Iran J Sci Technol Trans Electr Eng (2017) 41:103–113
DOI 10.1007/s40998-017-0021-9

RESEARCH PAPER

A Logistic Map-Based Fragile Watermarking Scheme of Digital Images with Tamper Detection

Saswati Trivedy[1] · **Arup Kumar Pal**[1]

Received: 11 March 2016 / Accepted: 19 June 2017 / Published online: 3 July 2017

Abstract Integrity protection is one of the security mechanisms used to prevent the originality of the content from illegal manipulation. In this paper, the authors have proposed an efficient fragile watermarking scheme to localize the temper region in digital images. To ensure the image integrity, the watermark information insertion is realized into the cover image using a key matrix. A logistic map-based chaotic sequence is considered to produce both the key matrix and the watermark information. The proposed scheme is able to retain high visual quality watermarked image and can precisely detect the tampered region if the image undergoes any attack by various malicious tampering methods. The effectiveness of the proposed scheme is presented by performing various malicious tampering attacks on the watermarked images. Experimental results show that the proposed watermarking scheme has achieved the satisfactory performance. The proposed scheme gives better perceptual quality of watermarked image and low false tamper detection rates compared to some other related schemes.

Keywords Fragile watermarking · Logistic map · Chaotic sequence · Tampering localization

✉ Saswati Trivedy
saswati.trivedy@gmail.com

Arup Kumar Pal
arupkrpal@gmail.com; pal.ak.cse@ismdhanbad.ac.in

[1] Department of Computer Science and Engineering, Indian Institute of Technology (ISM), Dhanbad 826004, India

1 Introduction

In today's digital world, the Internet has developed as the most suitable digital communication medium for transferring all kinds of data, especially multimedia data (image, audio, video, etc.) due to its easy and wide transmission capability. The forgery of multimedia data is considered as a serious issue since the Internet itself does not provide any security to the digital documents, so it should be a major concern to preserve the security of the data as a form of confidentiality, integrity and authenticity as it mostly consists of important personal and secret information. Based on different applications and requirements, security mechanisms like confidentiality, integrity and authenticity are used to protect the data during digital communication. Confidentiality refers to hiding information from unauthorized access and is provided by security tools such as cryptography (Stallings 2010) and steganography (Johnson and Jajodia 1998; Artz 2001). Digital Watermarking (Yeung and Mintzer 1998; Hartung and Kutter 1999; Tefas et al. 2005; Singh et al. 2013; Singh and Chadha 2013; Yu et al. 2015; Nguyen et al. 2016; Sridhar et al. 2014) provides a better result among the various tools used for checking integrity (i.e., protecting information from being modified by unauthorized parties) and authenticity (i.e., guarantee of provenance of a message). Digital watermarking refers to protection of a digital document by embedding secret information into the cover medium. One of the common attacks on the digital data is that the content can be easily manipulated by the illegitimate user in such a way that the tampering is not visually recognizable. Such type of attacks causes serious issues in medical related data. Fragile watermarking (Singh and Chadha 2013; Yu et al. 2015; Nguyen et al. 2016; Lu et al. 2003; Liu et al. 2007) is considered as one of the solutions to resolve such

issues. Fragile watermarking scheme is used for proving integrity and checking image authenticity.

Fragile watermarking is also capable of localizing these modifications. Several fragile image watermarking schemes based on chaotic maps (Liu et al. 2007; Xiao and Shih 2012; Botta et al. 2015; Wang et al. 2015) have been proposed so far. Chang et al. (2011) use a two-pass logistic map combined with hamming code to detect image modifications. The two-pass logistic map contains a private key to resist vector quantization attack and the embedding procedure is block independent. In Tsai (2013), the author combines chaotic system and wavelet tree for improving the security of watermarked image. Tong et al. (2013) use a cross chaotic map to confuse the blocks generated by the original image. This scheme uses flag and a combination of the most significant bits and the least significant bits to improve the rate of tamper detection and defense of attacks. Lambic et al. (2015) proposed a scheme for generating one-dimensional discrete chaotic map based on composition of permutation and is defined over finite set. Many other authors have proposed fragile watermarking techniques for digital images like Zhang and Wang (2009), who proposed a fragile watermarking scheme in which the least significant bits of all the image pixels carry the pixel-derived and block-derived watermark bits. At the receiver side, first the tampered block is detected then the hidden watermark data are exploited to exactly locate the tampered pixels. Aslantas et al. (2009) proposed a DCT-based fragile watermarking scheme; the watermark is embedded by modifying the least significant bits of the transformed coefficients, after watermark embedding the modified coefficients are transformed from transform domain to spatial domain which results in error due to the conversion of real numbers to integers. The intelligent optimization algorithms such as genetic algorithm, differential evolution algorithm, clonal selection algorithm and particle swarm optimization algorithm are used to correct the errors. The probability-based tamper detection scheme proposed by Hsu and Tu (2010) includes two processes, first embedding an image authentication message and second, tamper detection. The tampered area is located using the embedded authentication message and a probability theory is used to enhance authentication accuracy. Another fragile watermarking scheme (Solorio and Nandi 2011) has combined both a secure block-wise resilient to cropping mechanism and an iterative pixel-wise mechanism to improve the tampering localization and self-recovery capabilities. In Rawat and Raman (2011), the authors proposed a chaos-based watermarking scheme by employing two chaotic maps and the initial values of the chaotic maps are used as a secret key. A self-embedding fragile watermarking scheme (Zhang et al. 2013) was proposed for enhancing security using non-linear chaotic sequence. In the chaos-based fragile watermarking scheme (Munir 2015), the binary watermark is XORed with chaotic image which is generated using logistic map, the LSBs of cover image pixels are modified using the watermark bits. At the receiver side, authentication is checked by comparing the original watermark and the extracted watermark. Another fragile watermarking scheme (Yu et al. 2015) for authentication of stereo image with stereo matching technique and at detection phase the part of alterable-length watermark are used to increase accuracy of tamper localization at the receiver end.

To embed the watermark information, most of the suggested fragile watermarking schemes were devised after modifying the least significant bits of the cover image. These kinds of approaches modify the cover image directly but indirect embedding approaches are more suitable to retain the high visual quality of watermarked image. To improve the perceptual quality of watermarked image and rate of tamper detection, we propose a fragile watermarking scheme based on logistic map for tamper detection of gray scale images. The logistic map is used for generating the key sequence and the binary watermark. The scheme has enhanced the security since the watermark is embedded into the carrier image by indirect modification with reference to a key matrix.

The remainder of this paper is organized as follows. In Sect. 2, the procedure for generating chaotic sequence from logistic map is described and then the process obtaining the key matrix and binary watermark is given. In Sect. 3, the proposed fragile digital image watermarking scheme, including the watermark embedding, watermark extraction and tamper detection, is presented. In Sect. 4, the experimental results are presented to demonstrate the effectiveness of the proposed scheme. Section 5 states the conclusion about the proposed watermarking scheme.

2 Preliminaries

Prior to explaining the proposed fragile watermarking algorithm for tamper detection, we have presented the logistic map-based key generation and binary watermark generation in the following subsections.

2.1 Logistic Map Based Chaotic Sequence

Logistic map is one of the simplest chaotic maps. The Logistic map-based chaotic sequence has had wide applications in devising digital watermarking techniques during recent years. The most important characteristic of Logistic map is the sensitivity to initial conditions, which means that any small change in the initial values will produce significantly different subsequent values. So due to this

sensitivity property, the Logistic map-based sequence appears to be random. The initial values are known as the seed values and those seed values will be considered as secret keys. Only the authorized user will able to produce same sequence after using the same seed values.

In our proposed algorithm, we use logistic map for generating chaotic sequence, which is further used for generating key matrix. Here, the initial value x_0 and the positive number μ serve as secret keys and they are known as seed values. For a given initial value x_0 and μ, we get a random sequence which lies in the range between 0 and 1. If we make a very small change in the initial value, the newly generated random sequence will be significantly different from the previous one, because of the repeated iteration any small change can differentiate the sequence drastically. The logistic map is described by

$$x_i = \mu \times x_{(i-1)} \times (1 - x_{(i-1)}) \quad (1)$$

where the value of μ lies in the range of (0,4]. When the value of μ exists between $3.57 < \mu \leq 4$, the map is in chaotic state (Zhang et al. 2013; Munir 2015). As the present value X_i depends on previous value X_{i-1}, any small change results in significantly different sequence. Hence, a Logistic map-based chaotic system can be used as a pseudo-random sequence generator.

2.2 Key Generation

The elements of the chaotic sequence generated using Logistic map as described by Eq. 1 are floating point numbers in the range between 0 and 1. Here, we use the chaotic sequence obtained using Logistic map for generating a key matrix. In the proposed fragile watermarking scheme, the key matrix is of same size as that of the cover image and the value of each key matrix element will be an integer in the range from 0 to 255. We have used the algorithm 1 as described below for generating the key matrix. If our cover image is of size $m \times n$, then the Eq. 1 will be iterated i number of times, where i is equivalent to the total number of elements of a matrix of size $m \times n$. The algorithmic steps of the key matrix generation are discussed below.

Algorithm 1: Key Matrix Generation

```
Input: One dimensional chaotic sequence (CS) of length i.
Output: Key matrix (K) of size m × n
  Begin
        1. Temp_Key = round (255× CS)
        2. Rearrange the one dimensional array Temp_Key of lengthi in the
           form of a matrix of dimension m × ncalled Key matrix (K).
End
```

2.3 Watermark Generation

In the proposed scheme, we have obtained the binary watermark from chaotic sequence generated using Logistic map. As the watermark is generated using the logistic map, which increases the secrecy of embedded image and at the same time, it decreases the system payload, as the receiver can generate the key matrix and the binary watermark using the same seed values. As a small difference in seed values generates a significantly different sequence, so only the intended receiver can generate the binary watermark. In the binary watermark generation algorithm, we have used a random positive integer N less than 255. Here, N is chosen randomly to increase the secrecy. The floating point elements of the chaotic sequence are first multiplied with N and then the obtained values are rounded off to the nearest integer. Then, the integers are converted into binary form. We have used hamming weight (Sarabia and Márquez 2016) to obtain a single bit for each binary representation of each integer. These bits are to be rearranged into matrix form of size $m \times n$ same as that of cover image to obtain the binary watermark. At the receiver side, the generated watermark is compared with the extracted watermark to detect whether the received watermarked image is tampered or not and also to locate the tampered region in the received image. An example is given in Fig. 1 showing the watermark generation procedure briefly. The algorithmic steps of the binary watermark generation are presented below.

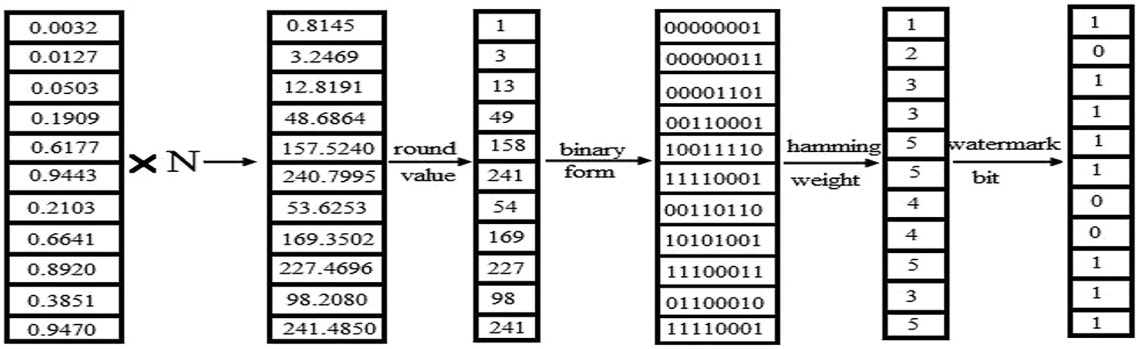

Fig. 1 Example of binary watermark generation process

Algorithm 2:Binary Watermark Generation

Input: Chaotic sequence (CS) of length i.
Output: A binary watermark (W) of same size as that of the cover image m × n
Begin

1. W'_i = round (N × CS_i), where N ∈ (0,255]
2. Convert the integers into equivalent binary representation.
3. Obtain a single bit for each of the binary numbers based on their hamming weight according to the following conditions:
   3.1 Select bit 1 if the hamming weight of the element of $W_i$is odd.
   3.2 Select bit 0 if the hamming weight of the element of $W_i$is even.
4. Rearrange the one dimensional array of length (i) into matrix called the binary watermark (W) of dimension m × n.

End

3 Proposed Scheme

This section presents the description of the proposed fragile digital image watermarking scheme for tamper detection. Our proposed watermarking algorithm is composed of three subparts: Watermark embedding, watermark extraction and tamper detection. The procedure and the algorithmic steps of the three subparts are described as follows:

3.1 Watermark Embedding

The block diagram for watermark embedding procedure is given in Fig. 2. In the Watermark Embedding section, the binary watermark generated using algorithm 2 as described in Sect. 2.3 is embedded in the cover image. The secret key matrix, the cover image and the binary watermark are of the same size $m \times n$. A difference matrix is formed by computing the absolute difference between cover image pixels and the elements of the key matrix. Embedding of a particular pixel value at (i, j)th position is dependent on the (i, j)th value of the difference matrix and the (i, j)th bit value of the watermark. The detailed algorithmic steps are described below in algorithm 3.

Algorithm 3: Watermark Embedding

Input: The gray scale cover image(C), key (K), binary watermark (W).

Output: The gray scale watermarked image.

Begin

1. Read a gray scale cover image (C) of size m×n in matrix form.
2. Find the difference (d) between the cover image (C) and the key(K) which is of same dimension m×n as of cover image.

$$d = |C-K|$$

3. For row = 1:m
4. For col = 1:n

If W(row, col) == 1

If mod (d (row, col), 2) ≠ 0

$$C'(row, col) = \begin{cases} C(row, col)+1; \text{ for } 0 \le C(row, col) < 255 \\ C(row, col) -1; \text{ for } C(row, col) = 255 \end{cases}$$

Else

$$C'(row, col) = C(row, col)$$

If end

Else

If mod (d (row, col), 2) ≠ 0

$$C'(row, col) = C(row, col)$$

Else

$$C'(row, col) = \begin{cases} C(row, col) - 1; \text{ for } 0 < C(row, col) \le 255 \\ C(row, col) +1; \text{ for } C(row, col) = 0 \end{cases}$$

If end

If end

5. For end
6. For end
7. The elements of obtained matrix C′ of size m×n is the modified image pixel values.
8. Construct the watermarked image (WI) using the matrix C′.

End

3.2 Watermark Extraction

The receiver receives the watermarked image (W_TI), *N* value and the seed value to generate chaotic sequence (CS). The receiver computes the key matrix (*k*) in the same procedure as done in the embedding process, and then the receiver performs the following procedure to extract the embedded watermark. The algorithm for watermark extraction is given below:

Algorithm 4: Watermark Extraction Process

Input: The gray-scale tampered watermarked image (W_TI), key (K).

Output: Extracted binary watermark (W_EX).

Begin

1. Read the received gray-scale watermarked image (W_TI) of size n×n in matrix form.
2. Find the difference (d') between the watermarked image (W_TI) and key matrix (K) of size m×n.
   d'=|W_TI-K|
3. For row = 1:m
4. For col = 1:n
   If mod (d'(row, col),2)== 0
   W_EX(row, col) = 1
   Else
   W_EX(row, col) = 0
5. End if
6. End for
7. End for
8. W_EX is the extracted watermark.

End

3.3 Tamper Detection

The receiver generates the chaotic sequence (CS) using the seed value. The proposed scheme is a blind scheme, so for checking the integrity of the received image the receiver generates the binary watermark (W) in the same process as it is generated at the sender side. If the watermarked image is tampered during transmission before reaching the receiver, it can be identified by comparing the extracted watermark with the original generated watermark at the receiver side. So the image authentication can be proved without sending the original watermark or the cover image. The following algorithm describes the procedure for tamper detection.

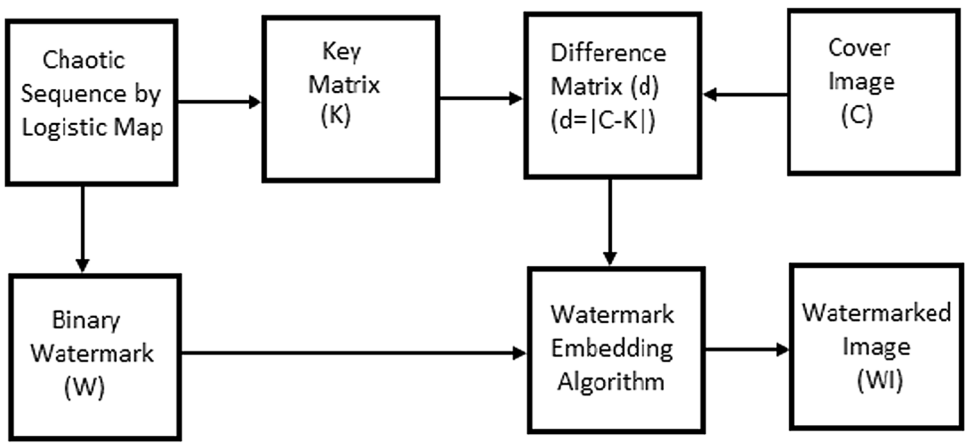

Fig. 2 The watermark embedding procedure

Algorithm 5: Tamper detection process

```
Input: The original watermark (W) generated at the receiver side, the
extracted watermark (W_EX) and the received watermarked image (W_TI).

Output: Tamper detected image (T_WI)

Begin

1. Compute the difference between original watermark (W) and the
   extracted watermark (W_EX) both of size m×n to find the matching
   values where the original watermark and the extracted watermark
   have the same values.
   D''=(W - W_EX)
2. For row = 1:m
3. For col = 1:n
4. If d''(row, col) ≠ 0
       T_WI (row, col) = 0
   Else
       T_WI (row, col) = W_TI (row, col)
5. End if
6. End for
7. End for
8. Reconstruct the tamper detected image using elements of matrix T_WI
   of size m×n.

End
```

The following figure (Fig. 3) describes the procedure of watermark extraction and tamper detection.

3.3.1 Example

An example is given below briefly showing the tamper detection procedure. At first, watermark is extracted from the received watermarked image as shown in Fig. 4b. Then, the original watermark is generated using received seed values as described in Sect. 2.3 as given in Fig. 4c. Next, we match the watermark bits of each position (i, j). If at a particular position the extracted and generated watermark bits do not match, we substitute the pixel value of that position with zero and other pixel values remain. The tampered position is represented by black as shown in Fig. 4d.

4 Experimental Results

The proposed scheme is implemented and a set of standard gray scale images is tested, but in this paper we have presented results for four standard gray scale images of size 256 × 256. The original test images are shown in Fig. 5. The experimental results are presented to show the effectiveness of the scheme.

4.1 Tamper Detection and Location Evaluation

The original Lena image as shown in Figs. 5a and 6a presents the watermarked Lena image. Tampered Lena image is shown in Fig. 6b, c represents the actual tampered areas for the Lena image and Fig. 6d shows the tamper detected areas by our proposed tamper detection scheme.

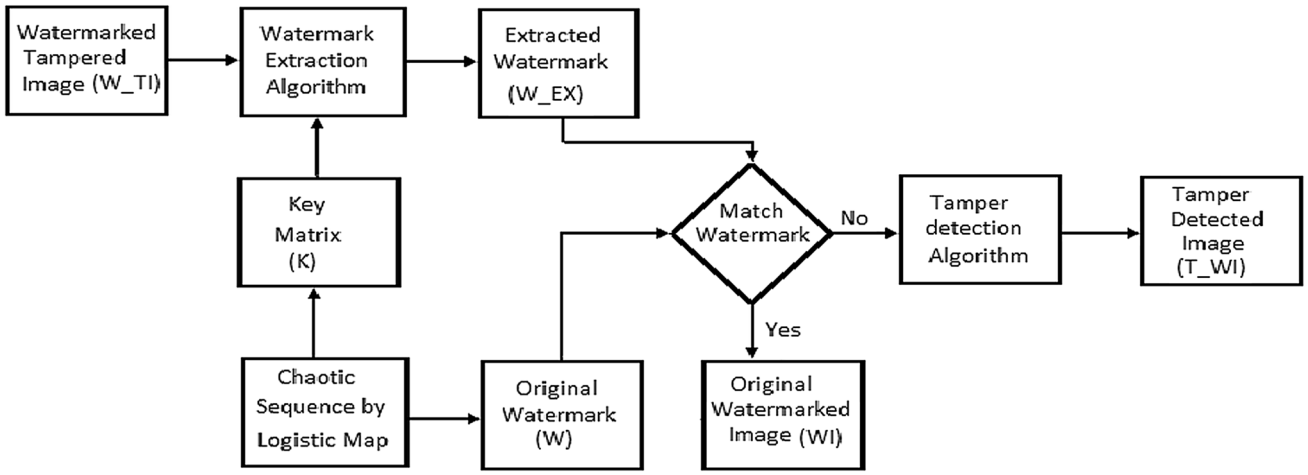

Fig. 3 The watermark extraction and tamper detection procedure

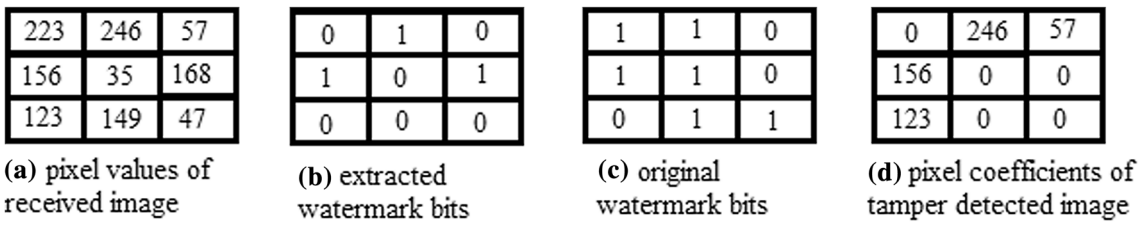

Fig. 4 Example of tamper detection procedure

The three other images used in the experiment have been altered in some other way. In the watermarked Pepper image, the direction of one of the vegetables has been altered (Fig. 7); in the Cameraman image the tower in the background has been removed (Fig. 8), and the background of the Barbara image has been modified (Fig. 9).

4.2 Perceptual Quality

The metric peak signal to noise ratio (PSNR) is used to evaluate the visual quality of the watermarked image. The PSNR is defined as:

$$\mathrm{PSNR} = 10\log_{10}\left[\frac{(2^{n}-1)^{2}}{\mathrm{MSE}}\right] \tag{2}$$

where n is the number of bits value of the signal, (typically $n = 8$, for an gray scale image). The mean square error (MSE) is computed by Eq. (3) given below:

$$\mathrm{MSE} = \frac{\sum_{i,j}[C(i,j) - \mathrm{WI}\ (\mathrm{i},\mathrm{j})^{2}}{M \times N} \tag{3}$$

where M and N are the width and length of the image, respectively, and $C(i, j)$ and WI (i, j) represent the pixel values of the ith row and jth column of the original image and the corresponding watermarked image, respectively.

The four watermarked images are shown in Figs. 6a, 7a, 8a and 9a. The PSNR values of the four images after embedding watermark are 51.1379, 51.1163, 51.1774 and 51.1465 dB, respectively. Table 1 shows the PSNR values of the watermarked images. The performance of the proposed scheme in terms of PSNR is high, with the average of 51.145 dB, which indicates that the watermarked images have good visual quality.

4.3 Comparison of Performance

The False-Positive rate and the False-Negative rate are also an important parameter to evaluate the performance of any fragile watermark scheme. The values of False-Positive rate and the False-Negative rate should be kept very low for watermarking systems. False-Positive pixels are the number of pixels that are identified as tampered when in fact they have not been tampered and False-Negative pixels are the number of pixels that are identified as not tampered, but in fact they have been tampered. True-Positive pixels are the number of pixels that are identified as having been tampered and indeed they are tampered, whereas True-Negative pixels are the number of pixels that are recognized as not having been tampered but actually they have not been tampered.

Let FN be the number of False-Negative pixels, FP be the number of False-Positive pixels, TN be the number of

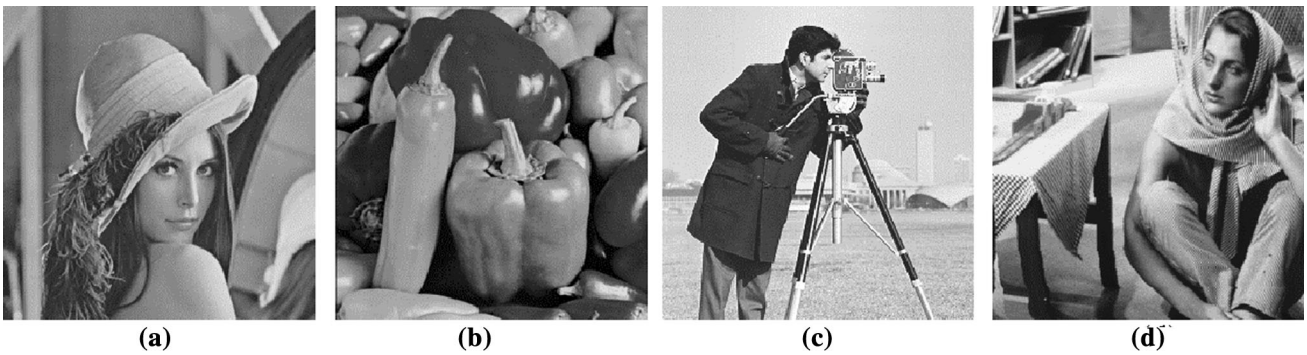

Fig. 5 Original test images of 256 × 256 pixels; **a** lena, **b** pepper, **c** cameraman and **d** barbara

Fig. 6 **a** The watermarked Lena, **b** tampered Lena, **c** actual tampered areas, and **d** located tampered areas

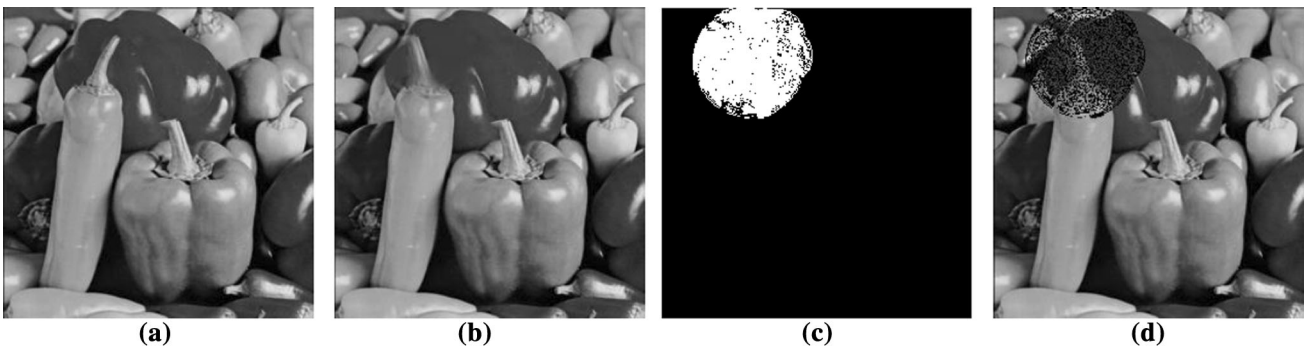

Fig. 7 **a** The watermarked Pepper, **b** tampered Pepper, **c** actual tampered areas, and **d** located tampered areas

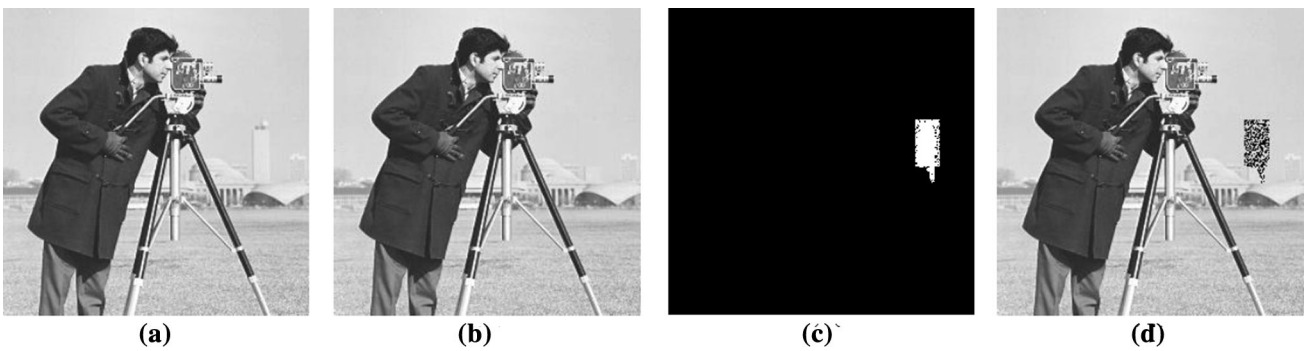

Fig.8 **a** The watermarked cameraman, **b** tampered cameraman, **c** actual tampered areas, and **d** located tampered areas

Fig.9 **a** The watermarked barbara, **b** tampered barbara, **c** actual tampered areas, and **d** located tampered areas

Table 1 The PSNR values (dB) of the watermarked images by the proposed scheme

Lena	Pepper	Cameraman	Barbara
51.138	51.116	51.177	51.147

Table 2 Comparisons of the proposed scheme with those developed by Chang et al. and Hsu and Tu with respect to Lena image

Scheme	PSNR	FNR	FPR
Proposed	51.14	0.00018	0.00012
Chang et al. (Chang et al. 2011)	37.76	0.00070	0.00430
Hsu and Tu (Hsu and Tu 2010)	44.18	0.00100	0.00420

True-Negative pixels, and TP be the number of true-positive pixels. Then, the false-negative rate (FNR), and false-positive rate (FPR) used to measure tampering detection accuracy are defined as follows (Yeung and Mintzer 1998; Hartung and Kutter 1999):

$$\mathrm{FNR} = \mathrm{FN} / (\mathrm{FN} + \mathrm{TP}) \quad (4)$$

$$\mathrm{FPR} = \mathrm{FP} / (\mathrm{FP} + \mathrm{TN}) \quad (5)$$

To further evaluate the performance of the proposed fragile watermarking scheme for digital images, the values of False-Positive Rate, False-Negative Rate and PSNR obtained from our scheme are compared with the values that are obtained by Chang et al. (2011) and Hsu and Tu (2010) for Lena image.

The comparison of FNR and FPR values obtained by our proposed scheme and with other schemes (Chang et al. and Hsu and Tu) for Lena image is given in Table 2.

4.4 Effectiveness and Applications of Proposed Scheme

The proposed method is an effective fragile watermarking scheme for gray scale images that can precisely detect and locate tampered areas. The proposed scheme is suitable for applications that require image authentication and integrity when images are stored and transmitted over the internet. As the key matrix and the binary watermark are generated using the chaotic sequence and secret value N, this increases the security of proposed method and decreases the data load over internet during transmission.

5 Conclusions

In this paper, a fragile digital image watermarking method based on chaotic sequence has been presented. The chaotic sequence is generated using logistic map; the key matrix and binary watermark are obtained from chaotic sequence. The proposed scheme can detect pixel-level tampering in the watermarked image. Experimental result shows that the method gives watermarked images of high PSNR values with an average of approximately 51 dB, and the false detection rate is very low. The proposed scheme can prove image authentication by precisely locating the tampered areas after various image manipulating attacks. As per the experimental result, it can be stated that the proposed scheme is an effective, efficient and secure digital image watermarking scheme for detecting tamper region.

References

Artz D (2001) Digital steganography: hiding data within data. Internet Comput IEEE 5(3):75–80

Aslantas V, OzerS Ozturk S (2009) Improving the performance of DCT-based fragile watermarking using intelligent optimization algorithms. Optics Commun 282(14):2806–2817

Botta M, Cavagnino D, Pomponiu V (2015) A successful attack and revision of a chaotic system based fragile watermarking scheme for image tamper detection. AEU Int J Electron Commun 69(1):242–245

Chang CC, Chen KN, Lee CF, Liu LJ (2011) A secure fragile watermarking scheme based on chaos-and-hamming code. J Syst Softw 84(9):1462–1470

Hartung F, Kutter M (1999) Multimedia watermarking techniques. 87:1079–1107

Hsu CS, Tu SF (2010) Probability-based tampering detection scheme for digital images. Optics Commun 283:1737–1743

Johnson NF, Jajodia S (1998) Exploring steganography: seeing the unseen. Computer 31(2):26–34

Lambić D (2015) A new discrete chaotic map based on the composition of permutation. Chaos, Solitons Fractals 78:245–248

Liu SH et al (2007) An image fragile watermark scheme based on chaotic image pattern and pixel-pairs. Appl Math Comput 185(2):869–882

Lu H, Shen R, Chung FL (2003) Fragile watermarking scheme for image authentication. Electron Lett 39(12):898–900

Munir R (2015) A chaos-based fragile watermarking method in spatial domain for image authentication. International Seminar on Intelligent Technology and Its Applications (ISITIA) 227–232

Nguyen TS, Chang CC, Yang XQ (2016) A reversible image authentication scheme based on fragile watermarking in discrete wavelet transform domain. AEU Int J Electron Commun 70(8):1055–1061

Rawat S, Raman B (2011) A chaotic system based fragile watermarking scheme for image tamper detection. AEU Int J Electron Commun 65(10):840–847

Sarabia MG, Márquez CR (2016) Generalized hamming weights and some parameterized codes. Discrete Math 339(2):813–821

Singh P, Chadha RS (2013) A survey of digital watermarking techniques, applications and attacks. Int J Eng Innov Technol (IJEIT) 2(9):165–175

Singh YS, Devi BP, Singh KM (2013) A review of different techniques on digital image watermarking scheme. Int J Eng Res 2(3):193–199

Solorio SB, Nandi AK (2011) Secure fragile watermarking method for image authentication with improved tampering localisation and self-recovery capabilities. Signal Process 91(4):728–739

Sridhar K et al (2014) Comparison of digital watermarking with other techniques of data hiding. (IJCSIT) Int J Comput Sci Inf Technol 5:350–353

Stallings W (2010) Cryptography and network security, principles and practice, 5th edn. Prentice Hall, New York

Tefas A, Nikolaidis N, Pitas I (2005) Watermarking techniques for image authentication and copyright protection. In: Bovik A (ed) Communications, networking and multimedia, handbook of image and video processing. Academic Press, Burlington, pp 1083–1109

Tong X, Liu Y, Zhang M, Chen Y (2013) A novel chaos-based fragile watermarking for image tampering detection and self-recovery. Signal Process Image Commun 28(3):301–308

Tsai MJ (2013) Wavelet tree based digital image watermarking by adopting the chaotic system for security enhancement. Multimedia Tools Appl 52:347–367

Wang B, Zhou S, Zheng X, Zhou C, Dong J, Zhao L (2015) Image watermarking using chaotic map and DNA coding. Optik Int J Light and Electron Optics 126(24):4846–4851

Xiao D, Shih FY (2012) An improved hierarchical fragile watermarking scheme using chaotic sequence sorting and subblock post-processing. Optics Commun 285:2596–2606

Yeung M, Mintzer F (1998) Invisible watermarking for image verification. J Electron Imaging 7(3):578–591

Yu M et al (2015a) New fragile watermarking method for stereo image authentication with localization and recovery. AEU Int J Electron Commun 69(1):361–370

Yu M, Wang J, Jiang G, Peng Z, Shao F, Luo T (2015b) New fragile watermarking method for stereo image authentication with localization and recovery. AEU Int J Electron Commun 69(1):361–370

Zhang X, Wang S (2009) Fragile watermarking scheme using a hierarchical mechanism. Signal Process 89(4):675–679

Zhang J, Zhang Q, Hi Lv (2013) A novel image tamper localization and recovery algorithm based on watermarking technology. Optik Int J Light Electron Optics 124(23):6367–6371