

Article

Digital Watermarking Image Compression Method Based on Symmetric Encryption Algorithms

Yanli Tan ^{1,*} and Yongqiang Zhao ²

¹ Department of Electronic Engineering, Taiyuan Institute of Technology, Taiyuan 030008, China

² Science and Technology Division, Taiyuan Institute of Technology, Taiyuan 030008, China; zyqtyl@126.com

* Correspondence: whytyl0310@126.com

Received: 21 October 2019; Accepted: 2 December 2019; Published: 11 December 2019



Abstract: A digital watermarking image compression method based on symmetrical encryption algorithm is proposed in this study. First, the original image and scrambled watermarking image are processed by wavelet transform, and then the watermarking image processed by the Arnold replacement method is transformed into a meaningless image in the time domain to achieve the effect of encryption. Watermarking is generated by embedding the watermarking image into the important coefficients of the wavelet transform. As an inverse process of watermarking embedding, watermarking extraction needs to be reconstructed by the wavelet transform. Finally, the watermarking is extracted from the inverse scrambled watermarking image, and a new symmetrically encrypted digital watermarking image is obtained. The compression method compresses the embedded digital watermarking image, so that the volume of the compressed watermarking image is greatly reduced when the visual difference is very small. The experimental results show that the watermarking image encrypted by this method not only has good transparency, but also has strong anti-brightness/contrast attack, anti-shearing, and anti-noise performance. When the volume of the compressed image is greatly reduced, the root mean square error and visual difference measurement of the watermarking image are very small.

Keywords: symmetric encryption algorithm; digital watermarking image; compression method; wavelet transform; Arnold permutation; watermarking embedding

1. Introduction

The copyright information of digital works is embedded in the digital works through the digital watermarking system in the form of watermarking, which cannot be perceived by human beings. The embedded watermarking information can only be detected by some special software [1]. At present, the research of digital watermarking technology mainly focuses on the robustness of watermarking. Most algorithms use pseudo-random noise sequence to construct watermarking, and use a hypothesis test to detect whether watermarking exists in the image. That is, when the sequence extracted from the image has a strong correlation with the original watermarking, indicating that the image contains watermarking information; otherwise, it does not contain watermarking information. However, in many practical applications, the embedded image watermarking information is required to be more readable or visual, for instance, meaningful information (such as text, icon, or image). This meaningful watermarking has incomparable advantages of random sequence watermarking. Digital watermarking in the wavelet domain has become one of the research hotspots in recent years [2]. On one hand, the research of wavelet theory itself is becoming more and more mature and perfect. On the other hand, the application of the wavelet multi-resolution analysis method is becoming increasingly more extensive, especially in information processing. In the transform domain of digital watermarking image, some characteristics of human visual system (HVS) can be more conveniently integrated

into the watermarking algorithm, so that the privacy and robustness of embedded information can be improved.

Wavelet transform-based digital watermarking image algorithm is a common symmetric encryption algorithm. In recent years, the research into it has become more and more mature and perfected. The application of wavelet transform in signal and image compression has the advantages of a high compression ratio, fast compression speed, unchanged features of signal and image after compression, and anti-interference in transmission. There are many image compression methods based on wavelet transform [3], such as embedded zerotree wavelet (EZW), set partitioning in hierarchical trees (SPIHT), and adaptive scanning wavelet difference reduction (ASW-D). Moreover, wavelet transform is also widely used in signal analysis, including boundary processing and filtering, time-frequency analysis, signal-noise separation and extraction of weak signals, fractal index, signal recognition and diagnosis, and multi-scale edge detection.

Symmetrically encrypted digital watermarking image is a newly-emerged digital image technology, which can obtain and store all the color and brightness information of the original scene. With the improvement of CMOS (Complementary Metal Oxide Semiconductor) and CCD optical sensor production technology, the improvement of display performance, the reduction of storage device price, and the popularization of high-performance computing, there is no doubt that symmetrically encrypted digital watermarking images will be widely accepted. However, owing to the large amount of information of symmetrically encrypted digital watermarking image itself, its storage space is very large. At present, the digital watermarking hiding method for video image is basically noncompressed [4], which takes up a large amount of space, thus seriously limiting the wide application of symmetric encrypted digital watermarking image. The wavelet transform-based JPEG Z000 image compression standard highlights the advantages of wavelet transform in image compression [5]. In this paper, a digital watermarking image compression algorithm based on symmetric encryption of wavelet transform is designed, which greatly reduces the volume of compressed image (about 10% of the original image) when the visual difference is small.

Foreign scholars have carried out many studies on digital watermarking image compression. Meyer, Lemarie, and Battle independently presented the exponential attenuation wavelet function, which reduced the volume of the compressed image to three-tenths of the original image. In 1987, Mallat used the concept of multi-resolution analysis to unify. This paper proposes Mallat fast wavelet decomposition and the reconstruction algorithm, which is widely used nowadays; however, this proposed algorithm does not consider the instability of the traditional wavelet multi-resolution analysis method in embedding the watermarking image into the important coefficients of wavelet transform. Therefore, this paper proposes a digital watermarking image compression method based on the symmetric encryption algorithm. In the transform domain, this method can more easily integrate the characteristics of human visual system (HVS) into the watermarking algorithm, so that the privacy and robustness of the embedded information can be improved.

2. Algorithmic Definitions

2.1. Digital Watermarking Image Based on Symmetric Encryption

2.1.1. Wavelet Transform of Image

Wavelet transform is a symmetrical encryption algorithm as well as a variable resolution analysis method. It uses a small window to analyze high frequency signals and a large time window to analyze low frequency signals, which coincides with the time-frequency distribution characteristics of natural medium-high frequency signals. Therefore, it is very suitable for image processing [6].

As a new branch of mathematics, wavelet transform theory is a milestone development after Fourier transform [7], which can be used to solve many difficult problems that cannot be solved by Fourier transform. The application of Fourier transform in signal processing can well describe the frequency characteristics of signals, but cannot solve problems such as abrupt signal and non-stationary

signal. The basic idea of wavelet transform is to expand the signal into a weighted sum of a family of basic functions, that is, to express or approximate preferences or functions by a family of functions. This family of functions is composed of the translation and expansion of basic functions. Wavelet transform is the extension of Fourier transform, which is basically a local transformation of space (time) and frequency.

The wavelet transform has been intensively applied in image processing in recent years. The basic idea of image processing is to decompose the image into sub-images of different spatial and independent frequency bands, and then process the coefficients of sub-images, such as image compression, image enhancement, image decomposition, and reconstruction. According to the pyramid decomposition algorithm proposed by S. Mallat, four 1/4-size subgraphs are formed after first-order decomposition (low-frequency approximation subgraph LL1 with most of the image information; medium and high-frequency detail subgraphs HL1, LH1, and HHH1 with edge and texture information in the horizontal, vertical, and diagonal directions, respectively; and then the approximation subgraph LL1 with the complete phase) [8]. In the same way, the smaller subgraphs LL2, HL2, LH2, and HH2 at the next resolution are low-frequency approximation subgraphs, and HL2, LH2, and HH2 represent high-frequency detail subgraphs; LL2 is decomposed once more. After decomposition, 10 subgraphs are obtained (as shown in Figure 1), including HL1, LH1, and HH1 (Level 1); HL2, LH2, and HH2 (Level 2); and LL3, HL3, LH3, and HHH3 (Level 3). With the increase of decomposition series, the resolution decreases and the energy of wavelet coefficients increases. In other words, the resolution of the first level is the highest and the frequency is the highest, the resolution of the third level is the lowest and the frequency is the lowest, the energy of the wavelet coefficients of the first level is smaller than that of the second level, and the energy of the wavelet coefficients of the second level is smaller than that of the third level. The low frequency band represents the best approximation of the original image at the maximum scale and the minimum resolution determined by the decomposition series of the wavelet transform. Its statistical characteristics are similar to those of the original image [9], where most of the energy of the image is concentrated. The high frequency band part represents the edge and principle of the image. On the premise of ensuring better transparency (invisibility) of the watermarking, the location of the hidden watermarking information is selected in the third-level wavelet coefficients with the largest energy, which can achieve better robustness.

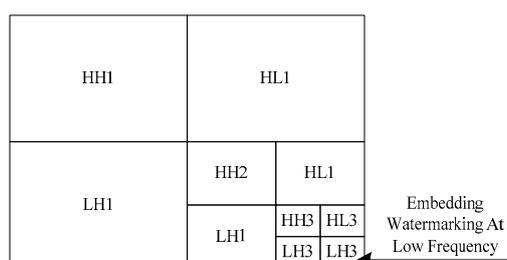


Figure 1. Image decomposition using three-level wavelet transforms.

HVS points out that human eyes are less sensitive to high-frequency information (such as complex areas) than to low-frequency information (such as smooth areas), so the more high-frequency watermarking is embedded, the less the impact on the original image, and the better the transparency of the watermarking. However, considering the robustness and distortion of the watermarking, the watermarking is embedded in the middle frequency band of the image [10]. When embedding image watermarking, Cox always excludes DC (Discrete Cosine) coefficients in order to avoid the block effect of watermarked image. This DCT (Discrete Cosine Transform) based embedding strategy is now well-accepted. However, as the wavelet transform is a global transform, adding watermarking to the low-frequency coefficients of the image will not produce the blocking effect.

The image embedded with watermarking is prone to image compression, filtering, and other processing. According to signal processing theory, low-frequency coefficients are less susceptible to

signal processing than high-frequency coefficients. Therefore, this paper proposes a method to embed the watermarking into the low-frequency coefficients of the wavelet image, which ensures both the reliability and stability of the image.

2.1.2. Watermarking Generation (Arnold Permutation)

The purpose of time domain transformation of watermarking image is to disorder the information of watermarking and achieve the effect of encryption [11]. The following functions are used:

$$A_N(k) : \begin{vmatrix} x' \\ y' \end{vmatrix} = \begin{vmatrix} 1 & 1 \\ k & k+1 \end{vmatrix} \begin{vmatrix} x \\ y \end{vmatrix} \pmod N, \quad (1)$$

where k is a control function; N is the size of the matrix; and (x, y) and (x', y') are the positions of the pixels before and after transformation, respectively. Let P represent an $m \times m$ matrix of binary watermarking information. After $A_N(k)$ transformation of the coordinates of each point, the matrix will become an $N \times N$ matrix. Each element of the matrix has a value of 0 or 1. As the transformation of $A_N(k)$ is periodic, the (x, y) can return to its original position after T transformations. Similarly, (i, j) point can be restored to their original positions after $T - n$ transformations. The watermark generation framework is shown in Figure 2.

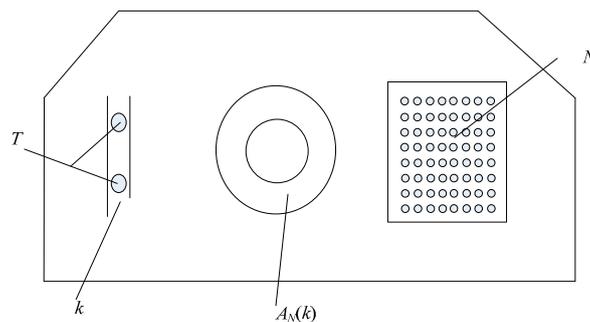


Figure 2. Schematic diagram of the watermark generation framework.

2.1.3. Watermarking Embedding and Extraction

(1) Watermarking Embedding Method

In order to improve the invisibility of watermarking information, the adaptive coefficient of watermarking is introduced to adjust the strength of watermarking. The series of wavelet decomposition is determined by the size of the original image and the watermarking information. Generally speaking, the original image should be decomposed by more than two levels of wavelet [12]. In the experiment, the original image is decomposed by three levels of wavelet, and the watermarking information is decomposed by one level of wavelet. The steps of the algorithm are as follows:

- (1) Arnold transform is used to scramble the watermarking image, and the scrambled watermarking is recorded as W_i .
- (2) The original image F is transformed by a three-level wavelet transform to obtain sub-images F_i^k in different directions at different resolutions.
- (3) W_i is decomposed into four subgraphs W_i^k by first-order wavelet decomposition.
- (4) The data in the watermarking and the data in the original image subgraph are coded in blocks according to the following formula:

$$C'_i = C_i(F_i^k + \alpha W_i^k) (k = 0, 1, 2, 3), \quad (2)$$

where C_i is the DWT coefficient before embedding, α is the wavelet strength parameter, W_i is the embedding watermarking, and C'_i represents the embedding watermarking. Subgraphs with

different intensities and in different directions allow the embedded watermarking to have a certain degree of self-adaptability.

(2) Watermarking extraction method

The extraction process of watermarking is basically the inverse process of embedding. When extracting watermarking, the original image is needed. Firstly, the original image and the watermarking image to be detected are processed by a three-level wavelet transform, and then the wavelet coefficients of the watermarking sub-image are compared [13]. According to the above formula, the wavelet coefficients of the watermarking sub-image are deduced, and the watermarking is reconstructed. Finally, the watermarking is extracted from the anti-scrambling watermarking image. The experimental results of watermarking embedding are shown in Figure 3.

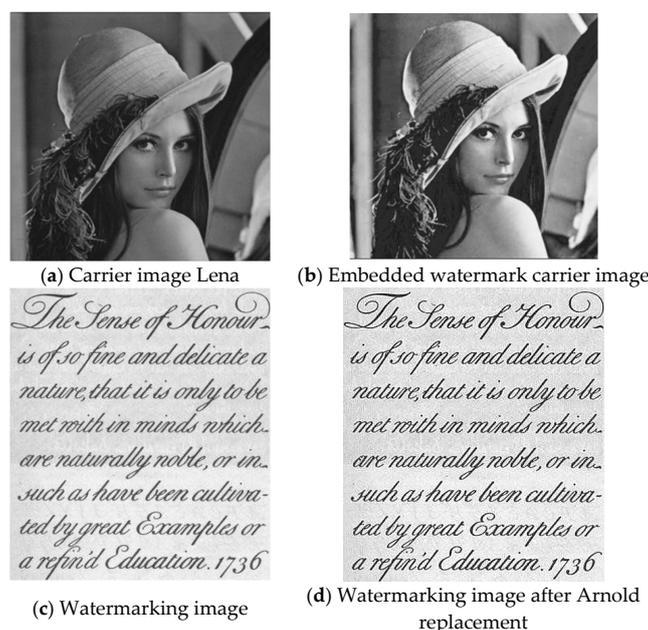


Figure 3. Experimental results of watermarking embedding.

2.1.4. Watermarking Detection

The original image is needed in the detection of this algorithm. If the image watermarking is not restored well, it is considered that the watermarking is damaged or even does not exist. The detection process is as follows:

The image $X'(i, j)$ to be detected and the carrier image $X(i, j)$ are transformed into 8×8 -pixel block DTC, then $F'_k(u, v)$ and $F_k(u, v)$ are obtained, where k represents the k image block. The absolute value of the five low-frequency coefficients in the DTC domain of the original image $X(i, j)$ is chosen as $F_{\max}(u, v)$, which is compared with the corresponding JND (Just Noticeable Distortion) threshold $T_k(u, v)$. If $F_{\max}(u, v)$ is greater than or equal to $T_k(u, v)$, the coefficient is obtained and watermarking is embedded; otherwise, no watermarking is embedded. For the coefficients embedded with watermarking, the k th watermarking signal W'_k is extracted according to Formula (3).

$$W'_k = \begin{cases} 1, & \text{if } |F'_k(u, v) - F_k(u, v)| \geq 0.61 \times T_k(u, v) \\ 0, & \text{if } |F'_k(u, v) - F_k(u, v)| < 0.61 \times T_k(u, v) \end{cases} \quad (3)$$

Then, the rotational transformation parameter L' is obtained by symmetrical decryption of the extracted watermarking sequence W' , which is combined with the remaining fractal feature parameters saved in the work of [14], and the gray image watermarking is restored using fractal image decoding technology.

After obtaining the digital watermarking image, the symmetrical encrypted digital watermarking image compression algorithm is adopted to realize the compression of the watermarking image.

2.2. Design of Symmetric Encryption Digital Watermarking Image Compression Algorithm

The symmetrically encrypted digital watermarking image has a wider application range than the ordinary image. Currently, one of the commonly used coding methods for symmetrically encrypted digital watermarking images is lossless coding, which occupies a larger storage space. For instance, a color symmetrically encrypted digital watermarking image (96-bit floating-point TIFF (Tag Image File Format) coding) with a size of 800×600 pixels occupies storage space of about 5.5 M Byte; in contrast, an uncompressed ordinary image (BMP (Bitmap) encoding) of the same size occupies about 1.4 M Byte. After lossy JPEG compression, it occupies about 0.05 M Byte (depending on compression rate and image content).

A typical web page may contain 10 or more images. If uncompressed images are used, the download time may be several minutes, which is obviously intolerable to users. Therefore, JPEG images are widely used in web design.

At present, lossless compression coding is the dominant coding scheme for symmetrically encrypted digital watermarking image. Despite the continuous improvement of Internet speed, at least in the visible future, such symmetrically encrypted digital watermarking image coding cannot be applied to web pages at all [15]. This paper designs a lossy compression algorithm for symmetrically encrypted digital watermarking image. Although lossy compression may lead to the loss of some details, the symmetrically encrypted digital watermarking image features are well preserved. It is hoped that this new coding scheme can be applied in future web page design.

The symmetrical encrypted digital watermarking image compression algorithm designed in this paper is inspired by the new international standard JPEG2000 for digital image compression. JPEG2000 is a compression standard prepared for the 21st century, which uses improved compression technology to provide a higher resolution. With the capacity of providing a variety of image quality and image selection from non-destructive to lossy for a file, JPEG2000 is considered to be an ideal image coding solution for Internet and wireless access applications.

“High compression, low bit rate” is the goal of JPEG2000. Under the same compression rate, the signal-to-noise ratio of JPEG2000 will increase by about 30% compared with that of JPEG. JPEG2000 has five levels of coding, including JPEG coding for color static picture, JBIG for two-value image. It has become a common coding method for all kinds of images. In coding algorithm, JPEG2000 uses discrete wavelet transform (DWT) and arithmetic coding). In addition, JPEG2000 can also send images with different resolutions and compression rates according to the user’s network transmission speed and mode of use (viewing on a personal computer).

JPEG2000 was initially formulated in March 1997, and the final draft agreement on the basic coding system was introduced March 2000. At present, JPEG2000 has been officially named “ISO15444” by ISO (International Organization for Standardization) and IEC (International Electro technical Commission). JTC1 SC29 Standardization Group is officially named “ISO15444”, and the basic part of JPEG2000 (Part1) has been published as an ISO standard.

The compression performance of JPEG2000 is 30%–50% higher than that of JPEG. That is to say, under the same image quality, JPEG2000 can reduce the size of image file by 30%–50% compared with that of the JPEG image file. At the same time, the system using JPEG2000 has good stability, stable operation, good anti-interference, and easy operation [16].

The biggest difference between JPEG2000 and traditional JPEG is that it abandons the block coding method based on discrete cosine transform adopted by JPEG, but adopts the multi-analytic coding method based on wavelet transform. Cosine transform is a classical spectral analysis tool, which investigates the frequency domain characteristics of the whole-time domain process or the time domain characteristics of the whole frequency domain process. Therefore, it has a good effect for stationary processes, but has many shortcomings for non-stationary processes. In JPEG, the discrete

cosine transform compresses the image into 8×8 blocks, and then puts them into the file in turn. This algorithm compresses the image by discarding the frequency information, so the higher the compression rate of the image, the more the frequency information is discarded. In extreme cases, JPEG images only retain basic information reflecting the appearance of the image, and fine image details are lost. Wavelet transform is a modern spectral analysis tool, which can investigate not only the frequency domain characteristics of local time domain processes, but also the time domain characteristics of local frequency domain processes. Therefore, it is applicable even for non-stationary processes. It can transform an image into a series of wavelet coefficients, so the image can be compressed and stored efficiently. In addition, the rough edge of the wavelet can better represent the image, because it eliminates the blocking effect commonly used in DCT compression. In recent years, discrete wavelet transform has been widely used in fields of image processing and image analysis because of time-frequency localization characteristics. Moreover, discrete wavelet transform can amplify arbitrary details as it uses a progressive sampling interval from coarse to fine for high-frequency components [17]. Therefore, wavelet analysis is praised as a mathematical microscope as well as a powerful tool to construct multi-resolution representation of images.

The compression algorithm is divided into five steps, including color space conversion, floating-point to integer conversion, discrete wavelet transform, quantization, and entropy coding.

(1) Color space conversion

In order to better balance the compression rate and image quality, the following criteria are used in the selection of color space:

The color space can express all color and brightness information visible to the naked eye.

The quantization step of the color space is just a noticeable difference.

Positive integers are used to express color and brightness information in order to improve the compression rate.

The correlation between different color channels is the smallest.

For a given pair of symmetrically encrypted digital watermarking images expressed in color space, its brightness channel Y is converted to luma, and the formula is as follows:

$$luma(Y) = \begin{cases} a \times Y & \text{if } Y \leq YL \\ b \times Y^c + d & \text{if } YL \leq Y \leq YH \\ e \times \log(Y) + f & \text{if } Y \geq YH \end{cases}, \quad (4)$$

where $a = 17.554$, $b = 826.81$, $c = 0.10013$, $d = -884.17$, $e = 209.16$, $f = -731.28$, $YL = 5.6046$, and $YH = 10469$.

The formula for conversion from luma to brightness Y is as follows:

$$Y(luma) = \begin{cases} a' \times L & \text{if } L \leq LL \\ b' \times (L + d')^{c'} & \text{if } LL \leq L \leq LH \\ e' \times \exp(f' \times L) & \text{if } L \geq LH \end{cases}, \quad (5)$$

where, $a' = 0.056968$, $b' = 7.3014e - 30$, $c' = 9.9872$, $d' = 884.17$, $e' = 32.994$, $f' = 0.0047811$, $LL = 98.38$, and $LH = 1204.7$.

This conversion function is shown in Figure 4. When the luminance range is from 1×10^{-4} cd/m² to 1×10^{10} cd/m² (candela per square meter), the output luma range is from 0 to 4000. When luma is taken as an integer, it can be expressed by 16-bit integers.

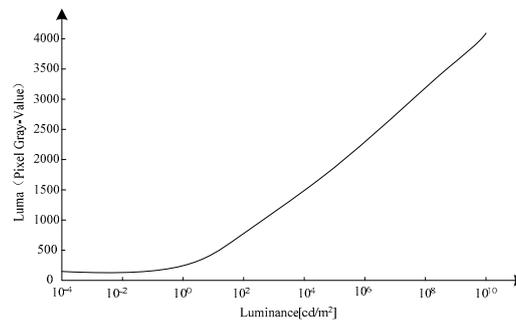


Figure 4. Functional mapping from brightness Y to luma.

As human eyes are more sensitive to brightness information than to color information, less bits (8 bits) are used to express color information [18]. In this paper, CIE (China Illuminating Engineering) 1976 uniform scale (u, v) is used to express color information. The transformation from XYZ space to CIE1976 uniform scale (u, v) is as follows:

$$\begin{cases} u = \frac{4X}{X+15Y+3Z} \\ v = \frac{9Y}{X+15Y+3Z} \end{cases} \quad (6)$$

(2) Conversion from floating point to integer

The conversion function in Figure 3 shows that the range of luma ranges from 0 to 4000, so the nearest neighbor integer method is adopted to express luma using 16-bit integers. The range of color information u, v is 0 to 0.62, which is multiplied by 410 and then expressed by an integer of 8.

(3) Discrete wavelet transform

The discrete wavelet transform in JPEG2000 is employed to carry out five-layer two-dimensional discrete wavelet transform for each channel $(luma, u, v)$. The Daubechies 9/7 wavelet coefficients used in this algorithm are shown in Table 1.

Table 1. Daubechies 9/7 wavelet coefficient.

Analytical Low Pass Filter	Analytical High Pass Filter	Synthetic Low Pass Filter	Synthetic High Pass Filter
0.026748757411	0	0	0.026748757411
-0.016864118443	0.091271763114	-0.091271763	0.016864118443
-0.078223266529	-0.057543526229	-0.057543526229	-0.078223266529
0.266864118443	-0.591271763114	0.591271763114	-0.266864118443
0.602949018236	1.11508705	1.11508705	0.602949018236
0.266864118443	-0.591271763114	0.591271763	-0.266864118443
-0.078223266529	-0.057543526229	-0.057543526229	-0.078223266529
-0.016864118443	0.091271763114	-0.091271763114	0.016864118443
0.026748757411	0	0	0.026748757411

(4) Quantification

After the $Luma, u, v$ channel undergoes wavelet transformation, its total wavelet coefficients are the same as the total number of pixels in the original image, but important visual information is concentrated in a few coefficients. In this paper, the wavelet coefficient a_b in the wavelet sub-band b is quantized to q_b , according to the following formula:

$$q_b = \text{sign}[a_b] \times \text{floor} \left[\frac{|a_b|}{2^{R_b - \varepsilon_b} \left(1 + \frac{\mu_b}{2^{11}}\right)} \right] \quad (7)$$

where the nominal dynamic ranges of self-band b , ε_b , and μ_b are the digits allocated to the index and tail of the current wavelet coefficients. The nominal dynamic range of b is the number of bits per pixel plus the number of increments in sub-band b of the original image. For the $Luma, u, v$ channel, different

quantization coefficients are used. For the luma channel, set $\varepsilon_b = 16$ and $\mu_b = 16$, and for the u and v channel, set $\varepsilon_b = 8$ and $\mu_b = 9$.

(5) Entropy coding

After quantization, arithmetic coding is applied to compress the quantized coefficients. Arithmetic coding is also adopted by JPEG2000. Generally speaking, arithmetic coding has a higher compression rate than Huffman coding [19]. Like other variable length entropy coding techniques, arithmetic coding uses shorter bits for high frequency characters and longer bits for low frequency characters.

Figures 5 and 6 show the flow charts of the compression and decompression algorithm.

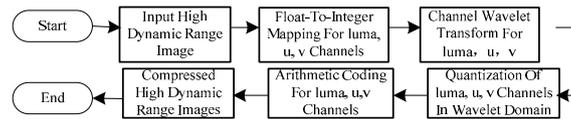


Figure 5. High dynamic intra-transmission image coding.

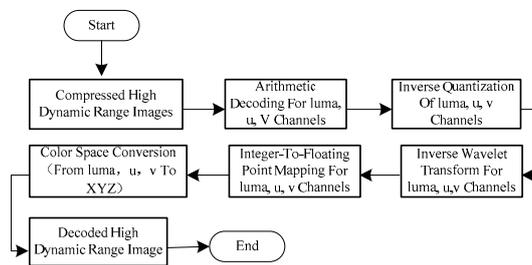


Figure 6. High dynamic range image decoding.

3. Results

In order to verify that the digital watermark image encrypted by this method has a strong anti-cutting and anti-noise performance, the image is simulated in this paper. In the experiment, the gray image and color image with the size of 243×243 pixels are used as the original carrier image. As shown in Figure 7a–i represent color and gray image in 64×64 binary image marked with “abcdefghigk”, which has rich color, texture, detail, area, theme, and plane background. Figure 7g,j show the original watermark image and extracted watermark image. Figure 7b,f,j test the anti-brightness performance and contrast attack performance of the image.

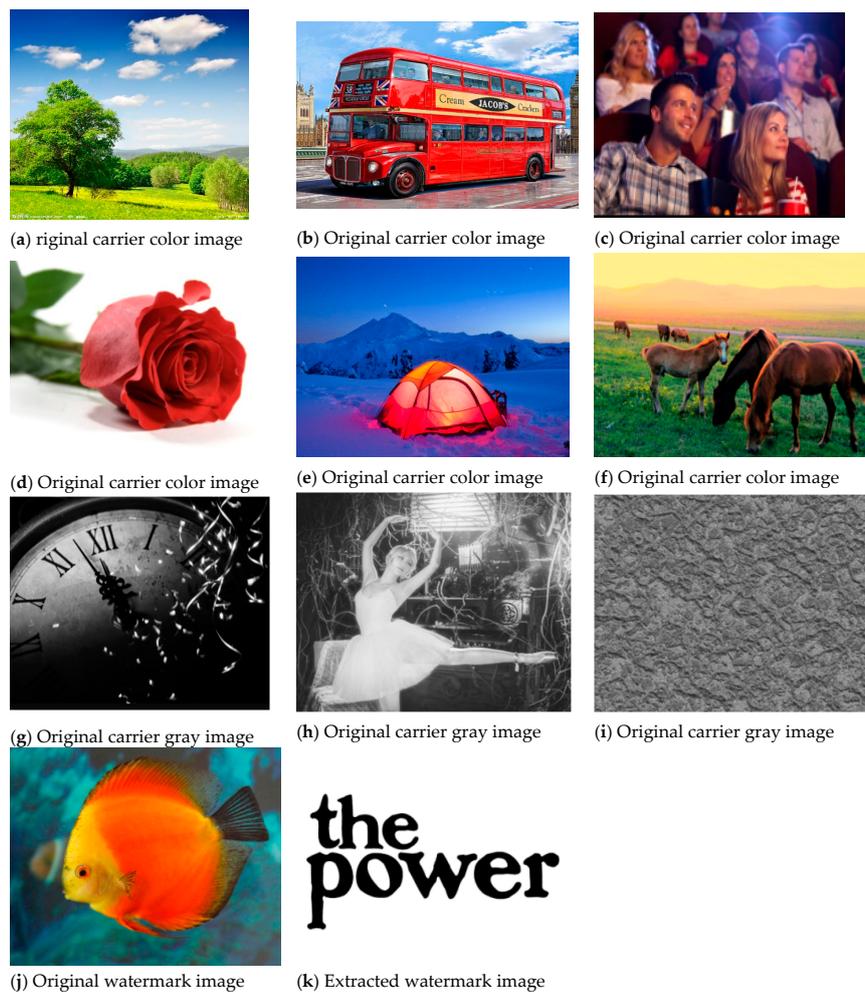


Figure 7. Original image and watermarking image.

3.1. Transparency Experiment

Peak signal-to-noise ratio (PSNR) is used to measure the quality of embedded watermarking image. For an 8-bit gray-scale image with $M \times N$ pixel size, the PSNR is as follows:

$$PSNR = 10 \lg \left(\frac{255^2 \times m \times n}{\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} (I'(i, j) - I(i, j))^2} \right). \quad (8)$$

For 24-bit color images with $M \times N$ pixels, the average peak signal-to-noise ratio (PSNR) of three RGB channels is used to measure the image quality.

$$\overline{PSNR} = (PSNR_R + PSNR_G + PSNR_B) / 3 \quad (9)$$

Figure 7 shows a small part of the original image and the watermarking image in the image database, both of which are 243×243 pixels in size.

The first three lines in Figure 7 are the original images, which represent color and gray images with rich colors, rich textures, rich details, distinct regions, distinct themes, and flat backgrounds. The last line is the watermarking image. In order to show the transparency of the symmetrically encrypted digital watermarking image, a watermarking image with rich color and distinct theme is embedded in the 24-bit watch image with a flat background and monotonous color, as shown in Figure 8.

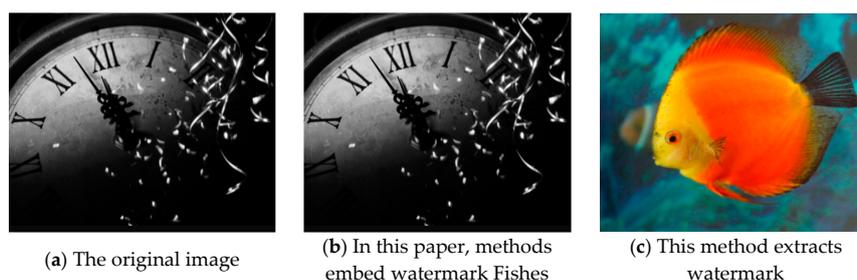


Figure 8. Original watermarked image and extracted watermarked image.

It can be seen from Figure 8 that the transparency of the symmetrically encrypted digital watermarking image is very good. In the experiment, 24-bit color watermarking (j) is embedded in 24-bit color images (a) to (g) in Figure 7, and 8-bit gray-scale watermarking (k) is embedded in 8-bit gray-scale images (h) and (i). The PSNR value is calculated for the obtained image and the original image, as shown in Table 2.

Table 2. Watermarking transparency experiment. PSNR, peak signal-to-noise ratio.

	PSNR	PSNR _R	PSNR _G	PSNR _B
a	45.7884	44.5741	45.7002	47.0909
b	45.6866	44.9539	45.6302	46.4757
c	45.1864	44.3810	45.0482	46.1301
d	45.6693	45.0324	45.6056	46.3700
e	46.0259	45.2301	46.0145	46.8602
f	45.8591	45.0048	45.6675	46.6050
g	46.6032	45.8702	46.2284	46.6032
h	44.8100	-	-	-
i	45.6100	-	-	-

It can be seen from Table 2 that the PSNR value between the watermark image and the original image is good, which conforms to the transparency standard. The results of embedding 24-bit color watermarking (j) in 24-bit color images (a) to (g) and embedding 8-bit gray-scale watermarking (k) in 8-bit gray-scale images (h) and (i) show that the transparency algorithm of a is better than that of other images.

3.2. Anti-Brightness/Contrast Attack Performance Detection

Figure 9 shows the experimental results of watermarking detection after adding brightness/contrast to the symmetrically encrypted digital watermarking image using Photoshop. The NC (Numerical Control) values of normalized cross-correlation function are compared. NC values are often used to evaluate the performance of the encrypted digital watermarking image.

Figure 9a–c show that, when brightness increases by 70 and contrast increases by 70, high-quality watermarking can still be extracted from tampered images with seriously degraded quality, with an NC value of 0.9961, while the traditional DCT transform-based watermarking algorithm has an NC value of 0.9863. Figure 9d–f show that, when the brightness increases by 70, the NC value is only 0.9710, so the proposed method has a strong brightness/contrast attack on symmetrically encrypted digital watermarking images.

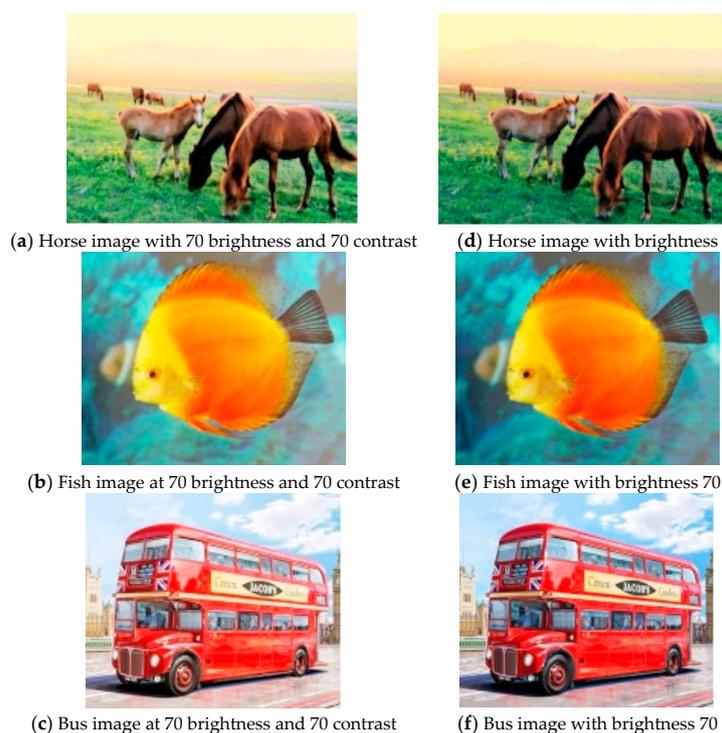


Figure 9. Anti-brightness/contrast attack performance detection.

3.3. Testing of Shear Resistance

Figure 10 shows the experimental results of embedding the watermarking into the image using the symmetric encryption algorithm proposed in this paper.

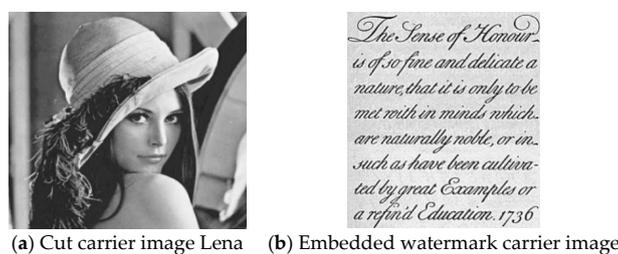


Figure 10. Shear resistance test.

After the symmetrically encrypted watermarking embedded image is cut, the watermarking of the cut image is extracted, as shown in Figure 10a. As shown in Figure 10b, the extracted watermarking image can still be restored to the watermarking image, which shows that the watermarking image encrypted by this method has an anti-shearing property.

3.4. Anti-Noise Performance Testing

In symmetrically encrypted watermarking embedded image, salt and pepper noise with an intensity of 0.02 is added to obtain the watermarking image with noise, as shown in Figure 11a. Wavelet transform is applied to the image, and the watermarking is extracted from the high frequency components in three directions, respectively. Then, the watermarking image is processed, as shown in Figure 11b.

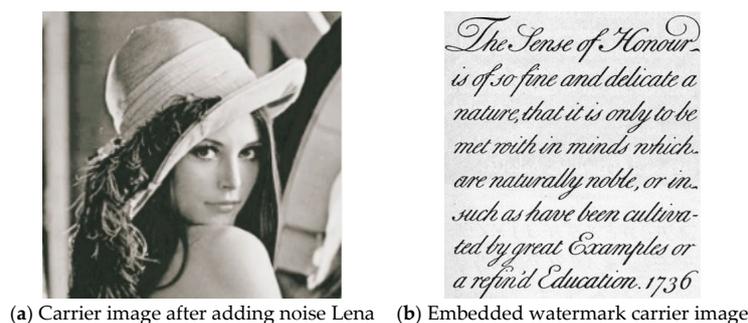


Figure 11. Noise resistance testing.

Figure 11 shows that, after adding noise to the symmetrically encrypted watermarking embedded image, the watermarking can still be extracted from the watermarking image, and the watermarking image can still be restored to the watermarking image after extracting the watermarking. It can be seen that the digital watermarking image encrypted by this method is noise-resistant.

3.5. Digital Watermarking Image Compression Detection Based on Symmetric Encryption

The symmetrically encrypted digital watermarking image (RGBE coding) provided by Munsell Color Science Laboratory of Rochester Institute of Technology University and the symmetrically encrypted digital watermarking image provided by Industrial Light and Magic Company are used in the experiment [20]. The visual quality of symmetrically encrypted digital watermarking image after lossy compression is measured based on root-mean-square error. The smaller the root-mean-square error, the better the digital watermarking image compressed by this method.

$$e_{rms} = \sqrt{\frac{1}{n} \sum_{i=1}^n [(X_1^i - X_2^i)^2 + (Y_1^i - Y_2^i)^2 + (Z_1^i - Z_2^i)^2]}, \quad (10)$$

where X_1 , Y_1 , and Z_1 are the three channels of the original graph, respectively; and X_2 , Y_2 , and Z_2 are the three compressed channels, respectively. It should be noted that their ranges are within $[10^{-4}, 10^{10}]$.

In addition to root-mean-square error, the visual error metric of symmetrically encrypted digital watermarking images is adopted to predict whether the difference between two symmetrically encrypted digital watermarking images can be perceived by human eyes. The visual error measurement of symmetrically encrypted digital watermarking image was proposed by Mantiuk et al. The input of HDR VDP is a pair of images (the original image and the changed image), and the output is a probabilistic image. The pixel value of the image is basically equal to the probabilistic value of the image difference visible to the naked eye. Table 3 shows the experimental result of symmetrically encrypted digital watermarking image compression.

Table 3. Experimental data of high dynamic range image compression.

Image Name	Original Size (byte)	Compressed Graph Size (byte)	Pixel Percentages of Image Differences Visible to the Naked Eye		Root Mean Square Error	Time (second)
			Probability >75%	Probability >95%		
Crissy Field. exr	1,304,619	750,382	0%	0%	1.7327	5"0
Flowers exr	758,083	200,512	0%	0%	1.8101	4"7
MtTamNorth. exr	1,422,492	487,324	0%	0%	2.8594	4"9
Cis front. hdr	7,893,724	640,179	0.01%	0%	0.3659	17"6
atrium. hdr	8,110,240	360,418	0.36%	0.11%	0.0515	17"3
Parking lot. hdr	7,767,193	666,102	0.01%	0%	0.3025	17"2
rooftops. hdr	7,336,883	500,505	0%	0%	0.1733	15"3
Albers. hdr	6,444,172	463,477	0%	0%	0.4152	15"7

Table 3 shows the experimental results of symmetrically encrypted digital watermarking image compression. The first column in the table is the image name, in which the image suffixed with HDR is

symmetrically encrypted digital watermarking image (R_GB_E encoding) provided by Munsell Color Science Laboratory of Rochester Institute of Technology University, and the image suffixed with EXR is symmetrically encrypted digital watermarking image (O) provided by Industrial Light and Magic Company. The second column is the size of the original image before compression, the third column is the size of the image after compression, the fourth column is the symmetric encryption of digital watermarking image visual error measurement (HDR VDP), the fifth column is the root mean square error of two images, and the last column is the time consumed by compression.

Figure 12 shows the image provided by Industrial light and Magic Company and Figure 13 shows the image provided by Munsell Color Science Laboratory. To display the results more clearly, both Figures 12 and 13 undergo tone mapping operation. In order to display symmetrically encrypted digital watermarking images on ordinary displays, we use tone mapping to compress symmetrically encrypted digital watermarking images into ordinary images.

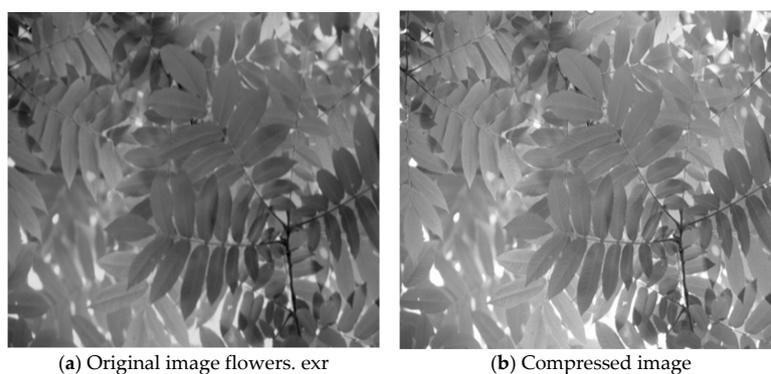


Figure 12. Image provided by Industrial light and Magic Inc.

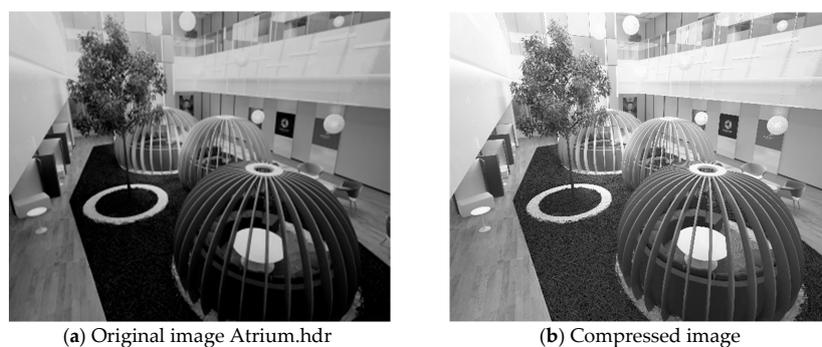


Figure 13. Image provided by Munsell Color Science Laboratory.

From Table 3, Figures 12 and 13, we can see that the volume of the compressed digital watermarking image is much smaller than that of the original image, and the visual difference of the compressed watermarking image as well as the root mean square error of the digital watermarking image are very small, indicating excellent performance of the compressed digital watermarking image.

4. Conclusions

This paper studies the digital watermarking image compression method based on symmetric encryption algorithm. This method uses the Arnold permutation method to transform the watermarking image in the time domain, and then uses the digital watermarking algorithm in the wavelet transform domain to embed the watermarking image into the important coefficients of the wavelet transform, so as to obtain the digital watermarking image. Using the symmetrically encrypted digital watermarking image compression method, the volume of the compressed watermarking image can be greatly reduced (about one-tenth of the original image) when the visual difference is very small.

The watermarking image encrypted and compressed by this method not only has good transparency, but also has strong anti-brightness/contrast attack, anti-shearing, and anti-noise performances. The proposed method has good application prospects in the future multimedia field because of its capacity to reduce image volume and lower the root mean square error and visual difference of digital watermarking image.

Author Contributions: Y.T. and Y.Z. carried a digital watermarking image compression method based on symmetrical encryption algorithm is proposed in this study. Y.T. processed the original image and scrambled watermarking image by wavelet transform. Y.Z. did the process of watermarking embedding, reconstructed watermarking extraction by the wavelet transform. Y.T. and Y.Z. did the experiments, recorded data, and created manuscripts. All authors read and approved the final manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Yin, X.; Huang, W.Q. Research on Color QR Code Watermarking Technology Based on Chaos Theory. *J. Commun.* **2018**, *373*, 54–62.
2. Wei, Q.L.; Sun, Q.Q. Digital Watermarking Algorithm Based on Contourlet Transform and SVD. *Comput. Eng. Des.* **2017**, *38*, 2369–2373.
3. Zhan, W.; Duan, X.H.; Yu, Y.C. Research on Image Compression Coding Method Based on Wavelet Transform. *Comput. Technol. Dev.* **2018**, *28*, 21–25.
4. Gu, F.M. The Compressed Video Image Multiple Digital Watermarking Hiding Method Simulation. *Comput. Simul.* **2017**, *34*, 199–202.
5. Zeng, C.; Yang, W.P. Research on Digital Watermarking Algorithm Based on DCT Transform for Image Copyright Protection. *Bull. Sci. Technol.* **2018**, *109*, 119–122.
6. Wu, C.M.; Zheng, H.K.; Wang, Y.J.; Fu, R.; Yu, M.; Sun, Y. An Image Compression Algorithm Based on Multi-node Cooperation in Wireless Multimedia Sensor Networks. *Trans. Beijing Inst. Technol.* **2018**, *38*, 109–114.
7. Li, S.Q.; Li, G.Q.; Xian, C.H. Eigenvector-Based Watermarking for 3D Mesh Models. *J. Graph.* **2017**, *38*, 155–161.
8. Dahmani, Z.; Abdellaoui, M.A. On a Three Point Boundary Value Problem of Arbitrary Order. *J. Interdiscip. Math.* **2016**, *19*, 893–906. [[CrossRef](#)]
9. Liao, R.H.; Sun, C.Q.; Liu, H. Fractional Fourier M-Band Dual-tree Complex Wavelet and SVD Based Digital Watermarking Algorithm. *Control Eng. China* **2017**, *24*, 1432–1438.
10. Delgado, J.; Peña, J.M. Monotonicity Preserving Representations of Curves and Surfaces. *Appl. Math. Nonlinear Sci.* **2016**, *1*, 517–528. [[CrossRef](#)]
11. Gong, M.L.; Zhang, W.; Wang, F.C. Image Compression Confidentiality Based on Compression Sensing Algorithm. *J. Detect. Control* **2017**, *39*, 106–110.
12. Ma, Z.; Sun, Y. An Application of ϵ -Expansion Method to the Dispersive Water System. *J. Interdiscip. Math.* **2016**, *19*, 335–344. [[CrossRef](#)]
13. Wang, C.H.; Han, D. An Effective Blind Forensics Detection Scheme of Median Filtering Image. *J. China Acad. Electron. Inf. Technol.* **2017**, *12*, 668–674.
14. Shen, Y.X.; Wu, J.; Wu, D.H. Fault Diagnosis Technology for Three-level Inverter Based on Reconstructive Phase Space and SVM. *J. Power Supply* **2017**, *15*, 114–121.
15. Maldonado, M.; Prada, J.; Senosiain, M.J. On Linear Operators and Bases on Köthe Spaces. *Appl. Math. Nonlinear Sci.* **2016**, *1*, 617–624. [[CrossRef](#)]
16. Liu, L.P.; Yin, J.T. Image Analysis of Chromium Doping on LiMn_2O_4 Spinel High Temperature Solubility. *Chin. J. Power Sources* **2017**, *41*, 1121–1123.
17. Lai, J.L.; Zhang, F.Q. Multimedia Image Reconstruction Based on Virtual Reality. *Autom. Instrum.* **2018**, *46*, 236–239.
18. Zhang, H. Digital Image Watermarking Algorithm Based on Compressive Sensing and Discrete Cosine Transform. *J. Jilin Univ. (Sci. Ed.)* **2017**, *55*, 1504–1510.

19. Liang, L.X.; Tang, L.H.; Bai, W.W. Simulation of Double Digital Watermarking Algorithm for Color Image. *Comput. Simul.* **2017**, *34*, 150–153.
20. Pyskunov, S.O.; Maksimyuk, Y.V.; Valer, V.V. Finite Element Analysis of Influence of Non-homogenous Temperature Field on Designed Lifetime of Spatial Structural Elements under Creep Conditions. *Appl. Math. Nonlinear Sci.* **2016**, *1*, 253–262. [[CrossRef](#)]



© 2019 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).