to embed one bit of the watermark, using an additive scheme, to the greatest singular value of each block. The block size is adapted to the amount of information to be hidden. The robustness of the whole scheme is increased by scrambling the watermark before insertion through the Arnold transformation. The basic idea is adapted to the wavelet transform of the green component by Yin et al. in [5]. In this case, the SVD of the chaotic scrambled watermark is embedded with additive scheme, into the SVD of the high frequencies subband components (LH, HL, HH). This method shows an improved resistance to some of the most common attacks as JPEG compression, cropping, median filtering, resizing, and additive Gaussian noise. Different approach is presented in [6] where the Discrete Fourier Transform-based watermarking scheme is applied to different color representations of the cover image (RGB, YUV, and YC_bC_r) to highlight the advantages and disadvantages of each color space. The color space YIQ, adopted in the NTSC color TV system, is considered in [7]: the watermark is embedded in the Discrete Wavelet Transform (DWT) of both Y and Q components. The system is robust against JPEG compression, filtering, cropping, and additive noise.

Discrete Cosine Transform (DCT) has also been used by several authors as a suitable watermarking domain. Among them, the scheme proposed by Ahmidi and Safabakhsh in [8] is based on the permutation and adaptation of the watermark before its embedding in the the middle DCT frequencies of a block of the image. Li and Xue in [9] redundantly embed the watermark into the DCT of the three color components (RGB) of the image by applying a Direct Sequence Spread Spectrum (DSSS) technique. This method grants robustness in case of transmission in noisy paths.

More recent and advanced methods consider the correlation among the color channels. Tsui et al. in [10] present two watermarking schemes. The first one inserts the watermark by performing the *spatiochromatic* Discrete Fourier Transform (SCDFT) in the CIE-L*a*b* color space. To satisfy the invisibility constraint the characteristics of the Human Visual System (HVS) are exploited. The second scheme they propose operates in the L*a*b* color space by using the Quaternion Fourier transform. Both schemes are resistant to different attacks. As can be noticed, all the methods are using some sort of scrambling to increase the security of the system. In the following we review some works that are going further in this direction, by adopting also cryptographic techniques.

2.2. Watermarking and Encryption. Different methods have been proposed to protect digital data exploiting the advantages of encryption and watermarking techniques. Noncommutative schemes are usually proposed: either is the cipher text used as secret information to be embedded or a watermarked document is ciphered and deciphered by an authorized user.

Puech and Rodrigues [11] encrypt the secret key with an encryption method based on public-private keys. Then, this secret key is embedded in the encrypted image by using a DCT based watermarking method. The same authors in [12] propose a lossless joint crypto-data hiding method for medical image in which the image is decomposed in bit planes: the first semipixel image (the four Most Significant Bit planes) is compressed with a similar Run Length Encoding algorithm and stenographed with the patient information; then, this image is ciphered with a secret-key and scrambled with the remaining semipixel image (the four Least Significant Bit (LSB) planes).

In [13] an hybrid image protection algorithm is proposed. A prepositioned secret sharing scheme is used to reconstruct encryption secret keys by communicating different activating shares. The activating share is used to carry copyright or usage rights data that are embedded in the content as a visual watermark. An SVD-based watermarking scheme is used to insert the watermark. When the encryption key needs to be changed, the data source generates a new activating share and embeds the corresponding watermark into the multimedia stream. Before transmission, the composite stream is encrypted with the key constructed from the new activating share. Once both the activating share and the encrypted content are obtained, each receiver is able to reconstruct the decryption key, decrypt the content, and extract the watermark.

In [14] the image is divided into blocks of size 16 × 16 pixels and the DCT of each block is computed. The watermark is embedded into the encrypted LSBs of High-DCT-data (the highest and the second highest frequency coefficients) of each block in order to replace one bit every 8 with one bit of the watermark; the encryption is performed with RSA [15] algorithm by using a private key. Then the watermarked encrypted LSBs are decrypted using the corresponding private key and then the watermarked DCT coefficients are obtained combining High-DCT-data with original Low-DCT-data. On the contrary, in [16] the authors propose to decompose an image in the Discrete Wavelet Transform, to cipher the subbands in the lowest level with Advanced Encryption Standard (AES), a NIST-standard cryptographic block cipher [17], to cipher the subbands in the high level with sign encryption, and to encrypt and to watermark at the same time the subbands in the middle level. Lian et al. in [18] recently designed a combined approach also for video encryption and watermarking.

Recently the authors proposed a novel watermarking and encryption method for color images, exploiting the Fibonacci Haar Transform (FHT) as suitable domain for the embedding [19]. Starting from those preliminary results, in this contribution we go further, by performing extensive tests on a database of color images. Moreover, the performances are evaluated by computing the mutual information between the original watermark and the extracted one. In this work an optimization of the parameters used for the simulations and the performances evaluation have been analyzed. Furthermore, in this contribution a novel formulation for the Fibonacci-Haar transform is introduced.

3. Proposed Method

Our goal is to create a joint embedding-encryption scheme to allow watermark insertion and extraction without interfering with the encryption scheme and vice versa. To increase the security of the method, a key-dependent transform domain, the Fibonacci-Haar transform, is used for both procedures. We summarize the properties of the selected transform in the next subsection. The crucial point is that no operation like watermark embedding or detection as well as encryption and decryption can be performed without the knowledge of the secret key used to perform the subbands decomposition. The embedding is based on SVD of the Fibonacci-Haar subband decomposition because of the well-known SVD properties: stability, scale invariance, rotational invariance, translation, and transposition invariance, which are suitable to counteract attacks like rotation, scaling, noise addition, and others.

3.1. Fibonacci-Haar Transform Domain. The Fibonacci-Haar transform is a generalization of the Haar transform [20] in which the subband decomposition depends on the particular Fibonacci *p-sequence* $F_p(n)$ defined by the following recursive formula:

$$F_p(n) = \begin{cases} 0, & n < 0; \\ 1, & n = 0; \\ F_p(n-1) + F_p(n-p-1), & \text{otherwise.} \end{cases} \tag{1}$$

Different values of p define different *p-sequences*. For example, if $p = 0$, we have the sequence of Fibonacci *0-numbers*:

$$1, 2, 4, 8, 16, 32, 64, 128, 256, \ldots, \tag{2}$$

that is, the sequence of power of two. If $p = 1$, the Fibonacci *1-numbers* are obtained:

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots, \tag{3}$$

that is, the classical Fibonacci sequence. It can be demonstrated [21] that, by using a Fibonacci *p-sequence*, with $p \geq 0$, any positive natural number N can be always represented as follows:

$$N = \sum_{i=p}^{n-1} c_i F_p(i), \tag{4}$$

where $c_i = \{0, 1\}$, n is the number of bits needed to represent N with the chosen *p-sequence* , and $F_p(i)$ are the generalized Fibonacci *numbers*.

These sequences have been used to define the Fibonacci-Haar transformation matrices $H^{(p,n)}$, as in (5),

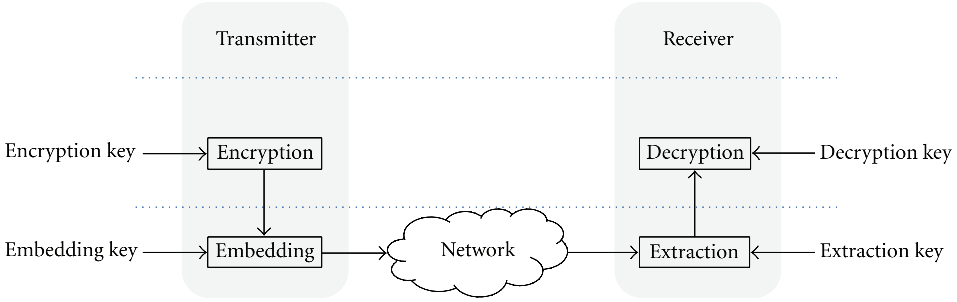


FIGURE 2: Layered security approach.

$$H^{(p,n)} = \begin{bmatrix} \overline{H}^{(p,n-p-1)} & 0_{F(p,n-p-2)\times F(p,n-p-2)} \\ 0_{[F(p,n-p-1)-F(p,n-p-1)]\times F(p,n-p-1)} & \overset{\frown}{H}^{(p,n-p-2)} \\ \widehat{H}^{(p,n-p-1)} & 0_{[F(p,n-p-1)-F(p,n-p-2)]\times F(p,n-p-2)} \\ 0_{[F(p,n-p-2)-F(p,n-p-3)]\times F(p,n-p-1)} & \widetilde{H}^{(p,n-p-2)} \end{bmatrix} \tag{5}$$

where, for $n \le p$, $H^{(p,n)} = [1]$, $H^{(p,p+1)} = \left[\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right]$, $\overline{H}^{(p,n-p-1)}$ is a rectangular matrix obtained from $H^{(p,n-p-1)}$ by taking its first $F(p,n-p-2)$ rows, that is,

$$\overline{H}_{i,j}^{(p,n-p-1)} = H_{i,j}^{(p,n-p-1)}, \quad i = 1,\dots,F(p,n-p-2), \tag{6}$$

for $i = 1,\dots,F(p,n-p-2)$, $j = 1,\dots,N$; and $\overline{H}^{(p,n-p-2)}$ is a rectangular matrix obtained from $H^{(p,n-p-2)}$ by taking its first $F(p,n-p-1) - F(p,n-p-2)$ rows:

$$\overset{\frown}{H}_{i,j}^{(p,n-p-2)} = H_{i,j}^{(p,n-p-2)}, \tag{7}$$

for $i = 1,\dots,F(p,n-p-1) - F(p,n-p-2), j = 1,\dots,N$; and $\widehat{H}^{(p,n-p-1)}$ is a rectangular matrix obtained from $H^{(p,n-p-1)}$ by taking the last $F(p,n-p-1) - F(p,n-p-2)$ rows:

$$\widehat{H}_{i,j}^{(p,n-p-1)} = H_{i,j}^{(p,n-p-1)}, \tag{8}$$

for $i = N - F(p,n-p-1) - F(p,n-p-2) + 1,\dots,N, j = 1,\dots,N$; and $\widetilde{H}^{(p,n-p-2)}$ is a rectangular matrix obtained from $H^{(p,n-p-2)}$ by taking the last $F(p,n-p-2) - F(p,n-p-3)$ rows:

$$\widetilde{H}_{i,j}^{(p,n-p-2)} = H_{i,j}^{(p,n-p-2)}, \tag{9}$$

for $i = N - F(p,n-p-2) - F(p,n-p-3) + 1,\dots,N,\ j = 1,\dots N$; and $0_{q\times r}$ is a $(q \times r)$ zero matrix.

Given a column vector $\mathbf{x}$ of size N, its Fibonacci-Haar transform $\mathbf{t}$ is

$$\mathbf{t} = H^{(p,n)}\mathbf{x}. \tag{10}$$

The *p-sequence* used in the embedding process is the secret key which is crucial for the security of the method. For example, the number 256 is the 46th element of the 24-*sequence*, the 66th element of the $p = 45$ sequence, and the 9th element of the 0-*sequence* (corresponding to the classical Haar decomposition).

As illustrated in Figure 3, for the two images Lighthouse and Parrot, the decompositions vary with p.

In general, if the cover image size is $N \times N$, where N is a Fibonacci number, the subband sizes are

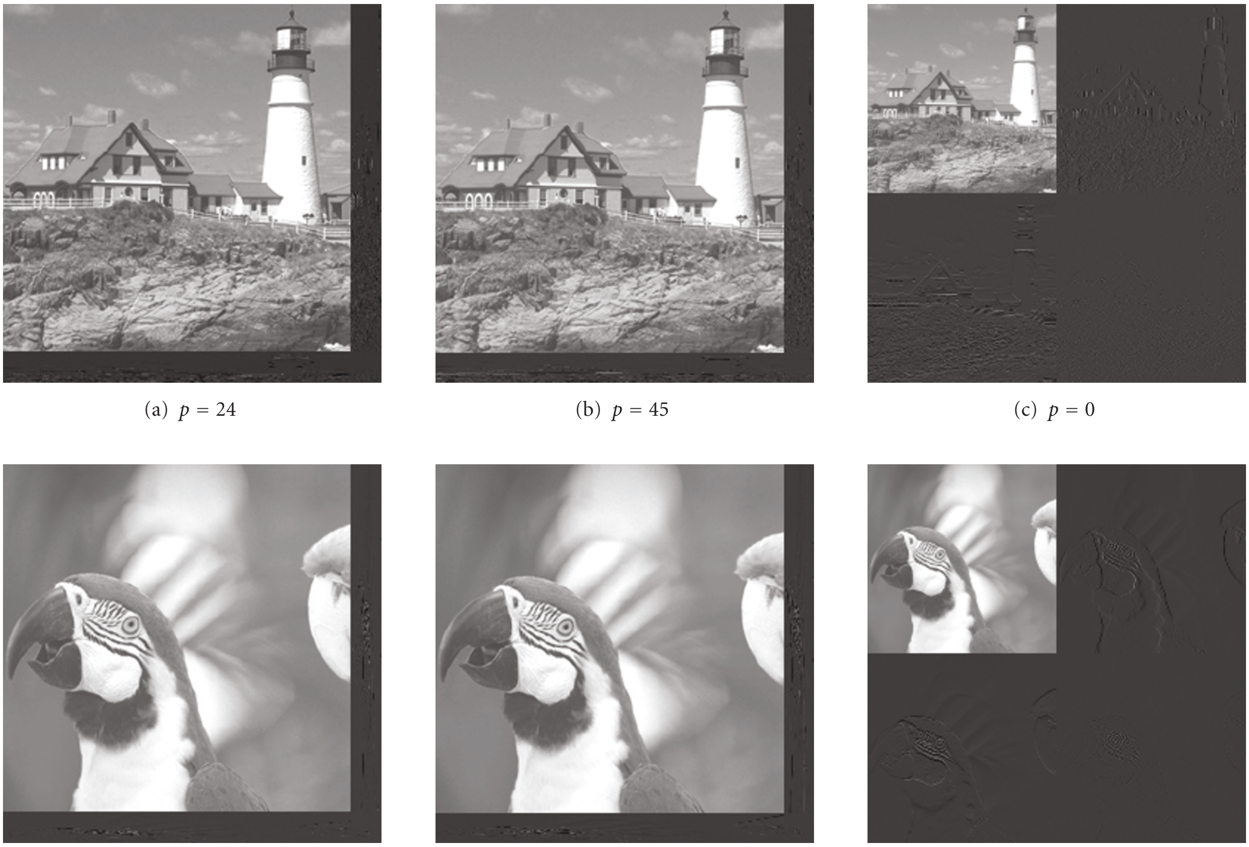
$$\begin{aligned} LL &: N_{n-1} \times N_{n-1} \text{ pixels}, \\ LH &: N_{n-1} \times N_{n-p-1} \text{ pixels}, \\ HL &: N_{n-p-1} \times N_{n-1} \text{ pixels}, \\ HH &: N_{n-p-1} \times N_{n-p-1} \text{ pixels}, \end{aligned} \tag{11}$$

where N_{n-1} is the number preceding N in the *p-sequence* and N_{n-p-1} is the number in $p-1$ positions before N in that sequence.

For instance, for an image of size 256 × 256 pixels decomposed by using the 24-*sequence*, the sizes of the four subbands are LL : 235 × 235, LH : 235 × 21, HL : 21 × 235, and HH : 21×21, respectively, since the Fibonacci-Haar 24-sequence is

$$\begin{gathered} 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, \\ 20, 21, 22, 23, 24, 25, 26, 28, 31, 35, 40, 46, 53, 61, 70, 80, \\ 91, 103, 116, 130, 145, 161, 178, 196, 215, 235, 256, \dots \end{gathered} \tag{12}$$

3.2. Watermarking Insertion and Encryption. Let us consider a color image X and let us denote by X_c, where $c = R, G, B$, its



(a) $p = 24$

(b) $p = 45$

(c) $p = 0$

(d) $p = 24$

(e) $p = 45$

(f) $p = 0$

Figure 3: First-level decomposition of the Lighthouse and Parrot images: (a)-(d) $p = 24$, (b)-(e) $p = 45$, and (c)-(f) $p = 0$.

color components. In the following we will use the subscript c to denote the generic color component. We propose to perform both watermarking and encryption of each color component in the Fibonacci-Haar transform domain. Let the watermark W be a binary sequence of length N_w. To increase the security of the watermarking system, W is spread in the three color components, namely, W_R, W_G, and W_B. In this way even if an attacker succeeds in deciphering one color component, he will not get enough information to extract or to modify the whole watermark.

The embedding-encryption procedure, performed on each X_c, can be summarized as follows (see Figure 4).

(1) The first-order decomposition of Fibonacci-Haar transform of X_c is computed according to the chosen p_c-*sequence* (different p_c-values can be used for each component). Let us indicate by $\mathcal{X}_c$ the correspondent transform.

(2) The LL_c subband is encrypted by using the symmetric block cipher AES with a 128-bit key.

(3) Each subband LH_c, HL_c, and HH_c of $\mathcal{X}_c$ is partitioned into B_c blocks of size $N_{n-p_c-1} \times N_{n-p_c-1}$ pixels, where

$$B_c = \left\lfloor \frac{N_{n-1}}{N_{n-p_c-1}} \right\rfloor \cdot 2 + 1, \tag{13}$$

$\lfloor z \rfloor$ denotes the largest integer smaller than z, and N_{n-1} and N_{n-p_c-1} are the larger and the smaller dimensions of LH_c and HL_c, respectively. For each color component B_c depends on the chosen p_c value.

(4) Each block is decomposed through the SVD. According to this representation every real matrix A can be expressed as product of three matrices:

$$A = USV^T, \tag{14}$$

where U and V are orthogonal matrices and S is a diagonal matrix whose singular values $\{s_1, \ldots, s_{N_{n-p_c-1}}\}$ are disposed in decreasing order. Since the largest singular values have a stronger impact on the perceived image quality, and the smallest ones are extremely sensitive to noise, we have selected the middle singular values $\{s_{l_c}, \ldots, s_{m_c}\}$ ($l_c > 1, m_c < N_{n-p_c-1}$) for watermark insertion. Notice that the maximum capacity N_{w_c} for each color component is given by

$$N_{w_c} = B_c(m_c - l_c + 1). \tag{15}$$

(5) For each block $A_i (i = 1, \ldots, B_c)$ the embedding is performed in the corresponding S_i diagonal matrix,

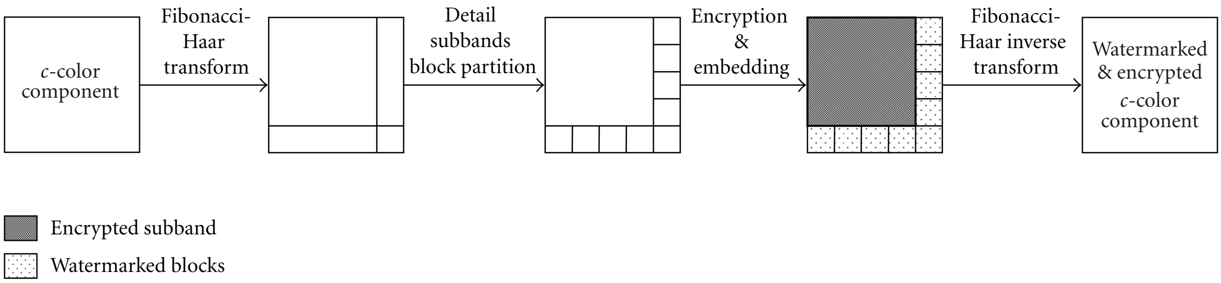
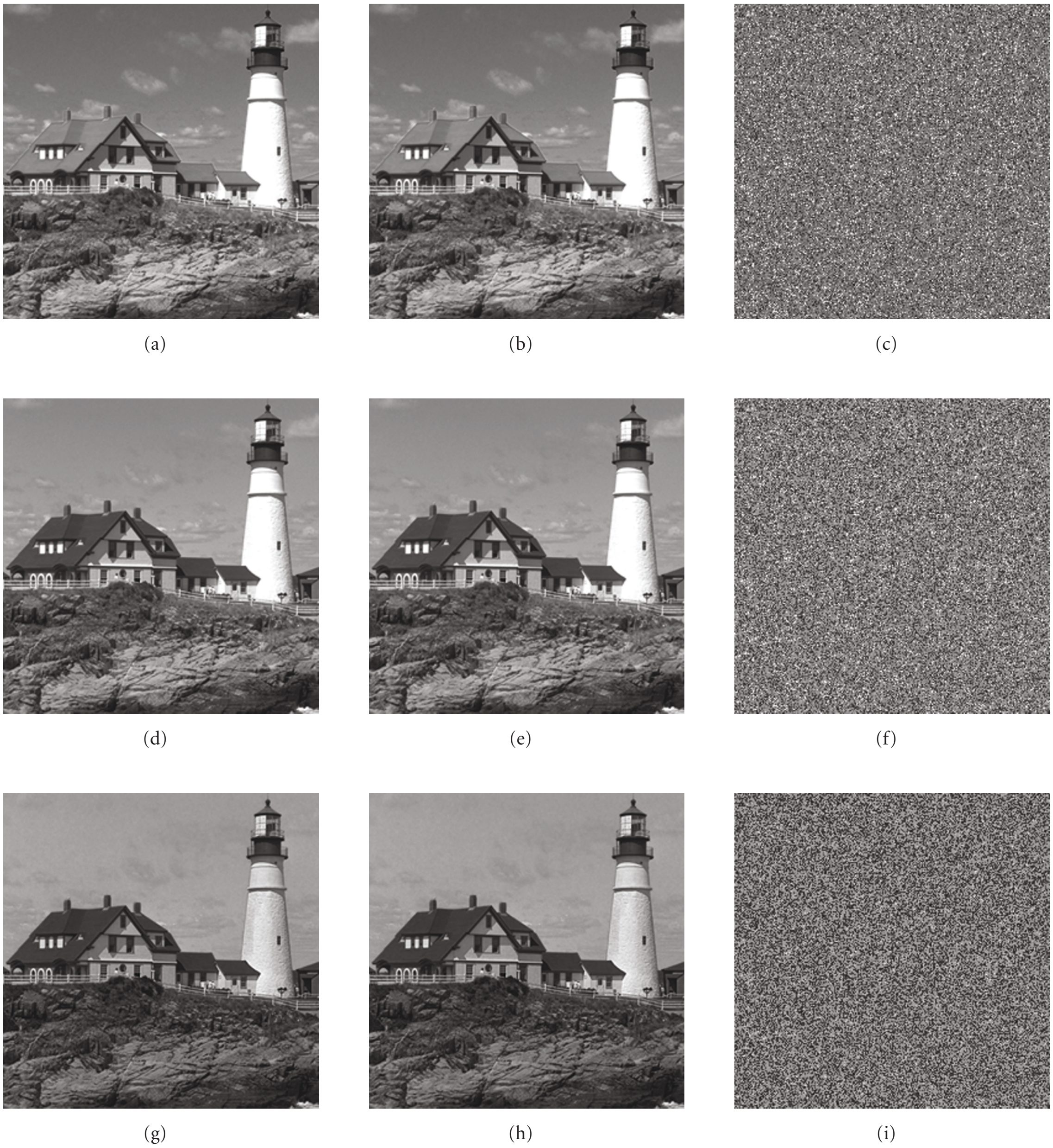

c-color component
Fibonacci-Haar transform
Detail subbands block partition
Encryption & embedding
Fibonacci-Haar inverse transform
Watermarked & encrypted *c*-color component
Encrypted subband
Watermarked blocks

Figure 4: Watermarking and encryption method for each color component.

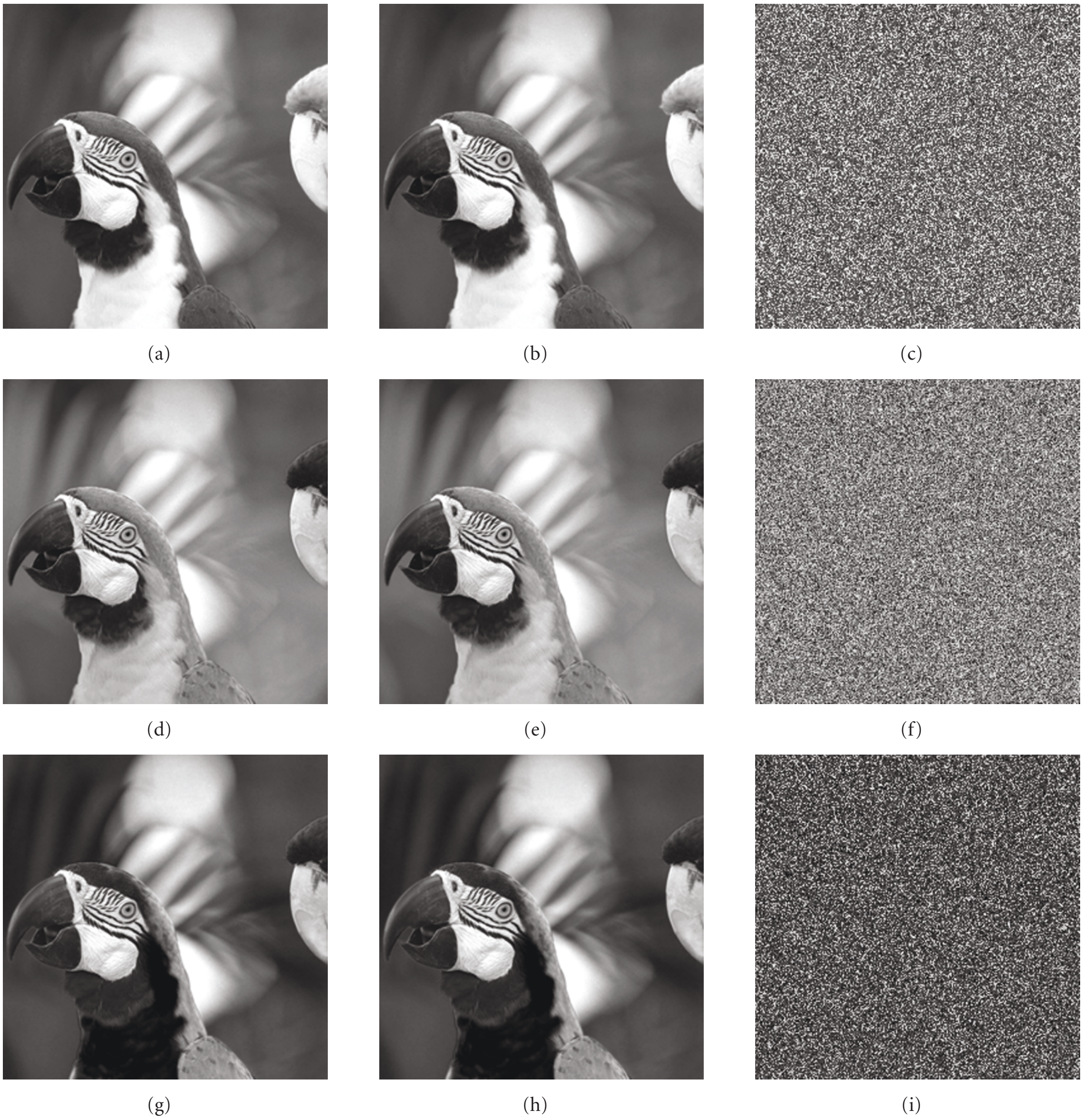


(a) (b) (c)

(d) (e) (f)

(g) (h) (i)

Figure 5: Color components of the Lighthouse image: original components (a),(d),(g), decrypted-watermarked components (b),(e),(h), and encrypted-watermarked components (c),(f),(i).


(a) (b) (c)

(d) (e) (f)

(g) (h) (i)

FIGURE 6: Color components of the Parrot image: original components (a),(d),(g), decrypted-watermarked components (b),(e),(h), and encrypted-watermarked components (c),(f),(i).

according to the SVD watermarking scheme proposed in [22]:

$$\begin{aligned}
&\widetilde{s}_{i_j} = s_{i_{j-1}} - 1.25\Delta, \quad \text{if } W_{c_{j+(i-1)(m_c-l_c+1)}} = 1,\ s_{i_{j-1}} - s_{i_j} < 1.25\Delta,\\
&\widetilde{s}_{i_j} = s_{i_j}, \quad \text{if } W_{c_{j+(i-1)(m_c-l_c+1)}} = 1,\ s_{i_{j-1}} - s_{i_j} > 1.25\ \Delta,\\
&\widetilde{s}_{i_j} = s_{i_{j-1}} - 0.25\Delta, \quad \text{if } W_{c_{j+(i-1)(m_c-l_c+1)}} = 0,\ s_{i_{j-1}} - s_{i_j} > 0.75\Delta,\\
&\widetilde{s}_{i_j} = s_{i_j} \quad \text{if } W_{c_{j+(i-1)(m_c-l_c+1)}} = 0,\ s_{i_{j-1}} - s_{i_j} \leq 0.75\Delta,
\end{aligned} \tag{16}$$

where s_{i_j} and $\widetilde{s}_{i_j}$ are the singular values of the original and watermarked block, respectively, $j = l_c, \ldots, m_c$, and Δ is the selected detection threshold.

(6) Find the smallest singular value $a = \widetilde{s}_{i_z}$, with $l_c < z < m_c$; in order to maintain the decreasing order of the singular values, find the first $b = s_{i_h} < a$, where $h > m_c$. Replace the singular values $[s_{i_{z+1}}, s_{i_{h-1}}]$ by linear interpolation between a and b.

(7) The inverse SVD of each block is computed.

(8) The inverse Fibonacci-Haar is computed according to the p_c-sequence in order to obtain the c component of the watermarked-encrypted image.

Figures 5 and 6 show the RGB components before and after the encryption-watermarking process for the two images Lighthouse and Parrot.

3.3. Watermarking Extraction and Decryption. The extraction of the watermark and the decryption procedures are performed individually by analyzing the RGB components of the watermarked-encrypted image $\widehat{X}$. The following steps are performed on each color component $\widehat{X}_c$.

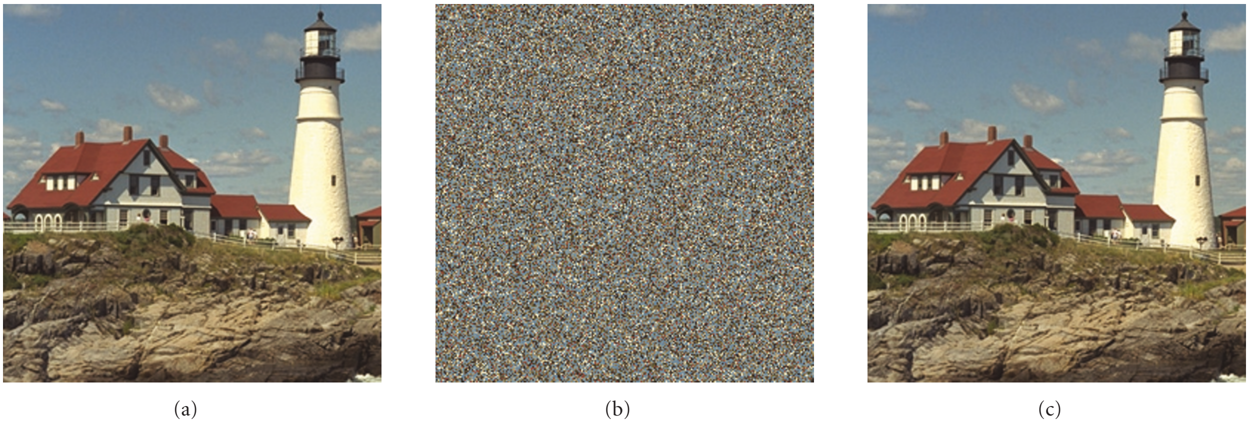


Figure 7: Visual impact of the proposed encryption-watermarking scheme for the image Lighthouse: (a) original image; (b) encrypted-watermarked image; (c) decrypted-watermarked image.

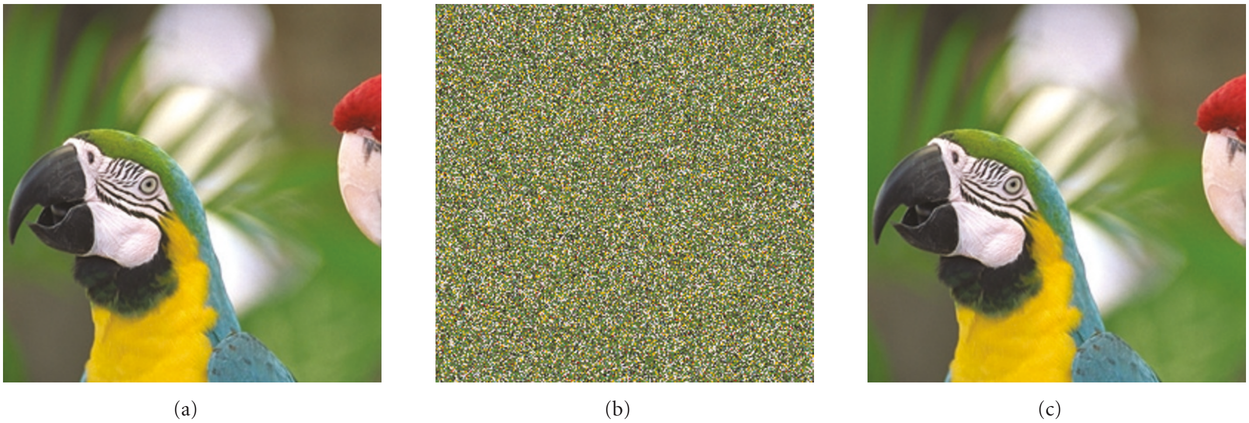


Figure 8: Visual impact of the proposed encryption-watermarking scheme for the image Parrot: (a) original image; (b) encrypted-watermarked image; (c) decrypted-watermarked image.

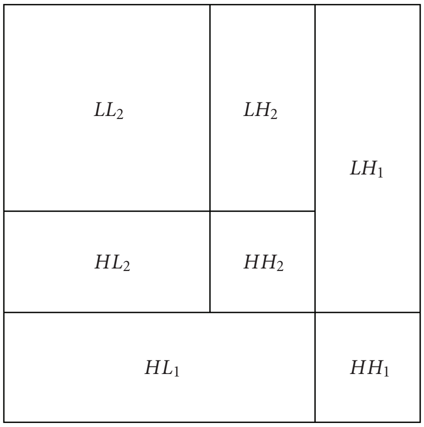


Figure 9: Second Level FHT Decomposition.

(1) The first-order Fibonacci-Haar decomposition is performed according to the secret key p_c yielding to $\widehat{\mathcal{X}}_c$, which allows the receiver to recover the Fibonacci sequence used in the embedding-encryption procedure.

(2) The $\widehat{LL}_c$ subband undergoes an inverse AES performed with the shared 128-bits secret key.

(3) Subbands $\widehat{LH}_c$, $\widehat{HL}_c$, and $\widehat{HH}_c$ are partitioned into the B_c blocks as described in Section 3.2 and each block is decomposed through the SVD. The watermark $\widehat{W}_c$ is extracted from the singular values of each block as follows:

$$\begin{aligned} &\text{if } \hat{s}_{i_{j-1}} - \hat{s}_{i_j} > \Delta, \qquad \widehat{W}_{c_{j+(i-1)(m_c-l_c+1)}} = 1, \\ &\text{if } \hat{s}_{i_{j-1}} - \hat{s}_{i_j} \leq \Delta, \qquad \widehat{W}_{c_{j+(i-1)(m_c-l_c+1)}} = 0, \end{aligned} \tag{17}$$

where $i = 1, \ldots, B_c$, $j = l_c, \ldots, m_c$, and Δ is the detection threshold.

(4) The three extracted watermark components $\widehat{W}_c$ are combined recovering $\widehat{W}$.

4. Experimental Results

In this section we show the results obtained in our experimental tests. In particular, our aim is to show that the

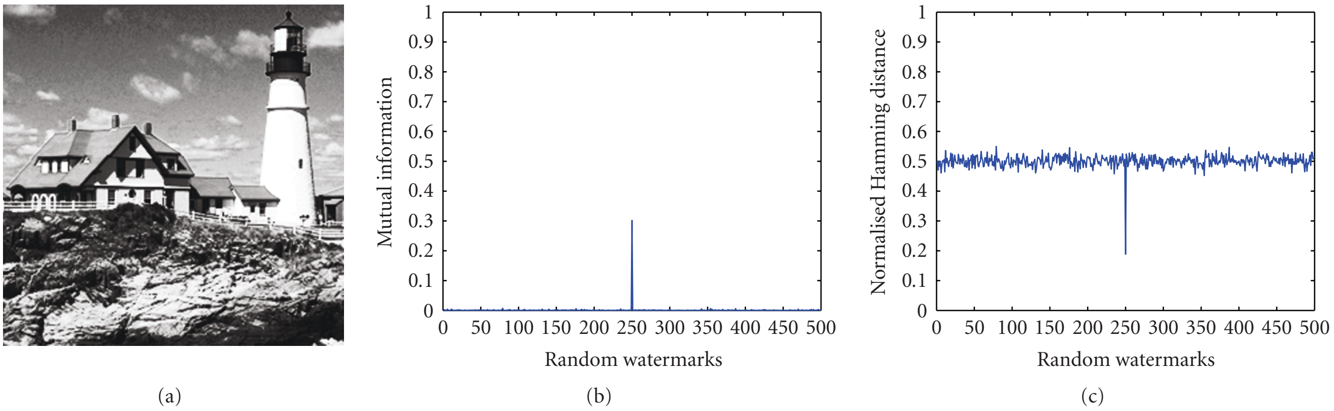


FIGURE 10: Equalization attack tested on a dictionary of 500 randomly generated watermarks: (a) red component after equalization attack; (b) mutual information; (c) normalized Hamming distance.

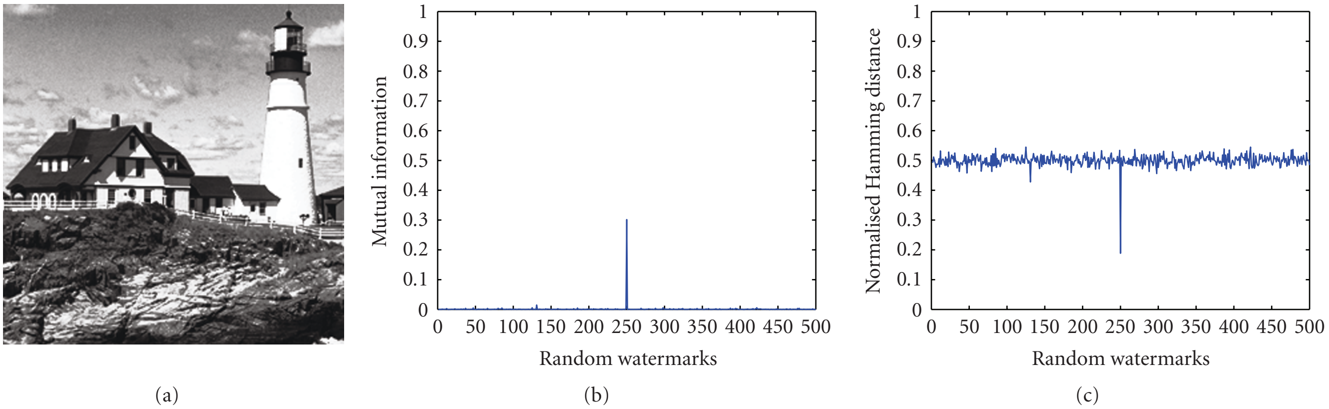


FIGURE 11: Equalization attack tested on a dictionary of 500 randomly generated watermarks: (a) green component after equalization attack; (b) mutual information; (c) normalized Hamming distance.

proposed method is compliant with both the robustness and the invisibility constraints.

The experimental tests have been performed on 25 color images (256 × 256 pixels) that have been extracted from the database freely available on the Internet (25 reference images, 17 types of distortions for each reference image, 4 levels for each type of distortion) [23, 24]. The watermark is a pseudorandom binary matrix generated by a secret seed.

4.1. Watermark Invisibility. In the design of a watermarking scheme there is always the need to find the best tradeoff between capacity and perceived quality of the watermarked data. In particular, considering color images, subjective tests show that the human perception is less annoyed by artifacts introduced in the blue component of the RGB color space [25]. A possible motivation lies in the higher spatial and temporal sensitivity of the red-green (Long-Middle wavelength regions) opponent mechanism with respect to the blue-yellow mechanism. Based on this consideration, since the proposed method allows to select the amount of data that can be embedded inside the color components of the host image, we have inserted a larger part of the watermark in the blue component.

The p_c-*sequences* used in the reported results are $p_R = 45$, $p_G = 24$, and $p_B = 0$. This choice allows to decompose each color component in blocks:

(i) the decomposition corresponding to $p_R = 45$ allows to obtain 23 blocks; in each block we set $l_R = 2$, $m_R = 17$, and $\Delta = 10$;

(ii) the decomposition corresponding to $p_G = 24$ allows to obtain 23 blocks; in each block we set $l_G = 2$, $m_G = 17$, and $\Delta = 10$;

(iii) the decomposition corresponding to $p_B = 0$ allows to obtain 3 blocks; in each block we set $l_B = 10$, $m_B = 105$, and $\Delta = 10$.

To allow the reader to visually verify the perceptual quality of the decrypted-watermarked images, in Figures 7 and 8 we report the original, the encrypted-watermarked, and the decrypted-watermarked images for two cases extracted from the cited database (images Lighthouse and Parrot). The encryption of the most perceptually significant subbands LL_c results in an image that is nonintelligible. The Fibonacci-Haar decompositions obtained with the selected p_c are shown in Figure 3 for both images.

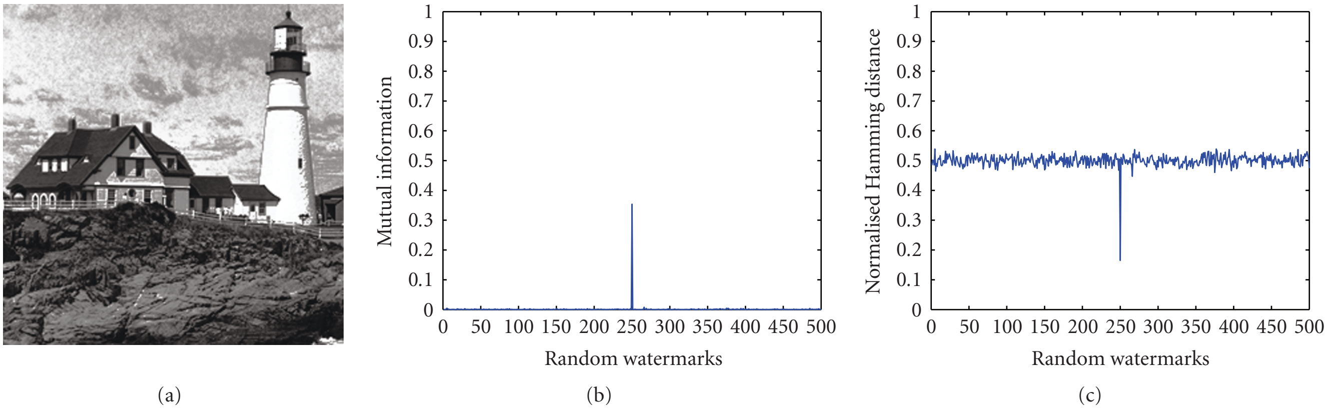


Figure 12: Equalization attack tested on a dictionary of 500 randomly generated watermarks: (a) blue component after equalization attack; (b) mutual information; (c) normalized Hamming distance.

Table 1: Quality evaluation of the watermarked components.

	R component		*G* component		*B* component	
	PSNR (dB)	WPSNR (dB)	PSNR (dB)	WPSNR (dB)	PSNR (dB)	WPSNR (dB)
Lighthouse	42	27	42	28	55	57
Parrot	45	30	44	31	55	49

In the performed experiments the first-order FHT decomposition has been employed, since it is the best trade-off between intelligibility of the ciphered data and perceptual quality of the watermarked data. This is due to the fact that when the FHT decomposition order increases, the size of the LL subband (the amount of information encrypted) decreases while the embedding capacity increases. In the performed simulations we have exploited the maximum embedding capacity, according to (15), for an image of size 256 × 256 pixels, by embedding a watermark of size 32 × 32 pixels.

To evaluate the watermark invisibility in the decrypted-watermarked images, the Peak Signal-to-Noise Ratio (PSNR) and the Weighted Peak Signal-to-Noise Ratio (WPSNR) have also been computed. The WPSNR is a modified version of the PSNR suggested in [26]. This objective quality metric is based on the computation of a Noise Visibility Function (NVF) which depends on a texture masking function. Following [26] we adopt a Gaussian model for estimating the amount of textures in an area of the image. The values of NVF are in the range zero (for extremely textured areas) to one (for smooth areas). The WPSNR can be computed as follows:

$$\text{WPSNR (db)} = 10 \log_{10}\left(\frac{L^2}{\text{NVF} \times \text{MSE}}\right), \qquad (18)$$

where L represents the maximum luminance value of the images (255 for 8 bit of representation) that are compared, and MSE is the Mean Square Error.

The perceptual impact of the watermark insertion in the test images Lighthouse and Parrot, in absence of attacks, is shown in Table 1. As can be noticed the PSNR and WPSNR show good performances concerning the imperceptibility requirement. Figures 7(c) and 8(c) show the decrypted-watermarked image. In this work we have also tested the possibility to recursively apply the FHT to the original image to increase the embedding capacity. For example, the second level decomposition results in a smaller *LL* subband and in six middle-high-frequency subbands (as shown in Figure 9).

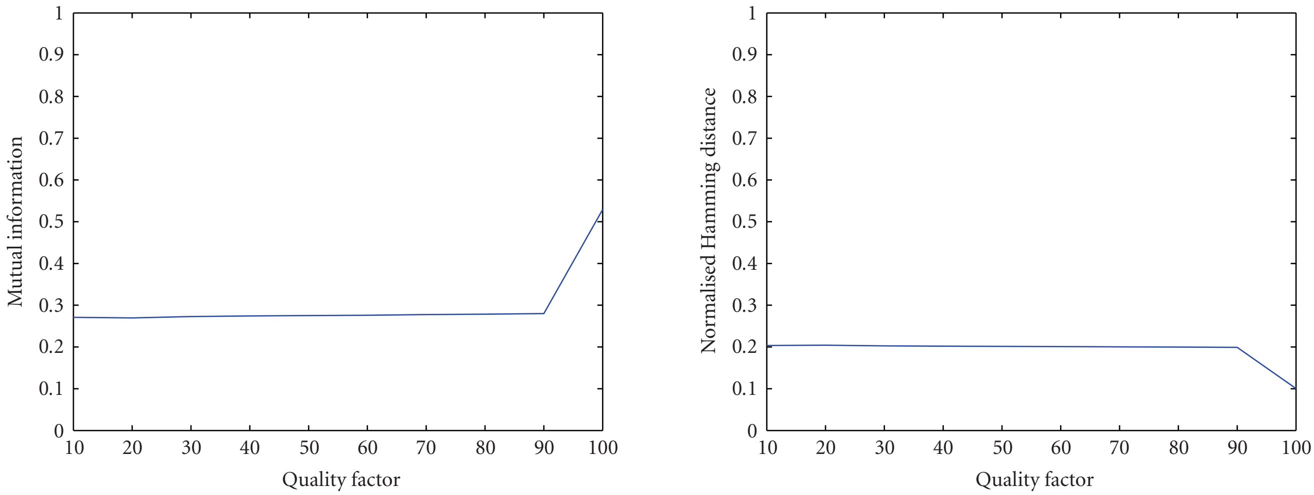
Experimental results show that the encryption effectiveness is preserved since it is not possible to visually understand the image content; moreover a smaller *LL* subband corresponds to an increased embedding capacity. The quality of the deciphered-watermarked image is still good. The average PSNR value for the three color components on the whole database, when the maximum capacity is used (56 × 34 bits for a 256 × 256 pixel image), is around 45 dB.

4.2. Robustness.

To evaluate the robustness of the embedding method we used the Stirmark [27] system to attack the watermarked images. Three kinds of attacks have been performed: each addressing a single color component. This choice is motivated by the fact that it is infeasible for an attacker to recover all the keys needed for joint decryption and watermark extraction from each component X_c. Simulations show similar performances for the three color components when the same attack is performed.

As an example of this common behavior in Figures 10, 11, and 12, the results obtained for the equalization attack on the image Lighthouse are reported.

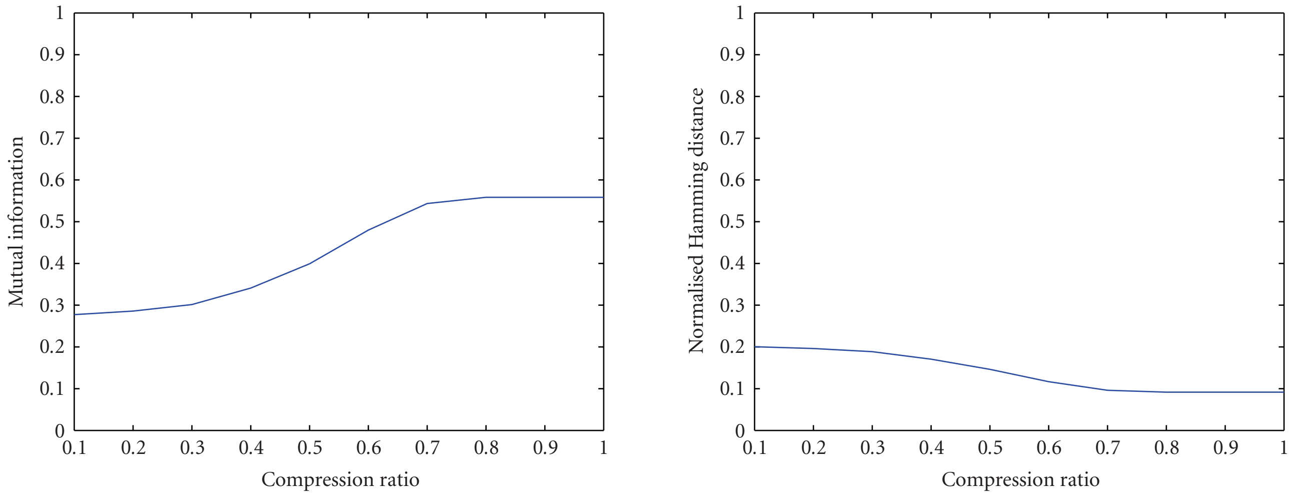
In the plots the Hamming distance $d_H(\widehat{W}, W)$ between the watermark $\widehat{W}$ extracted from the attacked image and the original watermark W, normalized with respect to the watermark size, is compared to the the Hamming distance $d_H(\widehat{W}, V^{(i)})$ between $\widehat{W}$ and the elements $V^{(i)}$, where $i = 1, \dots, 500$, of a watermark dictionary randomly generated. It



(a)

(b)

Figure 13: Detector response to JPEG compression attack: (a) mutual information; (b) normalized Hamming distance.



(a)

(b)

Figure 14: Detector response to JPEG2000 compression attack: (a) mutual information; (b) normalized Hamming distance.

can been noticed that, for all the three attacks, $d_H(\widehat{W}, W)$ is rather smaller than $d_H(\widehat{W}, V^{(i)})$, where $i = 1, \dots, 500$, thus assuring very good watermark detection performance. For completeness the mutual information $I(\widehat{W}, W)$ between $\widehat{W}$ and W, and the mutual information I$(\widehat{W}, V^{(i)})$ between $\widehat{W}$ and $V^{(i)}$ are plotted. For the mutual information between two binary i.i.d sequences X and Y of the same length M, the following formula has been applied:

$$\begin{aligned} I(X,Y) &= E_{X,Y}\left[\log\frac{p(x,y)}{p(x)p(y)}\right] \\ &= 1 - \hat{P}\log\frac{1}{\hat{P}} - \left(1-\hat{P}\right)\log\frac{1}{1-\hat{P}}, \end{aligned} \tag{19}$$

where

$$\hat{P} = \frac{d_H(X,Y)}{M}. \tag{20}$$

We noticed that the highest peak corresponds to W while for the other random watermarks the mutual information is practically null.

As mentioned before, the behavior for the three color components is similar; therefore, in the following, we discuss the results obtained for the green component averaged over the whole database. Several attacks have been considered; for each manipulation, Table 2 reports the mutual information between the embedded watermark and the watermark

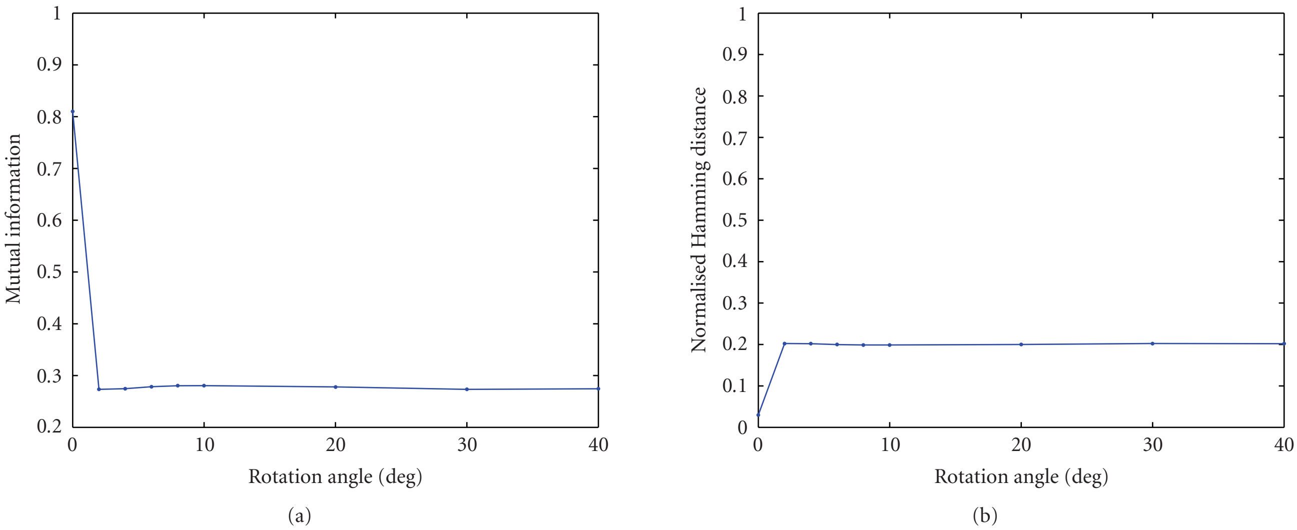


Figure 15: Detector response to rotation attack: (a) mutual information; (b) normalized Hamming distance.

Table 2: Mutual information values between the original watermark and the extracted one after attacks.

Attack	Parameters	Embedded
Gaussian	mean = 0, and standard deviation =1	0.29
Sharpening	3-by-3 contrast enhancement filter	0.28
Motion	linear motion of a camera by 10 pixels	0.27
Blurring	using a circular averaging filter within the square matrix of size = 5	0.26
Median	using a median filter within the square matrix of size = 3	0.28

extracted after the attack. For JPEG and JPEG2000 compression attacks the sensitivity of the mutual information to the compression ratio and quality factor has been assessed.

Results are, respectively, shown in Figures 13 and 14. In particular, quality factors from 10 to 100 with step 10 for JPEG, and compression ratios varying from 0.1 to 1 with step 0.1 for JPEG2000, have been employed. Mutual information between the detected watermark after decoding and 500 random watermarks is practically null and therefore has not been displayed. Even in this case, the presented values are the average values computed for the whole set of images contained in the database. Rotation attack has also been performed with rotation angle increasing from 0 to 40 degrees. In Figure 15 the average values of the mutual information are depicted. Once again mutual information between the restored watermark and 500 randomly selected watermarks is practically null.

Results show that it is always possible to extract the inserted watermark, thus verifying the robustness of the proposed method. As already stated, the proposed method is used to increase the security of the whole system, by further protecting the information with the data hiding technique, after the image decryption. The main security constraint is in the knowledge of the encryption keys used for the AES procedure. From a cryptoanalysis point of view, the strength of the whole procedure strictly depends on the security of the AES algorithm [28]. As mentioned before, once the encrypted and watermarked image has been decrypted, the content is still protected thanks to the watermark presence. To this aim the importance of the secret key p_c is crucial. To demonstrate this, we have extracted the watermark by choosing a different $\tilde{p}_c$ from the one used in the embedding-encryption procedure, and we have evaluated the performances in terms of mutual information between the original and the extracted watermark. For example, by using $\tilde{p}_R = 24$, $\tilde{p}_G = 0$, and $\tilde{p}_B = 45$ the mutual information value decreases from 0.92 (computed by using the correct p_c, that is $p_R = 45$, $p_G = 24$ and $p_B = 0$) to 0.03.

5. Conclusion

In this work we proposed a new joint watermarking and encryption technique for color images, which exploits the Fibonacci-Haar wavelet transform domain to increase its security. The three RGB color components are ciphered with the standard block cipher AES and watermarked via an SVD-based blind watermarking method. The intrinsic security of the method is in the AES scheme. Several experimental tests have been performed to verify the impact on the perceived quality of the watermark insertion and to verify the robustness of the adopted watermarking procedure.

The performances have been evaluated in terms of mutual information and normalized Hamming distance.

References

[1] A. Kerckhoffs, "La cryptographie militaire," *Journal des Sciences Militaires*, vol. 9, pp. 5–83, 1883.

[2] A. Kerckhoffs, "La cryptographie militaire," *Journal des Sciences Militaires*, vol. 9, pp. 161–191, 1883.

[3] I. J. Cox, G. Doërr, and T. Furon, "Watermarking is not cryptography," in *Proceedings of the 5th International Workshop on Digital Watermarking*, vol. 4283 of *Lecture Notes in Computer Science*, pp. 1–15, November 2006.

[4] Y. Xing and J. Tan, "A color watermarking scheme based on block-SVD and Arnold transformation," in *Proceedings of the 2nd Workshop on Digital Media and Its Application in Museum & Heritage (DMAMH '07)*, pp. 3–8, October 2007.

[5] C.-Q. Yin, L. Li, A.-Q. Lv, and L. Qu, "Color image watermarking algorithm R based on DWT-SVD," in *Proceedings of the IEEE International Conference on Automation and Logistics (ICAL '07)*, pp. 2607–2611, August 2007.

[6] R. Ridzon and D. Levicky, "Robust digital watermarking in color images," in *Proceedings of the 15th International Conference on Systems, Signals and Image Processing (IWSSIP '08)*, pp. 425–428, June 2008.

[7] G. Sun and Y. Yu, "DWT based watermarking algorithm of color images," in *Proceedings of the 2nd IEEE Conference on Industrial Electronics and Applications (ICIEA '07)*, pp. 1823–1826, May 2007.

[8] N. Ahmidi and R. Safabakhsh, "A novel DCT-based approach for secure color image watermarking," in *Proceedings of the International Conference on Information Technology: Coding Computing (ITCC '04)*, vol. 2, pp. 709–713, April 2004.

[9] X. Li and X. Xue, "Improved robust watermarking in DCT domain for color images," in *Proceedings of the International Conference on Advanced Information Networking and Application (AINA '04)*, vol. 1, pp. 53–58, March 2004.

[10] T. K. Tsui, X.-P. Zhang, and D. Androutsos, "Color image watermarking using multidimensional fourier transforms," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 1, pp. 16–28, 2008.

[11] W. Puech and J. Rodrigues, "A new crypto-watermarking method for medical images safe transfer," in *Proceedings of 12th European Signal Processing Conference (EUSIPCO '04)*, pp. 1481–1484, Vienna, Austria, September 2004.

[12] J. Rodrigues, W. Puech, and C. Fiorio, "Lossless crypto-data hiding in medical images without increasing the original image size," in *Proceedings of the 2nd International Conference on Advances in Medical Signal and Information Processing*, pp. 358–365, September 2004.

[13] X. Xu, S. Dexter, and A. Eskicioglu, "A hybrid scheme for encryption and watermarking," in *Security, Steganography, and Watermaking of Multimedia Contents VI*, vol. 5306 of *Proceedings of SPIE*, pp. 725–736, San Jose, Calif, USA, January 2004.

[14] K. Kuroda, M. Nishigaki, M. Soga, A. Takubo, and I. Nakamura, "A digital watermark using public-key cryptography for open algorithm," in *Proceedings of the 1st International Conference on Information Technology and Applications (ICITA '02)*, pp. 803–808, November 2002.

[15] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystem," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[16] S. Lian, Z. Liu, R. Zhen, and H. Wang, "Commutative watermarking and encryption for media data," *Optical Engineering*, vol. 45, no. 8, pp. 080 510.1–080 510.3, 2006.

[17] J. Deamon and V. Rijmen, *The Design of Rijndael. AES—The Advanced Encryption Standard*, Springer, 2002.

[18] S. Lian, Z. Liu, R. Zhen, and H. Wang, "Commutative encryption and watermarking in video compression," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 17, no. 6, pp. 774–778, 2007.

[19] F. Battisti, M. Cancellaro, M. Carli, G. Boato, and A. Neri, "Watermarking and encryption of color images in the Fibonacci domain," in *Image Processing: Algorithms and Systems VI*, vol. 6812 of *Proceedings of SPIE*, San Jose, Calif, USA, January 2008.

[20] K. Egiazarian and J. Astola, "Tree-structured Haar transforms," *Journal of Mathematical Imaging and Vision*, vol. 16, no. 3, pp. 269–279, 2002.

[21] V. Hoggatt, "Fibonacci and Lucas numbers," in *The Fibonacci Association*, 1969.

[22] J. Liu, X. Niu, and W. Kong, "Image watermarking based on singular value decomposition," in *Proceedings of the International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP '06)*, pp. 457–460, December 2006.

[23] N. Ponomarenko, V. Lukin, K. Egiazarian, J. Astola, M. Carli, and F. Battisti, "Color image database for evaluation of image quality metrics," in *Proceedings of the 10th IEEE Workshop on Multimedia Signal Processing (MMSP '08)*, pp. 403–408, October 2008.

[24] "Tampere Image Database 2008 TID2008," http://ponomarenko.info/tid2008.htm.

[25] G. R. Cole, T. Hine, and W. McIlhagga, "Detection mechanisms in L-, M-, and S-cone contrast space," *Journal of the Optical Society of America A*, vol. 10, no. 1, pp. 38–51, 1993.

[26] S. Voloshynovskiy, A. Herrigel, N. Baumgaertner, and T. Pun, "A stochastic approach to content adaptive digital image watermarking," in *Proceedings of the 3rd International Workshop on Information Hiding (IH '99)*, Dresden, Germany, September 1999.

[27] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, *Attacks on Copyright Marking Systems*, Springer, 1998.

[28] J. Nechvatal, E. B. L. Bassham, M. Dworkin, J. Foti, and E. Roback, "Report on the development of the advanced encryption standard (AES)," *Journal of Research of the National Institute of Standards and Technology*, vol. 106, no. 3, pp. 511–577, 2001.