applied system innovation

MDPI

Article

Security Authentication of Dual Chaotic Image Watermarking in Spatial Domain with Spatial and Frequency Domain Characteristics Analysis

Zhengmao Ye [1,*], Hang Yin [1] and Yongmao Ye [2]

[1] College of Engineering, Southern University, Baton Rouge, LA 70813, USA; hang_yin@subr.edu
[2] Liaoning Radio and Television Station, Shenyang 110003, China; yeyongmao@hotmail.com
* Correspondence: zhengmao_ye@subr.edu

Received: 27 July 2018; Accepted: 15 October 2018; Published: 17 October 2018

Abstract: This article presents an advanced dual chaotic watermarking scheme to improve information security. To ensure confidentiality in digital image transmission, a secure dual watermarking scheme is proposed by applying the chaotic logistic system and hyper-chaotic dynamical system. Chaotic watermarking was conducted in the spatial domain, where suboptimal secure hashing with a variable length was selected in preprocessing stages. The secret key was generated by the chaotic sequence for pixel shuffling using a chaotic logistic map, so that a controlled amount of distortion was inserted into the host digital image. Watermarking was proceeded after the chaotic watermark had been embedded into the shuffled image. To strengthen the security, the hyper-chaotic system was used to generate chaotic blocks for block scrambling in order to achieve dual chaotic watermarking. Characteristics analysis was conducted for multiple examples in both spatial and frequency domains. Potential effects induced by the chaotic driving parameter on processing time and integrity authentication of chaotic dual watermarking were also analyzed in detail.

Keywords: watermarking; information security; logistic map; hyper-chaotic system; hashing; shuffling; scrambling

1. Introduction

With rapid development of digital communication and computer networks, it becomes feasible to guarantee transmission security against malicious tampering or copyright infringement. Information security plays a critical role in data transmission. Watermarking, cryptography, or steganography could protect transmitted information. Since digital images are easy to modify, a secure authentication system is needed to ensure that no tampering is made. Digital watermarking is a simple way to protect intellectual property. Watermarking schemes should be designed to provide integrity authentication for digital images. Chaotic watermarks are better alternatives than pseudorandom signals that possess white spectra. The chaotic theory has been widely applied in the fields of cryptography for information security and varying feature representation. An encryption scheme based on chaotic logistic maps is proposed for secure transmission. A secret key of 80 bits and two chaotic logistic maps has been employed. To enhance the robustness of ciphering against various attacks, the secret key was updated after encrypting each block of sixteen pixels of the source image. The statistical analysis and key sensitivity tests demonstrated that the encryption scheme provided an efficient and secure way for real-time image processing [1–3]. Applications of both deterministic and chaotic digital image cryptosystems in the spatial domain and frequency domain have been introduced. The results of these applications were compared in both qualitative and quantitative points of view, using symmetric deterministic and chaotic encryption schemes. The 64-bit block ciphers were proceeded in secret key cryptography. Differential scrambling was applied in both cases where Exclusive OR operations between the plaintext and either deterministic key or chaotic key were made. Outcomes were evaluated using both qualitative and quantitative analysis. The chaotic scheme was shown to be better than deterministic schemes against entropy attack and ciphertext attack [4]. In the present paper, a pixel shuffling method is proposed for image encryption. Based on the unpredictable characteristics of chaotic systems, the chaotic sequences are used as encryption codes to implement digital image encryption with high security. The method, covering four differential chaotic systems and pixel shuffling, can fully banish outlines of the host image, disorder distributive characteristics of intensity levels, and dramatically reduce the probability of exhaustive attacks. The scheme has great encryption performance that reaches high confidential security [5]. A double image encryption method has been proposed by utilizing discrete multiple-parameter fractional Fourier transform and chaotic maps. The image scrambled by one chaotic map is encoded into the amplitude of complex signals. The complex signal, multiplied by another chaotic random phase mask, is encrypted by multi-parameter fractional Discrete Fourier Transform (DFT). Parameters in chaotic maps serve as the keys of this encryption scheme [6]. In another study an efficient scheme was applied for embedding the compressed binary watermark logo on a basis of based integer wavelet-based watermarking. The Peak Signal to Noise Ratio (PSNR) and Normalized Correlation Coefficient (NCC) analyses indicated a better performance than existing methods on protecting document image contents [7]. Recently, an overview of digital video watermarking has thoroughly summarized current state of the art techniques for 3D video watermarking. Watermarking, in the frequency domain, was one of their main areas of focus, where DFT, Discrete Sine Transform (DST), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT) were highlighted. The DFT function produced a set of complex coefficients covering real and imaginary parts at each frequency, with translational invariance of the magnitude, where the DST function focuses on its imaginary coefficients and the DCT function focuses on its real coefficients. Their research showed that DWT decomposed an image or video frame into a lower level approximation component and three detail components. However, the major drawbacks of frequency domain schemes lie in the computational complexity and the vulnerability to potential attacks (e.g., geometric attack) [8].

Theoretical performance analysis of watermarking schemes has also been conducted based on correlation detection. Correlation and spectral properties of the watermark sequences generated by the piecewise-linear Markov maps were easily adjusted. The family of chaotic maps was used to verify theoretical analysis. Skew tent chaotic sequences have been compared with widely used pseudorandom sequences, indicating superiority of the former in watermarking applications. The audio data experiments verified theoretical analysis results [9]. Chaotic parameter modulation was used to modulate copyright information into the bifurcating parameter of a chaotic system. The system output was a wideband signal acting as a watermark to be inserted into the host image. The scheme, based on the ergodic property of chaotic sequence, was applied in order to demodulate the embedded copyright information. The technique effectively removed interference from the host image that improved detection performance dramatically. It was effective for image watermarking with the presence of noises, attacks, and payloads. This approach has been shown to be superior to conventional holographic transform domain method and spread spectrum-watermarking schemes due to its simple design and short computation time [10]. A novel authentication scheme has been proposed based on chaotic semi-fragile watermarking. The timing information of video frames was modulated into parameters of a chaotic system. The noise-like system output was applied as the watermark to be embedded into the block-based discrete cosine transform domain. The embedded information can be demodulated using maximum likelihood estimation. Temporal tampering was detected by the mismatch of timing information. Spatial tampering was detected by the deviation of the extracted watermark. The scheme satisfied particular requirements to authenticate a digital video surveillance system [11]. Fractional order analysis of chaotic systems has also been conducted. Qualitative analysis of fractional orders on chaotic system characteristics was made which provided a solid basis for applying fractional order control to either generate or suppress chaotic behaviors [12]. The goal of image watermarking is to embed hidden data into the host image. A new watermarking scheme for embedding watermark bits has been based on Chaotic Fractal Coding. The chaotic signal was deterministic, pseudo periodic, and sensitive to initial conditions. Integration of the chaotic system and Fractal Coding plays an important role in the security, invisibility, and capacity of the scheme. The idea now, is to come up with a set of selective blocks for steady embedding. Chaos-Fractal Coding has shown confidential capacity [13].

Dual chaotic watermarking in the spatial domain has been proposed in the context in order to protect intellectual property, where the chaotic logistic map generated watermarking and the subsequent dual chaotic watermarked images possess sensitivity variations of high probability, which has extensive applicability for authentication systems by inserting a controlled amount of distortion to the host images. To evaluate variations after watermarking, two additional tests of NPCR (Number of Pixel Change Rate) and UACI (Unified Average Changing Intensity) will be provided as case studies in the spatial domain. The role of the chaotic driving parameter on computation time and information security is also discussed in terms of the testing data. Two additional security tests based on the discrete entropy and relative entropy will also be implemented in the frequency domain.

2. Spatial Domain Chaotic Watermarking

The initial chaotic watermarking was conducted in the spatial domain via scrambling with a generated sequence using the chaotic logistic map.

2.1. True Color Model

True color digital images were selected for this study. In the Cartesian coordinate system, a color representation is made by mixing three primary spectral components (Red, Green, and Blue) at the true color space. The actual scene results from the color composition. The RGB image was manifested by an array (M × N × 3) of intensity levels independent from each other. In the true color model, three primary color components were mapped into a cube in which the red, green, and blue values were set to be three corners. Furthermore, black was set to be the origin and white was set to be the opposite corner. The remaining three corners of the cube corresponded to cyan, magenta and yellow. The actual composite color was the vector on or inside the cube. The projection of RGB intensity components onto the diagonal produced the grayscale image of the size (M × N).

2.2. Suboptimal Secure Hashing with Variable Length

Hashing is the function to map an arbitrary string of characters into a shorter fixed length string, which can still represent the source string. For image watermarking, it was used to transform the visual feature of the source image into the binary feature array so as to apply the simple binary codes to represent the source image. For a true color host image of the total pixel size M × N with three primary color components (R, G, B), the color intensity of each pixel ranged from 0 to 255 which can be converted to an 8-bit binary plaintext. The host image array can be transformed into a sequence of strings by column indexing. To be robust against the preimage attack and collision attack, secure hashing with a variable length was implemented. For instance, collating plaintexts of consecutive pixels in the sequence would give rise to combinations of 256 or 512 bit plaintext in binary, corresponding to 64 and 128 bit plaintext in hexadecimal. The resulting strings from several possible combinations were compared with those of fixed length hashing. Sub-optimization was achieved with respect to the shortest Hamming distance. The specific number of consecutive pixels being collated determined the actual length of the hash function. Column indexing information was kept together with the chaotic key sequence for permutation based shuffling and watermarking.

2.3. Chaotic Logistic Map Watermark Generator

The chaotic system has characteristics of ergodicity, which is also sensitive to initials. The chaotic logistic map was chosen to generate the chaotic sequence in order to substitute the classical pseudorandom sequence. The chaotic sequence (key) was generated by a typical chaotic logistic map. The logistic difference equation is simply formulated as (1).

$$x_{n+1} = \mu x_n(1 - x_n) \tag{1}$$

where n is the index; x_n is between 0 and 1; $0 < \mu \leq 4$ is the driving parameter that could exhibit bifurcation behaviors and lead to oscillation between two values when μ = 3.0. A chaotic Boolean vector is generated when a number of the logistic map iterations are completed. It serves as the private key or chaotic watermark.

2.4. Host Image Shuffling and Watermark Embedding

The chaotic watermark was the Boolean sequence generated from the chaotic logistic map iterations. The indexing function came from sorting the chaotic sequence. The indexing matrix of pixel permutation was based on the generated chaotic sequence. The generated column indexing sequence was used for shuffling the pixels of the host image. The bitwise scrambling was conducted between the chaotic watermark and the shuffled host image. XOR binary operation (A$\oplus$ B or Exclusive OR) was conducted to embed the chaotic Boolean vector or chaotic watermark into the four Least Significant Bits (LSBs) at each target pixel on the host image such that initial chaotic watermarking was made. By joining corresponding bits in binary, the chaotic watermarked image was produced in the spatial domain. For each component (R, G, B) of the true color digital image of size of M $\times$ N in the spatial domain, the same chaotic watermarking scheme was applied. Shuffling may increase sensitivity to various attacks and enhance security. Similar to watermark embedding process, XOR binary operation can be conducted once again for potential watermark extraction.

2.5. Parametric Modulation for Chaotic Logistic Map

The chaotic behavior arises from typical nonlinear dynamical mapping of the logistic polynomial equation. Its driving parameter μ is also called the bifurcation parameter as it could exhibit a bifurcation diagram. This simple study was conducted to examine the best parameter value of μ that could speedup the watermarking process. Based on its initial interval of [0, 4], by numerical simulations, when the driving parameter μ is located within [3.6, 4.0], the turnaround time for image watermarking was within a reasonable range. However, when the driving parameter μ is less than 3.575, turnaround time for watermarking increases dramatically, which is no longer feasible for the watermarking scheme. Meanwhile, within [3.6, 4.0], it is found out that the greater the value of μ, the shorter the turnaround time (Figure 1). Thus, the driving parameter μ is chosen to be 4.0 for watermarking. However, when merely the single parameter (μ) is used in the logistics map, security vulnerabilities still exist. Rather than adopting logistics map modification, the *introduction* of dual chaotic scrambling turns out to be more powerful.

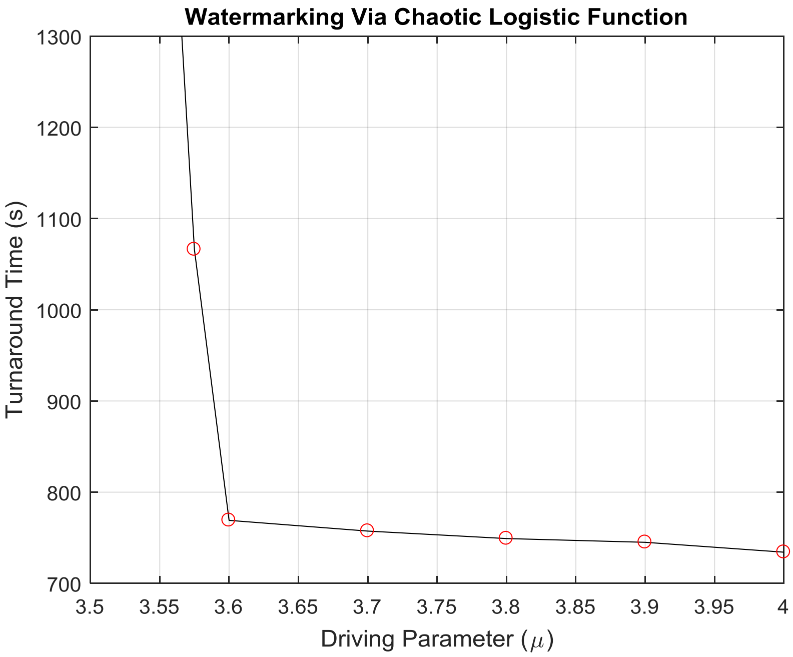

Figure 1. Turnaround time vs. parameter modulation of logistic map.

3. Dual Chaotic Scrambling to Enhance Security

Information security can be further strengthened using another hyper-chaotic watermarking scheme so as to be robust against various attacks. Overlaying the initial chaotic logistic watermark and another hyper-chaotic watermark makes the watermarking scheme robust against potential attacks. Dual chaotic watermarking is based on the 4D hyper-chaotic dynamical system, which is formulated as (2).

$$\begin{aligned} \dot{x}_1 &= -x_1 - x_2 \\ \dot{x}_2 &= x_1 + ax_2 + x_4 \\ \dot{x}_3 &= b + x_1x_3 \\ \dot{x}_4 &= -cx_3 + dx_4 \end{aligned} \tag{2}$$

It exhibited hyperchaotic behavior when parameter values were selected as a = 0.25, b = 3, c = 0.5 and d = 0.05. In numerical simulations, initial conditions of 4D chaotic systems can be selected as [−10, −6, 0, 10]. It is a dynamical system with 4 Lyapunov exponents. Exponents of Lyapunov have highlighted that, due to the hyperchaotic system's potential to lead to strong randomness, the hyperchaotic array may be used for watermarking. To generate the hyperchaotic array, the hyperchaotic map was used for generating four separate 64 bits or 128 bits hyperchaotic sequences (X_1, X_2, X_3, X_4) in hexadecimal, where $X_1 = \{x_1\}$, $X_2 = \{x_2\}$, $X_3 = \{x_3\}$, $X_4 = \{x_4\}$. After simple discretization with small quantization error, the hyperchaotic matrix of dimension 64 × 64 or 128 × 128 was formulated by (3), where T refers to transpose operation of a vector, which was used as another watermarking system so as to be embedded into the existing initial chaotic watermarked images.

$$H = (X_1X_2^T)(X_3X_4^T) \tag{3}$$

For each pixel considered in watermarking blocks, once again bitwise scrambling operation was made between the watermarked images and the hyperchaotic matrix using Exclusive OR binary operation (A$\oplus$ B), which gave rise to dual watermarked images. The advantage of dual chaotic watermarking lies in high confidentiality, easy implementation, and short processing time. Overlaying the two chaotic watermarking systems makes watermarks difficult to be removed and attacked. The same XOR operation was applied to all three color components of each pixel. At the same time, the characteristics of the RGB components were kept when pixel shuffling and modulo 2 additions were proceeded. Watermarking can be applied to individual RGB intensity levels and positions of each pixel simultaneously. In order to evaluate the variations between the host and watermarked images, some quantitative tests were needed afterwards.

4. Numerical Simulations of Digital Watermarking

Numerical simulations were conducted in this study where sizes of watermarks were typically specified for dual chaotic digital watermarking. All host images were true color images with three primary color components of red, blue, and green. Each individual color component was subject to dual chaotic watermarking. Without loss of generality, the basic block size for watermarking was selected to be 256 × 256 pixels and 512 × 512 pixels, respectively. In Figure 2, two watermark blocks of pixel size 256 × 256 were selected. In Figure 3, two watermark blocks of pixel size 512 × 512 were selected. In Figure 4, eight watermark blocks of pixel size 256 × 256 were selected. In Figures 2–4, the host and shuffled images are shown on the top row; while the initial single chaotic watermarked images and dual chaotic watermarked images are shown on the bottom row.

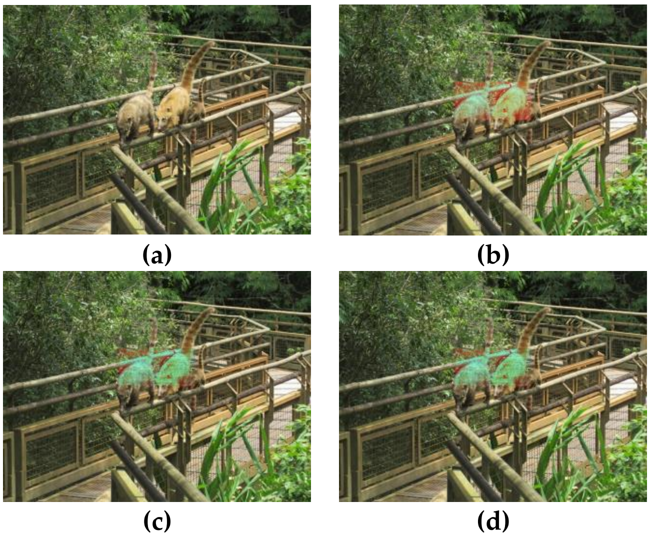
(a) **(b)** **(c)** **(d)**

Figure 2. True color image dual chaotic watermarking: Case 1 (2 Blocks: 256 × 256 pixels). (**a**) Host image, (**b**) shuffled image, (**c**) chaotic watermarking, (**d**) dual chaotic watermarking.

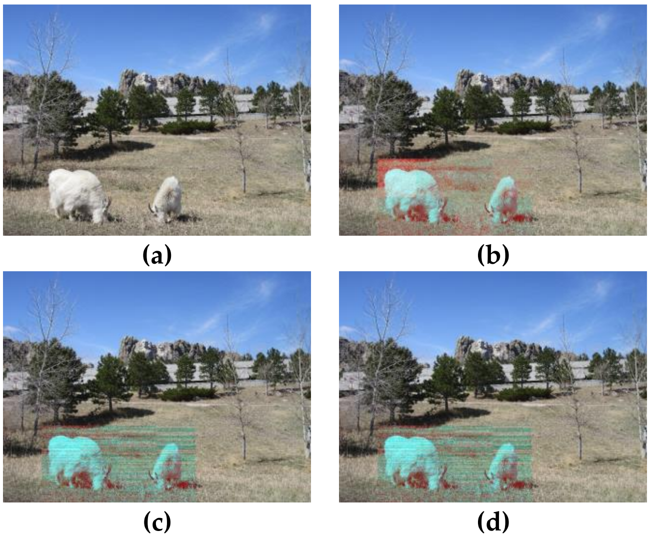
(a) **(b)** **(c)** **(d)**

Figure 3. True color image dual chaotic watermarking: Case 2 (8 Blocks: 512 × 512 pixels). (**a**) Host Image, (**b**) shuffled image, (**c**) chaotic watermarking, (**d**) dual chaotic watermarking.

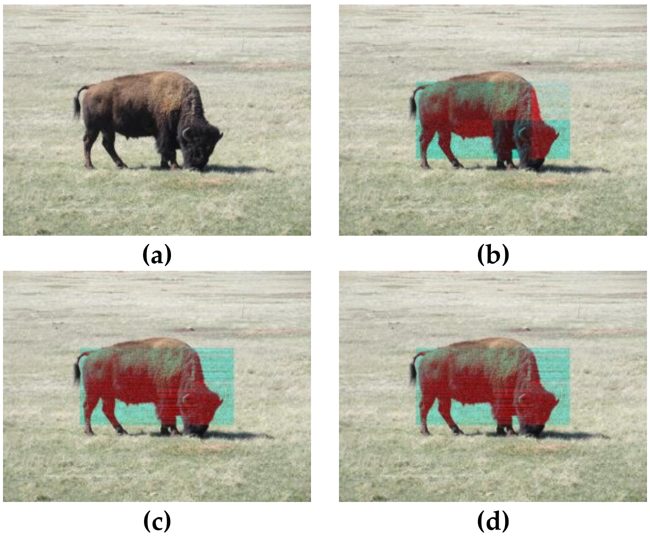

Figure 4. True color image dual chaotic watermarking: Case 3 (8 Blocks: 256 × 256 pixels). (**a**) Host image, (**b**) shuffled image, (**c**) chaotic watermarking, (**d**) dual chaotic watermarking.

At the same time, Case 3 has been chosen to compare the host image with the shuffled image, single chaotic watermarked image, and dual chaotic watermarked image. The mismatches between the host image and three outcomes after each processing step are shown in Figures 5 and 6. Similar outcomes of Figure 6 contain complementary colors to Figure 5.

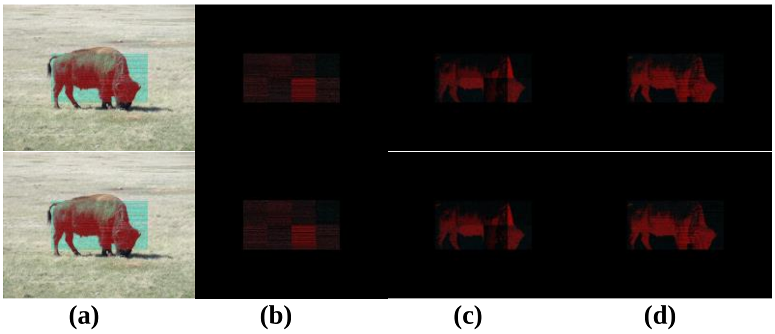

Figure 5. Dual chaotic watermarking: Watermarks. (**a**) Dual watermarking outcome, (**b**) shuffling, (**c**) watermarking, (**d**) dual watermarking.

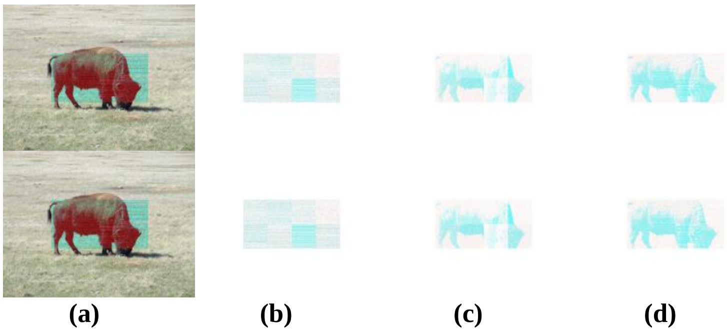

Figure 6. Dual chaotic watermarking: Watermarks shown in complementary colors. (**a**) Dual watermarking outcome, (**b**) shuffling, (**c**) watermarking, (**d**) dual watermarking.

In Figures 5 and 6, the host image and actual mismatches after shuffling, single chaotic watermarking, and dual chaotic watermarking are illustrated. For comparison purposes, the driving parameter μ was selected to be 3.6 and 4.0 corresponding to the top row and bottom row, respectively.

For both cases, mismatches—arisen from each subsequent stage are clearly manifested. To further analyze the impact of dual chaotic watermarking schemes, two quantitative analyses using NCPR and UACI in the spatial domain. were carried out in order to conduct objective evaluation. Then two tests using quantitative measures of discrete entropy and relative entropy were also implemented to verify the security analysis results.

5. Security Analysis in Spatial and Frequency Domains

In this session, to evaluate variations of security characteristics from the host images to dual chaotic watermarked images, both spatial domain and frequency domain analyses were conducted. Firstly NPCR (Number of Pixel Change Rate) and UACI (Unified Average Changing Intensity) were selected as quantitative metrics in the spatial domain. In each case, variations in dual chaotic watermarked image blocks were analyzed. Without loss of generality, Case 3 was selected for quantitative analysis in the spatial domain. Secondly the discrete entropy and relative entropy analyses in the frequency domain were also conducted. The primary color components of red, green and blue in three selected Cases (1, 2, 3) were processed individually. Similar conclusions were made even though quantitative analyses were implemented in another domain.

5.1. NPCR (Number of Pixel Change Rate)

Let $I(i, j)$ and $J(i, j)$ represent the actual intensity levels of the corresponding pixel (i, j) on a host image and dual chaotic watermarked image. $B(i, j)$ in Equation (4) was then defined as the binary array and NPCR was defined in Equation (5), where M and N stand for total numbers of pixels at each row and each column.

$$B(i,j) = \{ \begin{matrix} 0 & if & I(i,j) = J(i,j) \\ 1 & if & I(i,j) \neq J(i,j) \end{matrix} \tag{4}$$

$$\text{NPCR} = \frac{\sum_{i,j} B(i,j)}{M \times N} \times 100\% \tag{5}$$

The scores of NPCR are listed in Table 1. The range of driving parameter μ is from 3.6 to 4.0. The NPCR scores of the digital images after shuffling, after dual watermarking, as well as those of mismatches generated by shuffling and dual chaotic watermarking are listed in four separate rows. All the qualitative NCPR scores obtained were around 99%, which indicates that the dual chaotic watermarking scheme was very sensitive with respect to even low variations in the plaintext. NPCR was also applied to evaluate the impact of changing a single pixel in a host image on the dual chaotic watermarked image. The 99% NPCR score illustrates that the position of each pixel had been dramatically randomized which is very sensitive to the small variation. Thus it demonstrates suitable robustness of a dual chaotic watermarking scheme against possible differential attacks. After dual chaotic watermarking (2nd row), it showed that, in general, a bigger driving parameter μ corresponds to a larger NPCR score and better security. However the effect of driving parameter μ on NPCR and security should be applied to a large quantity of digital images to make the existing conclusion more convincing.

Table 1. Quantitative Metric of Number of Pixel Change Rate (NPCR).

μ **Outcomes**	μ **= 3.6**	μ **= 3.7**	μ **= 3.8**	μ **= 3.9**	μ **= 4.0**
Chaotic Watermarking	0.9883	0.9884	0.9882	0.9884	0.9886
Dual Chaotic Watermarking	0.9909	0.9909	0.9910	0.9911	0.9912
Mismatch Chaotic Shuffling	0.9895	0.9895	0.9895	0.9895	0.9895
Mismatch Dual Watermark	0.9894	0.9895	0.9894	0.9895	0.9895

5.2. UACI (Unified Average Changing Intensity)

UACI is defined in Equation (6). The outcomes of UACI are listed in Table 2. The range of the driving parameter μ is from 3.6 to 4.0. The UACI scores of the digital image after shuffling, after dual chaotic watermarking, as well as those of mismatches generated by shuffling and dual chaotic watermarking are listed in four separate rows. Appropriate UACI scores indicate that almost all intensity levels of pixels in the watermarked image are changed, which are no longer distinctive. The low UACI score also covers the broad distribution of intensity changes instead of the special cases exclusively. After dual chaotic watermarking (2nd row), it shows that generally a bigger driving parameter μ corresponds to a smaller UACI score and better security. Still the effect of driving parameter μ on UACI and security should be applied to a large quantity of digital images for comparison to make it more convincing.

$$UACI = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \frac{|I(i,j) - J(i,j)|}{255} \times 100\% \tag{6}$$

Table 2. Quantitative Metric of Unified Average Changing Intensity (UACI).

μ **Outcomes**	μ **= 3.6**	μ **= 3.7**	μ **= 3.8**	μ **= 3.9**	μ **= 4.0**
Chaotic Watermarking	0.1200	0.1201	0.1201	0.1199	0.1199
Dual Chaotic Watermarking	0.1426	0.1425	0.1425	0.1424	0.1421
Mismatch Chaotic Shuffling	0.6600	0.6600	0.6600	0.6600	0.6600
Mismatch Dual Watermark	0.6601	0.6601	0.6601	0.6601	0.6601

5.3. Discrete Entropy

Discrete Entropy (or Shannon Entropy) is a statistical measure of randomness so as to characterize the digital image. It is formulated as a sum of products of the probability of outcome times the logarithm of the inverse of the probability (7), over all potential outcomes in the event $\{x_1, x_2, \ldots, x_k\}$, where $p(i)$ is the probability distribution and k is the count of intensity levels. It can simply describe the uncertainty of an arbitrary set of discrete events. Intuitively it indicates the average amount of information conveyed from the digital image information source being selected.

$$H(x) = \sum_{i=1}^{k} p(i) \log_2 \frac{1}{p(i)} = -\sum_{i=1}^{k} p(i) \log_2 p(i) \tag{7}$$

Regardless of the host, chaotic watermarked and dual chaotic watermarked images, the greater the discrete entropy, the more the information content, and, in turn, the more the security. All three cases of digital image chaotic watermarking and dual chaotic watermarking were taken into account with all discrete entropy data listed in Table 3. The discrete entropies of three chaotic watermarked images are slightly bigger than those of three source images. It shows that the former was a little bit more complex than the latter with respect to information content. On the other hand, the discrete entropies of three dual chaotic watermarked images were much higher than those of three source images and three single chaotic watermarked images. It highlighted that a remarkable extra amount of information was covered using dual chaotic watermarking, making it much more secure and robust against attacks (e.g., Entropy Attack).

Table 3. Quantitative Metric of Discrete Entropy.

RGB Discrete Entropy	Red	Green	Blue
Source A	2.6470	2.6116	2.3542
Chaotic Watermarking	2.6551	2.6241	2.3564
Dual Chaotic Watermarking	2.6761	2.6443	2.3861
Source B	2.5103	2.4543	2.6716
Chaotic Watermarking	2.5277	2.4689	2.6985
Dual Chaotic Watermarking	2.5872	2.5522	2.7729
Source C	2.1757	2.1772	2.2911
Chaotic Watermarking	2.2327	2.2338	2.3550
Dual Chaotic Watermarking	2.2931	2.3444	2.4673

5.4. Relative Entropy

Relative Entropy (or Kullback-Leibler Divergence) is the measure of the distance between two probability distributions on a random variable. Given two discrete probability distributions $p(i)$ and $q(i)$ over histograms of the digital image, the relative entropy of one with respect to another is then defined as the sum of all possible states, which is formulated as (8).

$$d = \sum_{i=1}^{k} p(i) \log_2 \frac{p(i)}{q(i)} \tag{8}$$

Intuitively it is the expectation of a logarithmic difference between two probabilities, which measures quantitatively how one probability distribution differs from another. Divergence acts as a convex function on the domain of probability distributions. The relative entropy reaches zero when probability distributions $p(i)$ and $q(i)$ are identical with each other.

All three cases of digital image chaotic watermarking and dual chaotic watermarking were taken into account with the relative entropy data to the source images listed in Table 4. The relative entropies between dual chaotic watermarked images and source images were much greater than those of between single chaotic watermarked images and source images. It shows that dual chaotic watermarking was more secure and more robust than chaotic watermarking itself against various attacks (e.g., Ciphertext Attack).

Table 4. Quantitative Metric of Relative Entropy.

RGB Relative Entropy	Red	Green	Blue
Source A			
Chaotic Watermarking	0.0041	0.0176	0.0079
Dual Chaotic Watermarking	0.0047	0.0455	0.0177
Source B			
Chaotic Watermarking	0.0220	0.0132	0.0021
Dual Chaotic Watermarking	0.0285	0.0222	0.0039
Source C			
Chaotic Watermarking	0.0089	0.0115	0.0113
Dual Chaotic Watermarking	0.0122	0.0131	0.0133

6. Conclusions

The chaotic dual watermarking scheme in the spatial domain has been implemented to enhance information security successfully. Firstly the chaotic logistic system was applied for generating chaotic sequences as secret keys, so that pixel shuffling and chaotic watermarking in the spatial domain can be made to embed watermarks. The host image was shuffled and embedded using a secure chaotic sequence of a variable length. Secondly the hyper-chaotic system was used to generate another watermark for block scrambling to further strengthen information security via dual chaotic watermarking. Experimental results verified the information security and integrity authentication of the proposed chaotic dual watermarking scheme. To conduct quantitative analysis, two tests of NPCR and UACI in the spatial domain were carried out initially, followed by two tests of discrete entropy and relative entropy analyses being implemented in the frequency domain. The case studies using suboptimal hashing with the variable length gave rise to highly confidential chaotic watermarked images, which depicted the feasibility of potential applications for secure digital image watermarking.

Author Contributions: Conceptualization: Z.Y. and H.Y. conceived of the presented idea. Methodology: Z.Y., H.Y. and Y.Y. developed the theoretical formalism. Software: Z.Y. and Y.Y. designed the codes and performed the numerical simulations. Validation: Z.Y., H.Y. and Y.Y. verified the analytical methods. Formal Analysis: Z.Y. and H.Y. carried out analytic calculations. Writing-Original Draft: Z.Y. prepared the draft manuscript. Writing-Review: H.Y. conducted initial review. Visualization: Y.Y. provided feedback on visual appeal of all figures.

Funding: This research received no external funding.

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

References

1. Schilling, R.; Harris, S. *Fundamental of Digital Signal Processing Using Matlab*; Cengage Learning: Boston, MA, USA, 2005.
2. Lathi, B. *Modern Digital and Analog Communication Systems*; Oxford University Press: Oxford, UK, 2009.
3. Pareeka, N.; Patidara, V.; Suda, K. Image Encryption Using Chaotic Logistic Map. *Image Vis. Comput.* **2006**, *24*, 926–934. [CrossRef]
4. Ye, Z.; Yin, H.; Ye, Y. Information Security Analysis of Deterministic Encryption and Chaotic Encryption in Spatial Domain and Frequency Domain. In Proceedings of the 2017 International Conference on Electrical Engineering, Computing Science and Automatic Control, Mexico City, Mexico, 20–22 September 2017.
5. Huang, C.; Nien, H. Multi Chaotic Systems Based Pixel Shuffle for Image Encryption. *Opt. Commun.* **2009**, *282*, 2123–2127. [CrossRef]
6. Shan, M.; Chang, J.; Zhong, Z.; Hao, B. Double Image Encryption Based On Discrete Multiple-Parameter Fractional Fourier Transform And Chaotic Maps. *Opt. Commun.* **2012**, *285*, 4227–4234. [CrossRef]
7. Chetan, K.; Nirmala, S. An Efficient And Secure Robust Watermarking Scheme For Document Images Using Integer Wavelets and Block Coding Of Binary Watermarks. *J. Inf. Secur. Appl.* **2015**, *24–25*, 13–24. [CrossRef]
8. Asikuzzaman, M.; Pickering, M. An Overview of Digital Video Watermarking. *IEEE Trans. Circuits Syst. Video Technol.* **2018**, *28*, 2131–2153. [CrossRef]
9. Tefas, A.; Nikolaidis, A. Performance Analysis of Correlation-Based Watermarking Schemes Employing Markov Chaotic Sequences. *IEEE Trans. Signal Process.* **2003**, *51*, 1979–1992. [CrossRef]
10. Chen, S.; Leung, H. Ergodic Chaotic Parameter Modulation with Application to Digital Image Watermarking. *IEEE Trans. Image Process.* **2005**, *14*, 1590–1602. [CrossRef] [PubMed]
11. Chen, S.; Leung, H. Chaotic Watermarking for Video Authentication in Surveillance Applications. *IEEE Trans. Circuits Syst. Video Technol.* **2008**, *18*, 704–709. [CrossRef]
12. Ye, Z.; Mohamadian, H.; Yin, H. Impact of Fractional Orders on Characteristics of Chaotic Dynamical Systems. *Int. J. Electr. Electron. Data Commun.* **2017**, *5*, 72–77.
13. Keyvanpour, M.R.; Merrikh-Bayatb, F. An Effective Chaos-Based Image Watermarking Scheme Using Fractal Coding. *Procedia Comput. Sci.* **2011**, *3*, 89–95. [CrossRef]