Entropy **2013**, *15*, 3170-3185; doi:10.3390/e15083260

OPEN ACCESS

entropy

ISSN 1099-4300

www.mdpi.com/journal/entropy

Article

A Maximum Entropy-Based Chaotic Time-Variant Fragile Watermarking Scheme for Image Tampering Detection

Young-Long Chen [1], Her-Terng Yau [2,*] and Guo-Jheng Yang [1]

[1] Department of Computer Science and Information Engineering, National Taichung University of Science and Technology, Taichung 404, Taiwan; E-Mails: ylchen66@nutc.edu.tw (Y.-L.C.); s18013106@nutc.edu.tw (G.-J.Y.)

[2] Department of Electrical Engineering, National Chin-Yi University of Technology, Taichung 41170, Taiwan

* Author to whom correspondence should be addressed; E-Mail: pan1012@ms52.hinet.net; Tel.: +886-4-23924505-7229; Fax: +886-4-23924419.

Received: 16 April 2013; in revised form: 27 July 2013 / Accepted: 29 July 2013 / Published: 5 August 2013

Abstract: The fragile watermarking technique is used to protect intellectual property rights while also providing security and rigorous protection. In order to protect the copyright of the creators, it can be implanted in some representative text or totem. Because all of the media on the Internet are digital, protection has become a critical issue, and determining how to use digital watermarks to protect digital media is thus the topic of our research. This paper uses the Logistic map with parameter $u = 4$ to generate chaotic dynamic behavior with the maximum entropy 1. This approach increases the security and rigor of the protection. The main research target of information hiding is determining how to hide confidential data so that the naked eye cannot see the difference. Next, we introduce one method of information hiding. Generally speaking, if the image only goes through Arnold's cat map and the Logistic map, it seems to lack sufficient security. Therefore, our emphasis is on controlling Arnold's cat map and the initial value of the chaos system to undergo small changes and generate different chaos sequences. Thus, the current time is used to not only make encryption more stringent but also to enhance the security of the digital media.

Keywords: encrypt; watermark; logistic map; Arnold's cat map

1. Introduction

Technology is changing rapidly. In the current highly competitive atmosphere, the Internet has become an integral part of our lives, but although obtaining information is convenient, many problems have arisen. For example, digital media have matured quickly and are widely used, resulting in copyright disputes. The contents and applications of information technology are ever more important. When sending important information, the computer acts as one's "right-hand man". However, it can easily be accessed and important information stolen if it is not encrypted. In the case of data being intercepted, we all hope that confidential data will not be found. Therefore, hiding information to protect it is essential.

Due to the rapid development of the Internet and technology, digital data must be free from limitations of time and space to quickly spread throughout the Internet because users need to access messages immediately and save important data. Due to its convenience, users can use the Internet to easily obtain, copy, or modify digital data, and even use some powerful image editing software, such as Photoshop and Photo Impact. However, it is illegal to copy or modify unauthorized digital data. In order to protect the rights of the original owner while offering universal access, protecting intellectual property rights [1] is particularly important.

In order to address this issue, we have researched some of the published works on fragile watermarking [2–3] procedures based on schemes for image authentication [4]. A robust image watermarking scheme usually embeds a watermark into an original image. For copyright protection, the owner should be capable of verifying and extracting the embedded watermark from the modified image. Modifications may, however, be rancorous, for example intentional tampering [5] or other image attacks. Image authentication watermarking techniques are therefore necessary, and can be classified into three groups: (A) Semi-fragile watermarking localizes and detects modifications to the contents [6]; (B) Fragile watermarking can detect any modification to the image [7]; and (C) Content-based fragile watermarking can detect only the significant changes in the image when we permit content saving processing, for example, coding and scanning [8]. The first proposed watermarking-based scheme for image authentication was presented by Walton [9] who divided the image into 8×8 blocks and embedded the LSB checksum in each block. The disadvantage of Walton's scheme, however, is that modifying the blocks with the same position in two different authenticated images does not affect the image checksum. In order to improve this, Fridrich [10] used a pseudo-random sequence and modified the error diffusion method to embed a binary watermark into an image, so that it can be detected no matter how the values of the image pixels are changed. There are three basic steps in the method: (A) choose a chaotic map and generalize it by introducing some parameters, (B) make the chaotic map discrete with a finite square lattice of points that represent pixels, and (C) extend the discrete map to three-dimensions and further compose it with a simple diffusion mechanism. Using a different approach, Wong [11] proposed a public key fragile watermarking scheme for image authentication which divided the image into non-overlapping blocks and inserted digital signatures for authentication. In Wong's scheme, a public key is used to generate a signature that uses the seven most significant bits of the pixels in each image block, and then adds a logo to become a watermark, embedding the watermark into the LSB of the corresponding blocks. The signature may be a signed hash value or encrypted image content. If an image has been changed, it will be detected by these mechanisms. These mechanisms, however, cannot discover where the image was modified. In addition, the attached signature needs more storage or additional bandwidth, but they may not always be obtained [12]. Suthaharan [13] enhanced Wong's proffered security by using a gradient image and its bit distribution properties to generate a huge key space to counter any vector quantization attack. A geometric attack is recognized as one of the most difficult attacks to resist. In response to such attacks, Wang [14] used the nonsubsampled contourlet transform (NSCT) domain with good visual quality and reasonable resistance to geometric attacks. A binary logo is used as a watermark in our scheme. By using a Logistic map [15–21], a chaotic map pattern is generated. A scrambled image is obtained from the chaotic map pattern and the binary watermark undergoes the exclusive-or (XOR) operation, and then is embedded in the LSB of each point of the image. The original image with the watermark is obtained by executing a reverse cat map. Zhao *et al.* [22] used embedding of the watermark in the wavelet descriptors based on the Neyman-Pearson criterion. This method can obtain high fidelity under a geometric attack. In [23], Zhao *et al*. proposed different embedding watermark techniques in the wavelet descriptors, including a method for watermarking using a chaos sequence and neural network. Furthermore, Guyeux and Bahi [24] proposed discrete chaotic iterations in order to hide information; this method uses the most and least significant coefficients to determine the topological chaos. In recent years, digital watermarking techniques [25] have been widely used in the protection of digital media rights. They can add the message that you want to save or embed the copyright trademark into the digital data without impacting the data, and at the same time retain their integrity and authenticity. Through extraction techniques to obtain the watermark, we can identify the original creator.

This paper offers a chaotic system-based fragile watermarking scheme for image tampering detection [26]. It uses a novel watermarking scheme based on chaotic maps. The image is processed by Arnold's cat map to become an orderless image which is then divided into eight blocks. A chaotic watermark is obtained by using the XOR operation between the binary watermark and the binary chaotic image. Furthermore, we also embed the chaotic watermark into an orderless image of each block of least significant bits.

The disadvantage of a chaotic system-based fragile watermarking scheme for image tampering detection is its lack of variability, which means that it is not possible to obtain the iterate cat map. With its lack of variability and randomness, it will be easy to crack. In order to solve this problem, we propose the time-variant system to enhance security. We use the current time to obtain the cat map image, because it cannot know the period through the formula. Our proposed method combines the cat map image and the current time, which can avoid image repeatability in the cat map. It also means that the watermarked image cannot be easily extracted.

The rest of the paper is organized as follows: In Section 2, Arnold's cat map and the Logistic map are briefly described. In Section 3, the proposed watermarking scheme is explained. The experimental results are given in Section 4, and conclusions are presented in Section 5.

2. Chaotic Mapping Algorithm

2.1. Arnold's Cat Map Encryption Algorithm

A digital image is constituted of pixels. If there is an arbitrary arrangement of the original pixel positions, it will become confused and unrecognizable, but if it goes through position transformation several times, it can then revert to the original digital image. This arrangement, called Arnold's cat map, was proposed by a Russian mathematician, Vladimir I. Arnold. The original image *P* is an $N \times N$ array, and the coordinate of the pixel is $F = \{(x, y) \mid x, y = 0,1,2,3,..., N-1\}$. Arnold's cat map encryption algorithm is described as follows:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & c \\ d & cd+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod N \tag{1}$$

where $A = \begin{bmatrix} 1 & c \\ d & cd+1 \end{bmatrix}$

Therefore, we obtain:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = A \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod N \tag{2}$$

where *c* and *d* are positive integers, and the value of the *A* matrix determinant is 1. When Arnold's cat map algorithm is executed once, the original pixel position's coordinate will be transferred from the (x, y) to a new original pixel position; then the process is repeated with the *A* matrix multiplied. The pixels will continue to move until they return back to their original position; the number of moves is *T*, and the size of the pixel space is n = 0, 1, 2, , N−1. Pixels move with periodicity, and *T*, *c*, *d* and the original image's size *N* are correlated; thus, whenever the values change, it generates a completely different Arnold's cat map. After being multiplied a few times, the correlation between the pixels will be completely chaotic. However, Arnold's cat map encryption algorithm has periodicity, which reduces its encryption security. This is why we add the Logistic map into the chaos system to enhance security.

T depends on the original *c*, *d* and *N*. Thus *c*, *d* and *r,* which are decided by the current time *t* (s), can serve as the private key; *r* is described as follows:

$$r = t \bmod T \tag{3}$$

From Equations (1)–(3), Arnold's cat map encryption algorithm with r times is described as follows:

$$\begin{aligned} \begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} &= \begin{bmatrix} 1 & c \\ d & cd+1 \end{bmatrix}^r \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod N \\ &= A^r \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod N \end{aligned} \tag{4}$$

Assuming $c = 1$, $d = 1$ and $N = 256$, we can conclude that the period *T* is 192; the periodic phenomenon in the cat map is shown in Figure 1.

2.2. Logistic Map

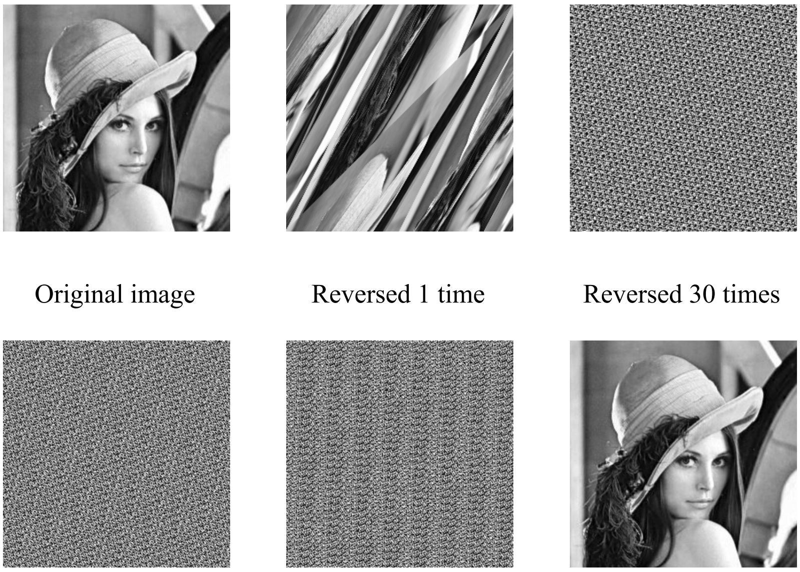
In a seemingly chaotic system, there is in fact order. In the situation of two identical chaotic systems with different initial values, they look like two different things, but with a narrow view of the two systems, they still have the same appearance, such as the weather in Taiwan that changes every day, yet the four seasons of every year are fixed. Values usually change within a certain range that is not exceeded, so the chaos system can be controlled.

A Logistic map uses different initial values to serve as parameters that assort different users; it produces different chaotic sequences. The chaos sequence has randomness; the greater the sequence length, the better the randomness. X is an array generated from the chaos system whose range is restricted to 0–1. X_t is the position of instant start; and X_{t+1} is the next position of instant start, described as follows:

$$X_{t+1} = uX_t(1 - X_t) \tag{5}$$

where $0 < u \leq 40$ is the range of chaotic sequence, but the value between 3.5,699,456 and 4 has positive entropy. The maximum entropy is 1 with the parameter $u = 4$ as shown in Figure 2, and it has the best effect. If u is fixed and the initial condition is $x(0)$, the sequence of the Logistic map is very sensitive. Different initial conditions $x(0)$, produce different sequences; they do not have any correlation. If one is unable to get the initial value, it is hard to get the same sequence without obtaining the initial value.

Figure 1. Periodic phenomenon in the cat map.



Original image

Reversed 1 time

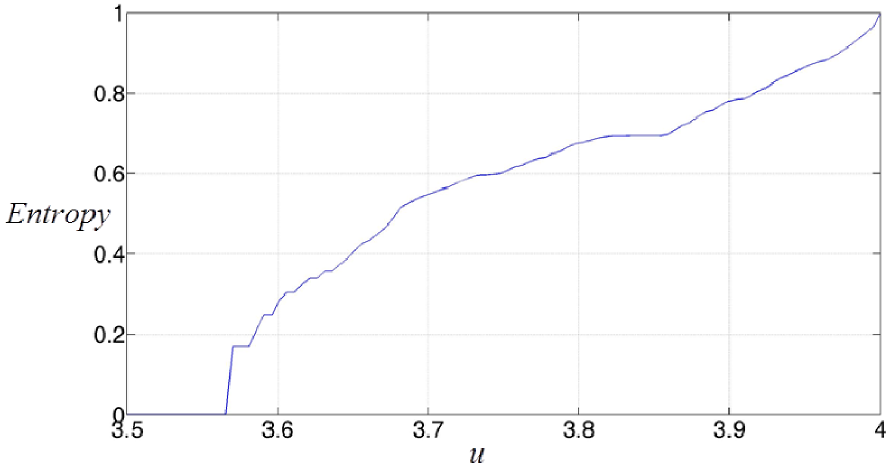
Reversed 30 times

Reversed 60 times

Reversed 120 times

Reversed 192 times

Figure 2. The entropy of the Logistic map for $3.5 \leq u \leq 4$.



3. The Proposed Method

Assuming that the original image *P* size is $M \times N$, the binary watermark image W_b size is $m \times n$.

3.1. Embedding the Watermark

The watermark of our proposed algorithm is embedded as follows:

- Step 1: Original image P goes through Arnold's cat map; we can obtain the period T from Equation (1).
- Step 2: Interception of minutes and seconds obtains the current time t; we get the value r which represents that P goes through Arnold's cat map r times from Equation (3), and we can obtain the scrambled image P_{scr} from Equation (4).
- Step 3: Divide P_{scr} into 8-bit blocks.
- Step 4: From the current time t, the chaotic system can generate a chaotic sequence S from Equation (5) which ranges between 0 and 1; round it off and apply it to the Logistic map; fetch from t to $m \times n + t$ and then we can obtain the chaotic image S_{cp}.
- Step 5: Using the XOR operation between W_b and S_{cp}, we can obtain W_c which is a binary chaotic watermark to be expressed as:

$$W_c = S_{cp} \oplus W_b \tag{6}$$

- Step 6: The least significant bit of P_{scr} is replaced by W_c.
- Step 7: Use Arnold's cat map to let the modified P_{scr} reverse (T–r) times to obtain the final result P_w.

Figure 3 shows our proposed block diagram of the embedding process. For example, embedding the watermark process with $r = 69$ is shown in Figure 4.

Figure 3. Our proposed diagram of the embedding process.

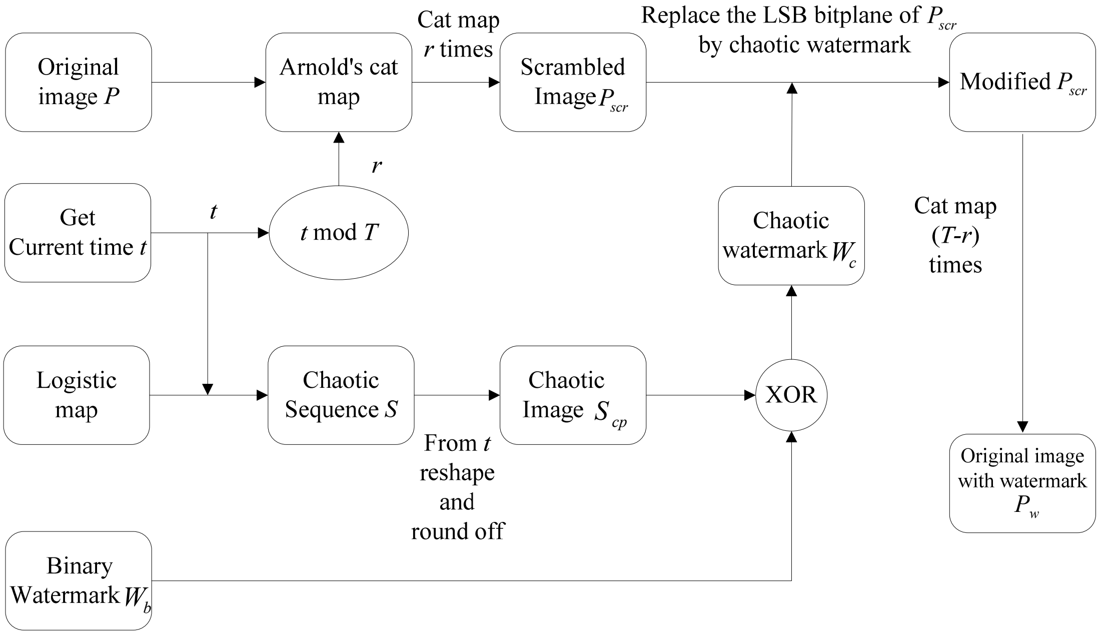
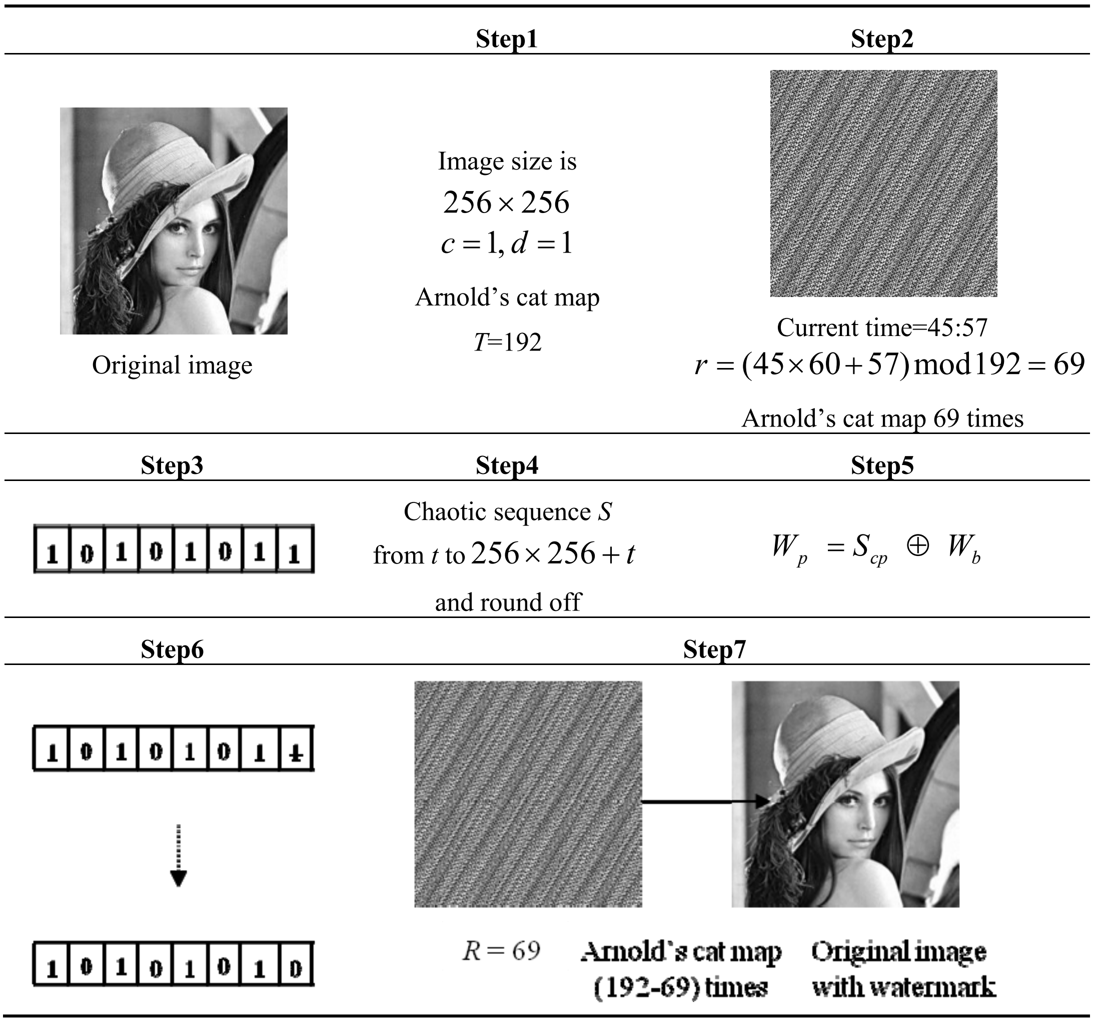


Figure 4. Process of embedded watermark with $r = 69$.



3.2. Fetching the Watermark

The watermark of our proposed algorithm is fetched as follows:

- Step 1: Intercept of minutes and seconds obtains the current time t from Equation (2); the analysis image P_a goes through Arnold's cat map r times; it can obtain the scrambled image P_{ascr}.
- Step 2: Divide P_{ascr} into 8-bit blocks.
- Step 3: From the current time t, the chaotic system can generate a chaotic sequence S from Equation (5), which ranges between 0 and 1; round it off and apply it to the Logistic map; fetch from t to $m \times n + t$, and then we can obtain the chaotic image S_{cp}.
- Step 4: Using the XOR operation between the LSB of P_{ascr} and S_{cp}, we can obtain W_e, which is a binary fetched watermark to be expressed as:

$$W_e = LSB\ of\ P_{ascr} \oplus S_{cp} \tag{7}$$

- Step 5: The binary watermark W_b is compared with W_e; take a different place going through Arnold's cat map (*T*–*r*) times, and then we can see which place was modified.

The block diagram of the extraction process is shown in Figure 5. Fetching the watermark is shown in Figure 6.

Figure 5. Block diagram of the extraction process.

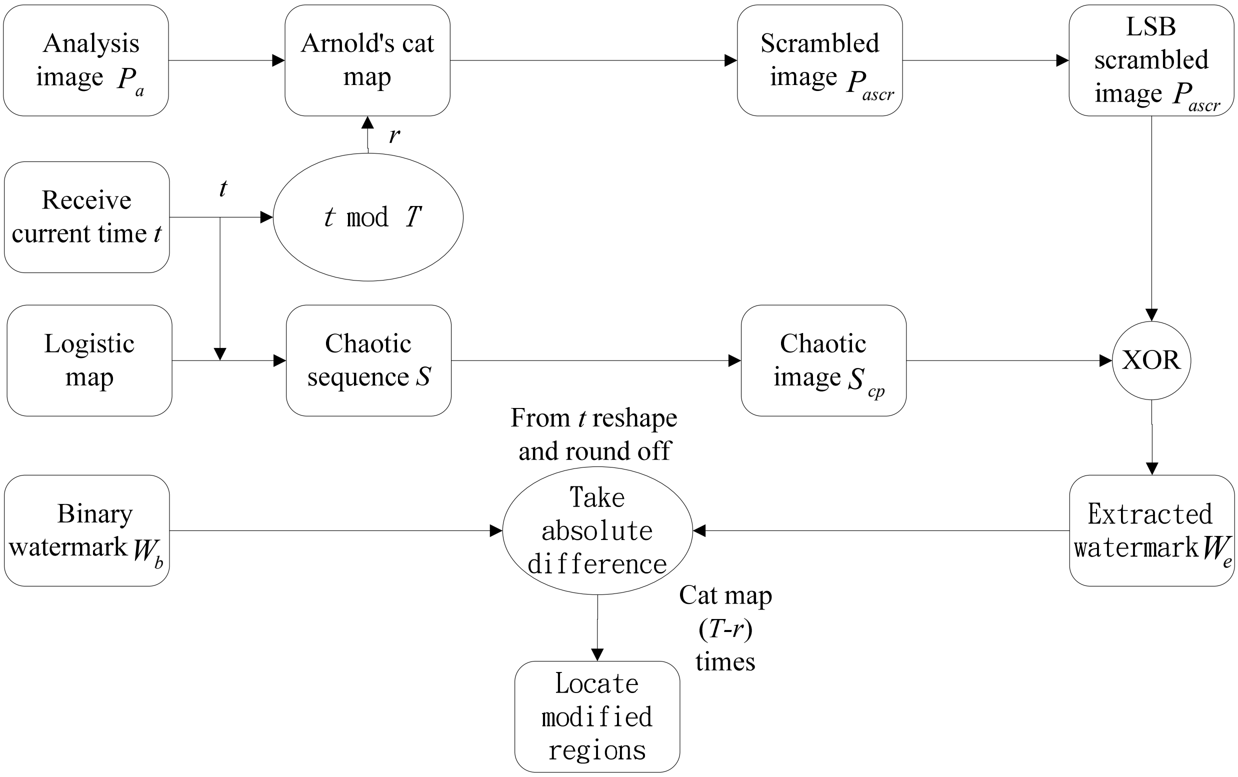


Figure 6. Process of fetching the watermark.

	Step1	Step2
 Analysis Image	Image size is 256×256 $c = 1, d = 1$ Arnold's cat map T=192	1 0 1 0 1 0 1 1

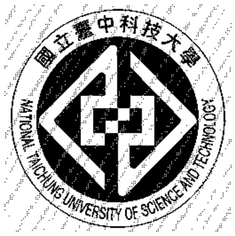
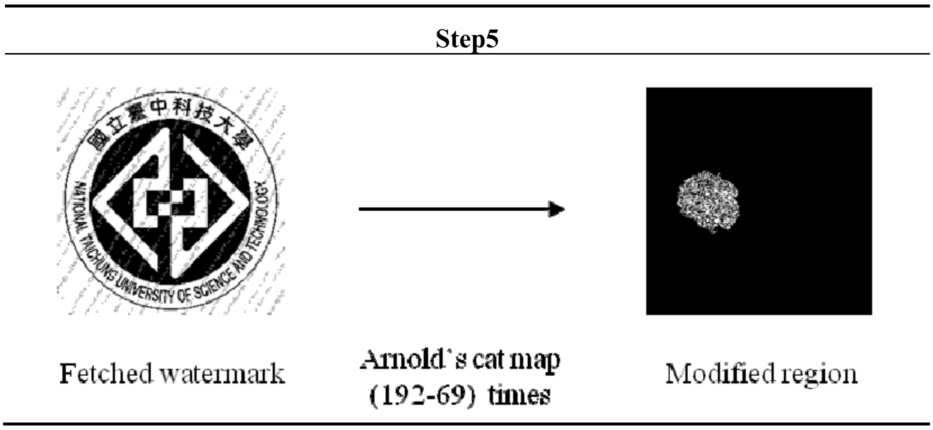
Step3	Step4
Chaotic sequence $S$from t to $256 \times 256 + t$ and round it off	$W_e = LSB\ of\ P_{ascr} \oplus S_{cp}$  Fetched watermark

Figure 6. *Cont.*

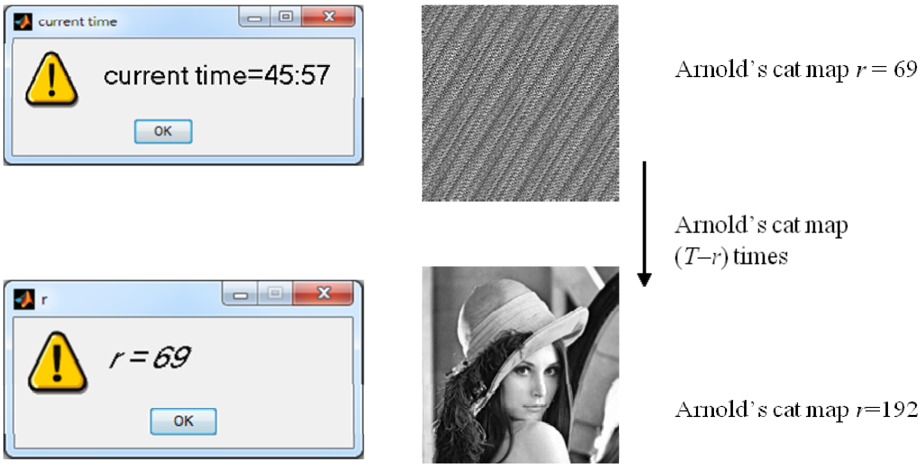


By using the current time *t* to control the value *r* of Arnold's cat map, not only can the chaotic image reduce the image's repeatability, but also the generated original image with the watermark has a considerable number of combinations because the original image with the watermark is generated from the parameters *c*, *d*, *r*, and t. The range of *c* and *d* is infinite positive integers, the range of *r* is (0, *T*), and the range of *t* is 0–3,660. If the values of *c*, *d*, r and t are not known, it is impossible to obtain the original image with the watermark; thus, it can enhance security.

4. Experimental Results

In this paper, we execute a variety of experiments to evaluate the performance of our algorithm. The pixel of the image is 256×256 via Arnold's cat map algorithm, generating the period $T = 192$ and set $c = 1, d = 1$. Because the value of *r* is decided by the current time *t*, it can get a key which changes with the current time *t*. The key's distinctive quality is that it just affects the decoding, without the difference being obvious; for example, we obtain the minutes and seconds of the current time as 45 and 57; then the value of $r = (45 \times 60 + 57) \bmod 192 = 69$. After we know *r*, we can know the reverse time that is just *T*–*r*, so that we can obtain the original image. The result is shown in Figure 7.

Figure 7. Reverse time process.


current time=45:57

r = 69

We divided our experiments into two parts, modifying the range and numerical comparison. In the modified range, we used the Lena images to analyze the images to see whether they had been modified; the pixel of the original and watermarked images is 256×256 via the Logistic map algorithm. We set the parameter $c = 1$, $d = 1$, $T = 192$, $u = 3.7$, $x(0) = 0.5$, and $r = 69$ according to the current time *t*. In Figure 8, the experimental result shows that a larger modified region results in a more indistinct watermarked image. The analysis image of Lena is shown in Figure 8a1, while a2 is the extracted watermark from Figure 8a1. The modified region result is shown in Figure 8a3, a1 shows that the image has not been modified, because in Figures 8a2, a3, one does not see the place which has been modified. Figure 8b1 is Figure 8a1 combined with a flower. We can see the modified region in Figure 8b2, 8b3 shows the pattern of the modified region.

Furthermore, we used the Baboon image to analyze the region which had been modified; the pixel of the original and watermarked images is 256×256 *via* the Logistic map algorithm, and we set the parameters $c = 1$, $d = 1$, $T = 192$, $u = 3.7$ and $x(0) = 0.5$. We obtained r according to the current time *t*, because the current time of each experiment is different, and $r = 133$ according to the current time *t*. In Figure 9, the experimental result shows that the larger modified region results in a more indistinct watermarked image. The analysis image of Baboon is shown in Figure 9a1, while a2 is the watermark extracted from Figure 9a1. The modified region result is shown in Figure 9a3. Figure 9a1 shows that the image has not been modified, because in Figure 9a2, a3, one does not see the place which has been modified. Figure 9b1 is Figure 9a1 combined with blinkers. We can see the modified region in Figures 9b2, b3 show the pattern of the modified region.

If the modified region area increases, the extracted watermark will become increasingly blurred, as the experimental figures show in Figures 8 and 9. However, we can still clearly distinguish the embedded watermark. Therefore, the extracted watermark of our proposed method is high fidelity. Besides, our proposed method can accurately show that the image is modified in location.

In this paper, peak signal-to-noise ratio (*PSNR)* is used to compare the visual quality of the watermarked image with that of the original image *P*, where *PSNR* is defined as:

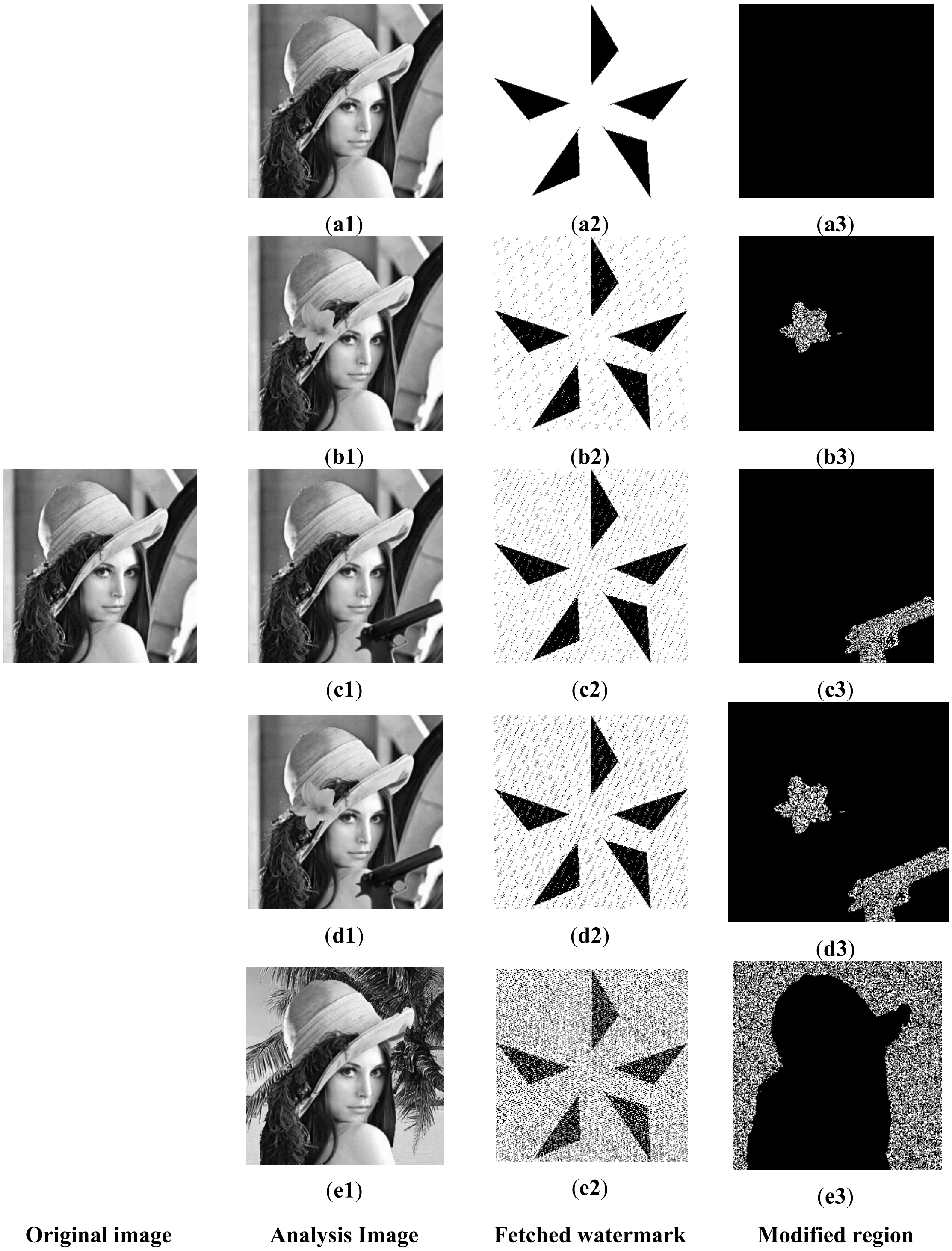
$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right)dB \tag{8}$$

The mean square error (*MSE*) is between the original and the modified image, where *MSE* is defined as:

$$MSE = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left[P(i,j) - P'(i,j)\right]^2 \tag{9}$$

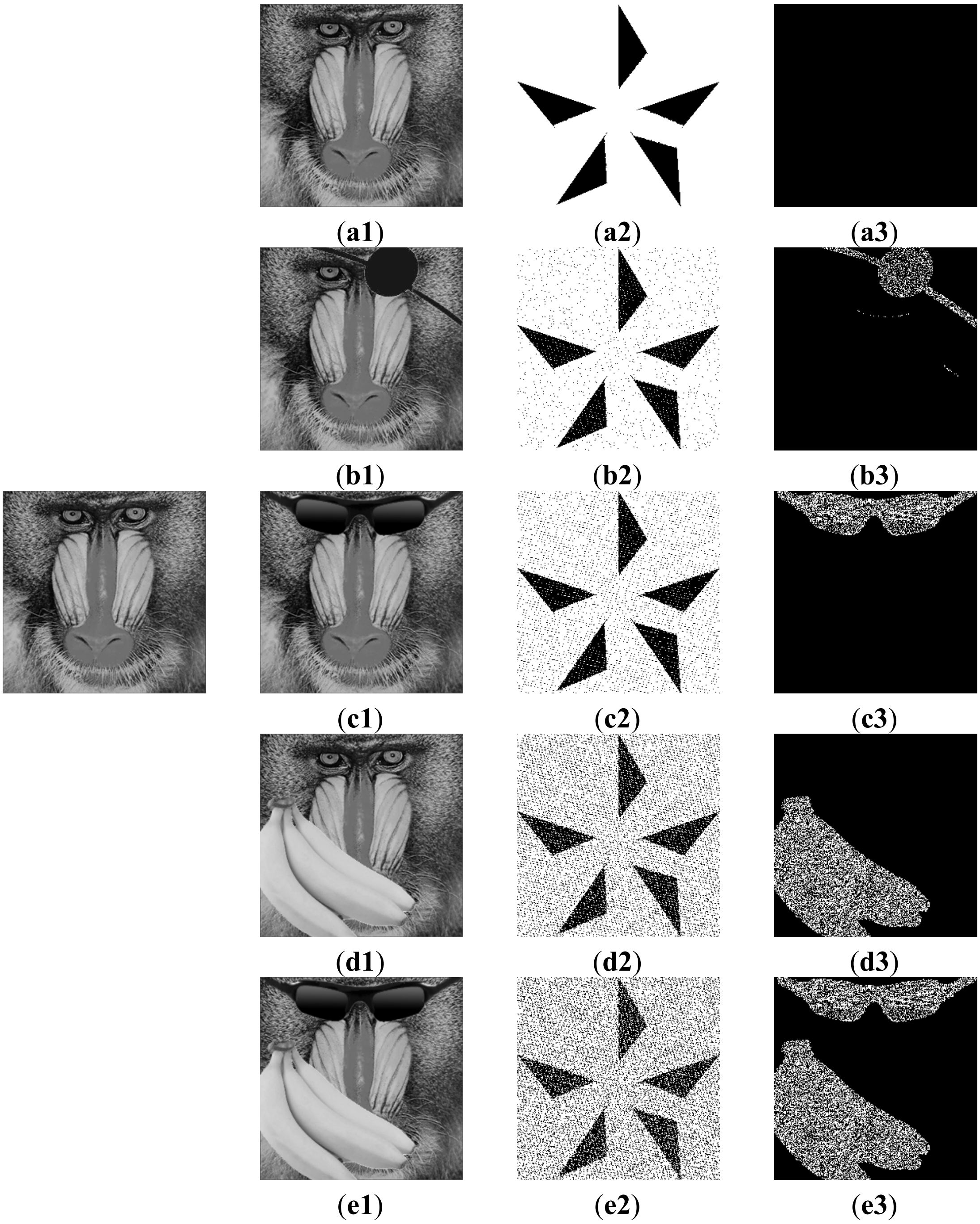
In Equations (8) and (9), we can conclude that when *PSNR* rises, it means there is relatively less distortion; when *PSNR* falls, it means the distortion increases and the place has changed more from Equation (8). *MSE* is inversely proportional to *PSNR*, so for *MSE,* ‘the smaller the better’ in Equation (9); if the modified region increases, the value of *PSNR* will rise and the value of *MSE* will be less.

Figure 8. Comparison of different modifications of Lena.



In the numerical comparison, Figure 8 shows the extracted watermark and modified region of Lena. We used *PSNR* and *MSE* numeric to show that a larger modified region causes a higher value of *PSNR* and a lower value of *MSE* according to Equations (8) and (9). The experimental figures are shown in Figure 10. In Figure 10a1, the *PSNR* and *MSE* values are infinite and 0, respectively. Figure 10a1 is equal to the original image. We compare it with Figure 10b1–e1. In Figure 10b1, the *PSNR* with *MSE* values are + 21.58 dB with + 0.01 dB, respectively. In Figure 10c1, the *PSNR* with *MSE* values are + 17.12 dB with + 0.02 dB, respectively. In Figure 10d1, the *PSNR* with *MSE* values are + 15.79 dB with + 0.03 dB, respectively. In Figure 10e1, the *PSNR* with *MSE* values are + 14.57 dB with + 0.06 dB, respectively.

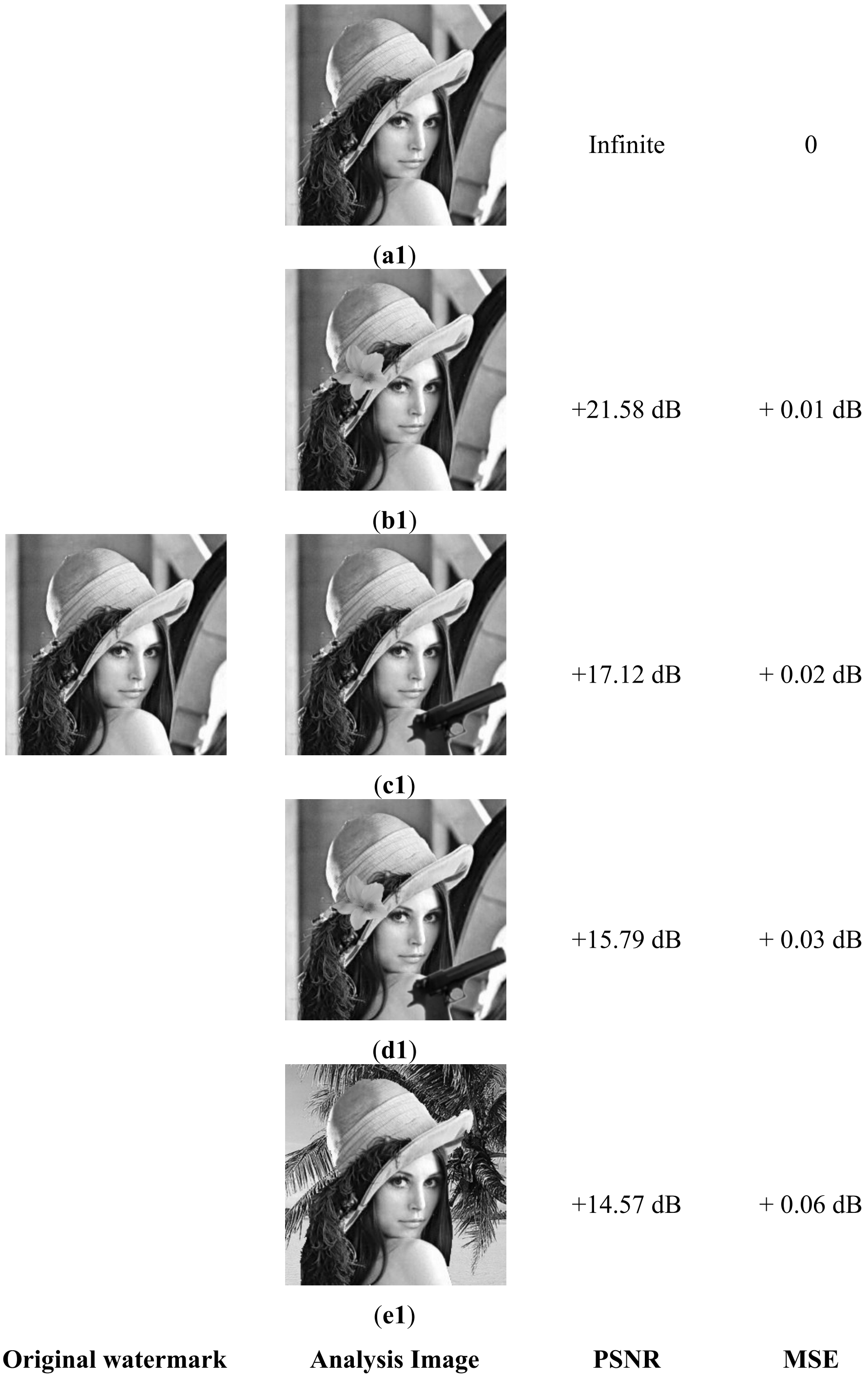
Figure 9. Comparison of the different modifications of Baboon.



Original watermark **Analysis Image** **Fetched watermark** **Modified region**

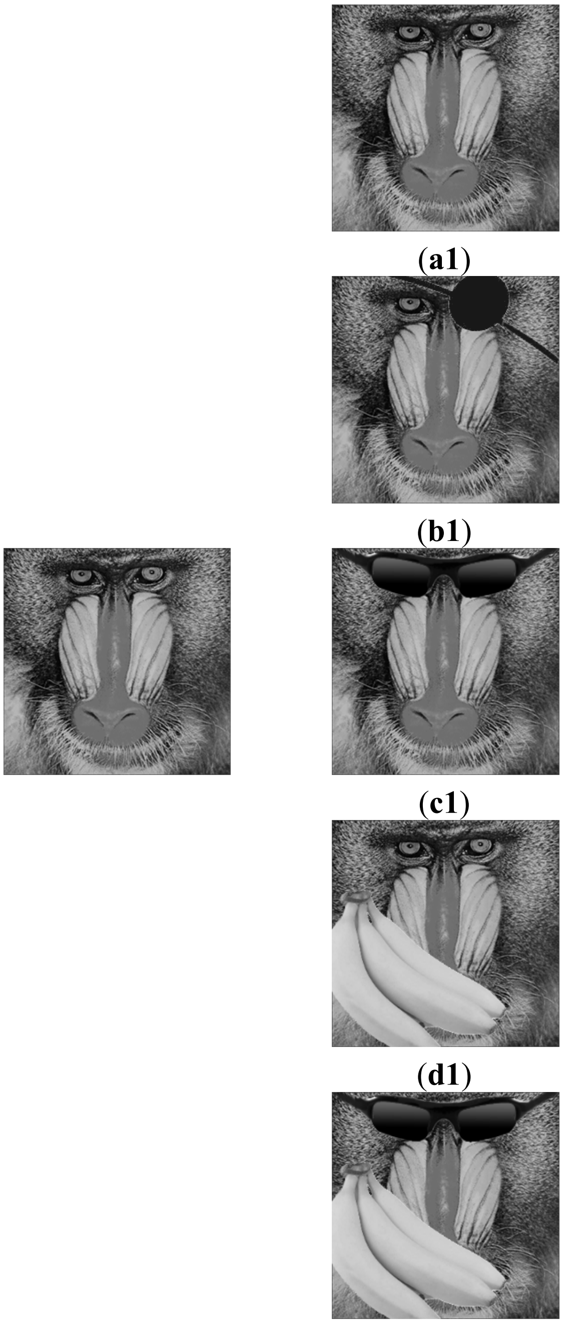
Based on the above result, Figure 10 a1 is the least modified region, and Figure 10 e1 is the most modified region. Likewise, Figure 11 a1 is the least modified region, and Figure 11 e1 is the most modified region. As mentioned above, we derive the result that the size of the modified region will affect the value of *PSNR* and *MSE*.

Figure 10. Comparison of PSNR and MSE for Lena.



Besides, we also used the Baboon image to gauge *PSNR* and *MSE*. In Figure 11a1, the *PSNR* and *MSE* values are infinite and 0, respectively, so Figure 11a1 is equal to the original image. We compare it with Figures 11b1–e1, and Figure 11e1 of the modified region is a synthesis of Figure 11c1 of the modified region and Figure 11d1 of the modified region. In Figure 11b1, the *PSNR* with *MSE* values are + 22.53 dB with + 0.01 dB, respectively. In Figure 11c1, the *PSNR* with *MSE* values are + 20.61 dB with + 0.01 dB, respectively. In Figure 11d1, the *PSNR* with *MSE* values are + 14.06 dB with + 0.04 dB, respectively. In Figure 11e1, the *PSNR* with *MSE* values are + 13.19 dB with + 0.05 dB, respectively. In Figure 11 c1–e1, the numerical comparison experiments are the same as the *PSNR* and *MSE* rules.

Figure 11. Comparison of PSNR and MSE for Baboon.



Original watermark	Analysis Image	PSNR	MSE
	(a1)	infinite	0
	(b1)	+22.53 dB	+ 0.01 dB
	(c1)	+20.61 dB	+ 0.01 dB
	(d1)	+14.06 dB	+ 0.04 dB
	(e1)	+13.19 dB	+ 0.05 dB

5. Conclusions

Rawat and Raman proposed a new watermarking scheme with chaos in which a watermark was produced by Arnold's cat map. The watermark becomes an orderless image, and is then divided into eight blocks. A chaotic watermark is obtained by using the XOR operation between the binary watermark and the binary chaotic image, and then the chaotic watermark is embedded into an orderless image of each block of the least significant bit. However, the drawback is that Arnold's cat map cannot be changed, and when r cannot change, it will lack variability and randomness. Supposing that one of the encryption images had been extracted, then the information of all images would be cracked.

In order to address this problem, we propose the chaotic system with a time-variant watermarking scheme to enhance security by using the current time t to obtain the Logistic map and Arnold's cat map. The current time decides the initial time of the Logistic map and Arnold’s cat map r times. In other words, the value of the Logistic map and Arnold's cat map depends on the current time. We can obtain the value of the chaotic binary watermark using the XOR operation between the value of the Logistic map and the value of the binary watermarked pixel. The location of the current image pixel depends on the value of Arnold's cat map and the location of the original image pixel. Therefore, the information of the binary original watermark will be more difficult to capture, because each encrypted image is manufactured at a different time. There are four advantages to our proposed scheme. First, it has high fidelity. Secondly, it enhances randomness and security. Thirdly, it protects the watermark and the watermarked image from different attacks, and finally, it can locate modified regions in watermarked images. In our further study, embedding watermarks will be applied in other fields, such as video and sound. In addition, we will discuss chaotic strategies and the cat map’s period.

Acknowledgement

The authors would like to thank the National Science Council of the Republic of China, Taiwan, for financially supporting this research under Contract No. NSC-2628-E-167-002-MY3.

Conflict of Interest

The authors declare no conflict of interest.

References

1. Koch, E.; Zhao, J. Towards robust and hidden image copyright labeling. In Proceedings of IEEE Workshop on Nonlinear Signal and Image Processing, Neos Marmaras, Greece, 20–22 June 1995; pp. 452–455.
2. Hsu, E.; Wu, J.L. Multiresolution watermarking for digital images. *IEEE Trans. Circuit Syst. II: Analog Digital Signal Process.* **1998**, *45*, 1097–1101.
3. Chang, C.C.; Chen, C.F.; Liu, L.J. A secure fragile watermarking scheme based on chaos-and-hamming code. *J. Syst. Software.* **2011**, *84*, 1462–1470.
4. Abhayaratne, C.; Bhowmik, D. Scalable watermark extraction for real-time authentication of JPEG 2000 images. *J. Real-Time Image Process.* **2011**, *6*, 1–19.
5. Lin, P.L.; Hsieh, C.K.; Huang, P.W. A hierarchical digital watermarking method for image tamper detection and recovery. *Pattern Recognit.* **2005**, *38*, 2519–2529.
6. Fridrich, J. Image watermarking for tamper detection. In Proceedings of the IEEE International Conference on Image Processing, Chicago, IL, USA, 4–7 October 1998; pp. 404–408.
7. Fridrich, J.; Goljan, M.; Baldoza, A.C. New fragile authentication watermark for images. In Proceedings of the IEEE International Conference on Image Processing, Vancouver, BC, Canada. 10-13 September 2000; pp. 446–449.

8. Dittmann, J.; Steinmetz, A.; Steinmetz, R. Content-based digital signature for motion pictures authentication and content-fragile watermarking. In Proceedings of the IEEE International Conference on Multimedia Computing Systems, Florence, Italy, 7–11 June 1999; pp. 209–213.
9. Walton, S. Information authentication for a slippery new age. *Dr. Dobbs Journa.* **1995**, *20*, 18–26.
10. Fridrich, J. Symmetric ciphers based on two dimensional chaotic maps. *Int. J. Bifurcation Chaos.* **1998**, *8*, 1259–1284.
11. Wong, P.W. A public Key watermark for image verification and authentication. In Proceedings of IEEE International Conference on Image Processing, Chicago, IL, USA, 4–7 October 1998; pp. 455–459.
12. Lagendijk, R.L.; Langelaar, G.C.; Setyawan, I. Watermarking digital image and video data: A state-of-the-art overview. *IEEE Signal Process. Mag.* **2000**, *17*, 20–46.
13. Suthaharan, S. Fragile image watermarking using a gradient image for improved localization and security. *Pattern Recognit. Letters.* **2004**, *25*, 1893–1903.
14. Wang, X.Y.; Miao, E.N.; Yang, H.Y. A new SVM-based image watermarking using Gaussian-Hermite moments. *Appl. Soft Comput.* **2012**, *12*, 887–903.
15. Cavalcante, H.L.D. de S.; Vasconcelos, G. L. Power law periodicity in the tangent bifurcations of the logistic map. *Phys. A: Stat. Mech. Appl.* **2001**, *295*, 291–296.
16. Pareek, N.K.; Vinod Patidar, Sud, K.K. Image encryption using chaotic logistic map. *Image Vision Computing.* **2006**, *24*, 926–934.
17. Hauhs, M.; Widemann, B.T. Applications of algebra and coalgebra in scientific modelling: Illustrated with the Logistic Map. *Electron. Notes Theor. Comput. Sci.* **2010**, *264*, 105–123.
18. Díaz-Méndez, A.; Marquina-Pérez, J.V.; Cruz-Irisson, M.; Vázquez-Medina, R.; Del-Río-Correa, J.L. Chaotic noise MOS generator based on logistic map. *Mater. J.* **2009**, *40*, 638–640.
19. Jie Dai, J. A result regarding convergence of random logistic maps. *Statistics Probability Lett.* **2000**, *40*, 11–14.
20. Savely, R.; Victor, M.; Shlomo, H. An explicit solution for the logistic map. *Phys. A: Stat. Mech. Its Appl.* **1999**, *264*, 222–225.
21. Leonel, E. D.; Kamphorst Leal da Silva, J.; Oliffson Kamphorst, S. Transients in a time-dependent logistic map. *Phys. A: Stat. Mech. Its Appl.* **2001**, *295*, 280–284.
22. Zhao, D.; Chen, G.; Liu W. A chaos-based robust wavelet-domain watermarking algorithm. *Chaos, Solitons Fractals.* **2004**, *22*,47–54.
23. Zhao, J.; Zhou, M.; Xie, H.; Peng, J.; Zhou X. A novel wavelet image watermarking scheme combined with chaos sequence and neural network. *Lecture Note Comput. Sci.* **2004**, *3174*, 663–668.
24. Guyeux, C.; Bahi, J.M. A new chaos-based watermarking algorithm. In Proceedings of the International Conference on Security and Cryptography (SECRYPT), Athens, Greece, 26-28 July 2010, pp. 1–4.
25. Lee, Z.J.; Lin, S.W.; Su, S.F.; Lin, C.Y. A hybrid watermarking technique applied to digital images. *Appl. Soft Computing.* **2008**, *8*, 798–808.
26. Rawat, S.; Raman, B. A chaotic system based fragile watermarking scheme for image tamper detection. *AEU-Int. J. Electron. Commun.* **2011**, *65*, 840–847.