Two Fragile Encryption-Watermarking Combined Schemes for Image Authentication with Tamper Detection and Localization

M.A. Mohamed, Abdelhameed Ibrahim
Faculty of Engineering, Mansoura University
Mansoura, Egypt

M.G. Abd-El-Fattah, A.S. Samrah
Faculty of Engineering, Mansoura University
Mansoura, Egypt

ABSTRACT
This paper presents two fragile watermarking schemes for digital image authentication with tamper detection and localization. We combine a proposed chaos-based encryption algorithm with the two schemes in order to improve the security, tamper detection sensitivity and tamper localization accuracy of the two schemes. The first proposed fragile watermarking scheme can be classified as a block-based scheme that divides the cover image into non-overlapping 4×4 blocks. We generate an 8-bit authentication watermark for each cover image block based on the block contents and then we use the proposed chaos-based encryption algorithm to encrypt this watermark. These encrypted 8-bit watermark are then embedded into the least significant bits (LSBs) of the highest intensity eight pixels of the block. On the other hand, the second proposed watermarking scheme can be classified as a wavelet-based scheme which uses an external secret watermark. This watermark is encrypted using the proposed chaos-based encryption algorithm. We decompose the cover image using Discrete Wavelet Transform (DWT) and then we use the encrypted watermark to update the approximation coefficients (LL sub-band) of the image. Various experimental tests are carried out to evaluate the performance of the two schemes. Experimental results demonstrate that the two proposed schemes can detect and localize tampering attacks accurately. The two schemes also achieve high degree of imperceptibility performance. Compared to some fragile watermarking schemes, our proposed schemes are more secure and efficient.

General Terms
Watermarking, Algorithms, Security.

Keywords
Fragile Watermarking, Tamper detection, Image Authentication, Discrete Wavelet Transform (DWT).

1. INTRODUCTION
The expansion of the internet in the past years has rapidly increased the availability of digital multimedia data such as audio, images and videos to the public. This digital data can be easily manipulated, tampered, and distributed with the help of powerful multimedia editing tools which are now readily available on personal computers [1]. Insuring digital multimedia content authentication has therefore become an important issue in applications where verification of integrity and authenticity of the multimedia content is essential. Recently, digital watermarking techniques have been considered as one of the most promising techniques for image content authentication. Digital watermarking schemes can be classified based on robustness into fragile, semi-fragile and robust watermarking schemes [2]. Fragile watermarking schemes are well suited for image content authentication because any attempt to modify the content of an image will alter or destroy the fragile watermark. Various fragile watermarking schemes have recently been proposed for verifying the integrity and authenticity of the image content. In general, fragile watermarking schemes can be classified into two main categories: block-based schemes [3-8] and pixel-based schemes [9-13].

In block-based Schemes, the image is divided into sub-blocks and the watermarking information is embedded into each and every block. Each individual block is authenticated by the successful retrieval of the watermark embedded in it. If the watermark of a particular sub-block is not retrieved successfully, then that sub-block alone is identified to be tampered and the remaining parts of the image are authenticated. In [3], a block-based technique which is based on self-embedding was proposed. The authors have proposed two techniques to prove the image integrity. The first technique is based on quantization of block-based Discrete Cosine Transform (DCT) coefficient and represented as 64 or 128 bits. In the second technique a new image is produced by reducing gray level of the original image. If some modification is done on watermarked image then the quantized DCT coefficient and the new reduced gray level image can be used to reconstruct the principal content of the tampered area. In [4], a block-based fragile watermarking scheme based on scramble encryption is proposed. In that algorithm, the watermark derived from a block was randomly distributed on to the LSB of the whole image. A self-recovery watermarking technique is proposed in [5]. This proposed scheme embeds the encrypted feature comprising 6-bit recovery data and 2-bit key-based data of the image block into the LSB of its mapping block. The validity of a test block is determined by comparing the number of inconsistent blocks in the 3×3 block neighborhood of the test block with that of its mapping block. The 3×3 block-neighborhood is also used to recover the tampered blocks whose feature hidden in another block is corrupted. An approach in transform domain is proposed in [6]. In this approach the watermark bits are embedded into the middle frequency region of each block after applying Slant transform (SLT) of the host image. The host image is further compressed and then embedded into the LSBs of the watermarked image for subsequent self-restoration. The tampered regions of the watermarked image can be detected and localized by extracting the embedded watermark to compare with the original watermark for authentication. Localized tampered regions are self-recovered by extracting the LSBs of the watermarked image. A

reversible image authentication scheme based on residual histogram shifting had been proposed in [7] to protect the image integrity of the grayscale images. J. C. Chuang et al. proposed an image tamper detection and recovery scheme for grayscale images in [8]. In this scheme, the compressed codes of vector quantization are used to recover the tamper areas. In general, block-based fragile watermarking schemes have some limitations. One of these limitations is the tamper detection resolution which is based on the block size of the image blocks. Therefore a particular block in which some pixels are modified and the rest are correct may be considered as a tampered block. Hence notion of pixel-based fragile watermarking came into picture in which any alteration in the value of a watermarked pixel will be responsible for wrong value of watermark in further calculation at the receiver side hence one can easily recognize altered pixel with high precision.

In pixel-based watermarking schemes, watermark information embedded into the cover image pixels. If gray scale value of any pixel is changed then embedded watermark corresponding to that pixel will also be changed hence one can easily localize the each altered pixel [9]. In these schemes, an image is scanned in a certain order to embed the watermark. The scan order may be public or secret. A pixel wise fragile watermarking scheme is proposed in [10]. In this technique seven Most Significant Bit (MSB) of a gray value is given as an input to the hash function. The hash value for each pixel which is either 0 or 1 is embedded into the first LSB of corresponding pixel. Any change in the pixel value will return wrong hash value and altered pixel can be identified easily. In [11] a statistical watermarking technique for accurately localizing tampered pixel is proposed. In this algorithm a set of tailor-made authentication data for every pixel is calculated with some additional test data and embedded into the host image. On the receiver side by examining the pixels and their respective authentication data, one can reveal the exact pattern of the content alteration. Another algorithm which is based on self-embedding technique is proposed in [12]. The authors used the function of composite chaotic iterative dynamic system. According to the value of the specific position in chaotic iterative sequence and the seed value, one can get the watermarking information used for embedding in LSBs. Here only a single pixel value is used for self-authentication. That authentication bit is embedded in the lowest significant bit of the pixel's gray scale value. This algorithm utilizes the sensitiveness and randomness of the composite chaotic iterative dynamic system and does not require any additional information for localizing the pixel. A novel fragile watermarking scheme using hierarchical mechanism is proposed in [13]. In this technique pixel-wise and block-wise watermark data, which are derived from MSBs are used to directly replace all the LSBs of a host image. On the receiver side, after identifying the blocks containing tampered content, the watermark data hidden in the rest blocks are exploited to exactly locate the tampered pixels.

Recently, the researchers have focused on wavelet-based watermarking schemes for image authentication since VQ attack and oracle attack are not possible in wavelet domain model. Hence, it is more secure than the other two models [14]. In this model, DWT is applied to the original image to obtain the four sub-bands LL, HL, LH and HH. The watermark used here is usually a random binary string or a logo kind of image. The watermark bits are embedded in either of the sub-bands. Embedding data in high frequency sub-bands generates watermarked images with less distortion. The watermark bits are embedded in sub-bands by modifying the wavelet coefficients. To improve security, the coefficients can be selected in random order. D. Kundur and D. Hatzinakos embed a watermark in the quantized DWT domain in [15]. G. Yu et al. [16] embed a watermark in the average values of a number of wavelet coefficients in one of the detail sub-bands. X. Zhou et al. [17] proposed an algorithm to embed a signature from the original image into the wavelet coefficients. H. Kang and J. Park [18] incorporate the just noticeable differences feature to better discriminate malicious from non-malicious attacks. Y. Hu and D. Han [19] proposed to extract image features from low-frequency wavelet coefficients to generate two watermarks: one for classifying the intentional content modification and the other for indicating the modification location. H. Liu et al. [20] use DWT-based Zernike moments as features for the authentication task. Y. Zhu et al. [21] apply the block-mean-based quantization strategy to embed the inter-block and intra-block signatures in the DWT domain for tamper detection and localization, respectively. H. Yang and X. Sun [22] embed the watermark by integrating the human visual system model to modify the vertical and horizontal sub-bands of image sub-blocks. S. Che et al. [23] use the dynamic quantized approach to embed watermark in low-frequency wavelet coefficients. C. Cruz et al. [24] employ the vector quantization method to embed a robust signature into the approximation sub-band of each image sub-block. However, all these schemes are only robust to JPEG compression with compression ratio of higher than 50% or 60% quality factor.

More recently, chaotic maps have been used for digital watermarking, to increase the security. The most attractive features of chaos in information hiding are its extreme sensitivity to initial conditions and the outspreading of orbits over the entire space. These special characteristics make chaotic maps excellent candidates for watermarking and encryption [25]. Chaos-based encryption algorithms have suggested several advantages over the traditional encryption algorithms such as high security, speed, reasonable computational overheads and computational power [26]. It can be therefore combined with fragile watermarking to provide high confidentiality and integrity for image content authentication.

In this paper, two fragile watermarking schemes for image authentication with tamper detection and localization are proposed. Unlike the traditional fragile watermarking schemes, a proposed chaos-based encryption algorithm based on a 2D logistic map is combined with the two proposed watermarking schemes to improve the tamper detection and localization accuracy through enhancing the schemes fragility and to provide additional level of security. The first proposed fragile watermarking scheme can be classified as a block-based scheme that divides the cover image into non-overlapping 4×4 blocks. We generate an 8-bit authentication watermark for each cover image block based on the block contents and then we use the proposed chaos-based encryption algorithm to encrypt this watermark. These encrypted 8-bit watermark are then embedded into the least significant bits (LSBs) of the highest intensity eight pixels of the block. On the other hand, the second proposed watermarking scheme can be classified as a wavelet-based scheme which uses an external secret watermark. This watermark is encrypted using the proposed chaos-based encryption algorithm. We decompose the cover image using Discrete Wavelet Transform (DWT) and then we use the encrypted watermark to update the approximation coefficients (LL sub-band) of the image. The remainder of this paper is organized as follows: Overview and details of the proposed chaos-based encryption

algorithm are described in Section 2. In Section 3 Details of the two proposed fragile watermarking schemes are introduced. In Section 4, the experimental results are presented to demonstrate the effectiveness of the two proposed fragile watermarking schemes. Conclusions are finally introduced in Section 5.

2. CHAOS-BASED ENCRYPTION ALGORITHM

2.1 Overview on Chaos-Based Encryption

Chaos theory [27-28] describes the behavior of certain nonlinear dynamic systems that under specific conditions exhibit dynamics that are highly sensitive to initial conditions. The chaos-based encryption has suggested a new and efficient way to deal with the intractable problem of fast and highly secure image encryption. It provides a good combination of speed, high security, complexity, reasonable computational overheads and computational power. Chaos-based encryption algorithms are usually composed of two processes generally: (i) chaotic confusion of pixel positions by permutation process and (ii) diffusion of pixel grey values by diffusion process.

2.2 Choosing the chaotic map

Choosing chaotic maps for encryption algorithms is a critical task and one should consider only maps with the following properties [29]:

(i) Mixing property: the mixing property or in other words, sensitivity to initial conditions, is closely related to property of diffusion in encryption algorithms that implies spreading out of the effect of a single plaintext digit over many cipher text digits.

(ii) Robust chaos: The keys of an encryption algorithm represent its parameters. A good encryption algorithm spreads also the influence of a single key digit over many digits of cipher text. Therefore, we should consider only such transformations in which both parameters and variables are involved in a sensitive way.

(iii) Sufficient number of Parameters: One should consider only systems that have robust chaos for large set of parameters (keys).

In this paper, our proposed chaos-based encryption algorithm is based on the 2D logistic map which has the pervious properties [30]. We combine the encryption algorithm with the two fragile watermarking schemes to (i) improve the tamper detection and localization accuracy of the schemes, (ii) enhance the schemes fragility and (iii) provide additional level of security to the two schemes.

$$x(n+1) = ax(n)\big(1 - x(n)\big) + by^2(n) \quad (1)$$

$$y(n+1) = cy(n)\big(1 - y(n)\big) + d(x^2(n) + x(n)y(n) \quad (2)$$

When 2.75< a<3.4, 0.15< b<0.21, 2.7< c<3.45, 0.13< d<0.15, the system comes into chaotic state and can generate a chaotic sequence in the interval (0, 1]. The proposed encryption algorithm uses $a = 3.1, \mathrm{b} = 0.19, \mathrm{c} = 2.75, \mathrm{d} = 0.15$.

2.3 The Proposed Chaos-Based Encryption Algorithm

Let us call the input plain data as "D" and the output encrypted data as "D_E". We encrypt the plain data using the following steps:

(i) Reshape the plain data "D" to be a vector "D_r" of length l.

(ii) Generate two chaotic vectors "V_1" and "V_2" of length l by iterating the 2D logistic map l times to generate the required number of elements.

(iii) Generate two vectors "V_{R1}" and "V_{R2}" using the following equation:

$$V_{Ri} = round\big((V_i .* 10^{14}) mod 255\big); i = 1,2. \quad (3)$$

(iv) The permutation stage: (1) arrange the two vectors "V_1" and "V_2" in ascending or descending order and store the indices of the two arranged vectors, (2) use these indices to, sequentially, permute the "D_r" vector and generate the permuted "D_P" vector.

(v) The diffusion stage: determine the encrypted data "D_E" using the following equation:

$$D_E(1) = D_p(1) \oplus V_{R1}(1)$$
$$D_E(i) = D_p(i) \oplus D_E(i-1) \oplus V_{R1}(i) \oplus V_{R2}(i);\ 2 \le i \le l \quad (4)$$

(vi) Decryption algorithm: the plain data "D" can be determined by applying the same steps but in reversed order to decrypt the encrypted data "D_E".

3. THE PROPOSED FRAGILE WATERMARKING SCHEMES

3.1 The First Proposed Watermarking Scheme

The first proposed scheme can be considered as a modified version of Sumalatha et al. [31] scheme. The imperceptibility performance and the tamper detection and localization accuracy of the Sumalatha et al. scheme are good but they can be further improved. The authentication process of Sumalatha et al. scheme is based on 4-bit content watermark that is generated for each block. The first proposed scheme improves the tamper detection and localization accuracy of the Sumalatha et al. scheme by using (i) the proposed chaos-based encryption algorithm which increases the scheme sensitivity and security and (ii) different authentication strategy based on 8-bit content watermark for each block. The first proposed scheme improves the imperceptibility performance and the tamper detection and localization accuracy of the Sumalatha et al. scheme as illustrated in the experiment results. General block diagrams of embedding and extracting processes of the first proposed scheme are shown in Fig.1 and Fig.2, respectively.

3.1.1 Watermark Generation and Embedding Process

(i) Read the cover image "I" and then set its LSBs to zero. Let we call the resultant image as "I_L".

(ii) Divide "I_L" into 4×4 non-overlapping blocks and then reshape each block to be a vector of 16 elements. Let us call this vector as "P_k" ; $k = 1,2,..,16$.

(iii) Calculate the block 8-bits watermark value as follows:

a) $xp(i) = \oplus_{i=1}^{8} \big(P_l, P_{l+1}, K(i)\big)$ (5)
Where '⊕' represents the bitwise XOR operation, l is incremented every round by two and $K(i)$ is a secret integer number selected from the interval [0,255] and this number is updated for every round.

b) The eight values of "xp" are XORed with each other to generate the block authentication watermark "W_B":
$W_B = \oplus_{i=1}^{8} \big(xp(i)\big)$ (6)

c) Represent the block authentication watermark in binary format as 8-bits and then encrypt these 8-bits

using the proposed chaos-based encryption algorithm.

(iv) Select the highest intensity eight pixels of the "I_L" 4×4 block, starting from the upper-left pixel and moving, row by row, towards the lower-right pixel of that block.

(v) Embed the 8-bits encrypted watermark of each 4×4 cover image block into the LSBs of the highest intensity eight pixels of that block.

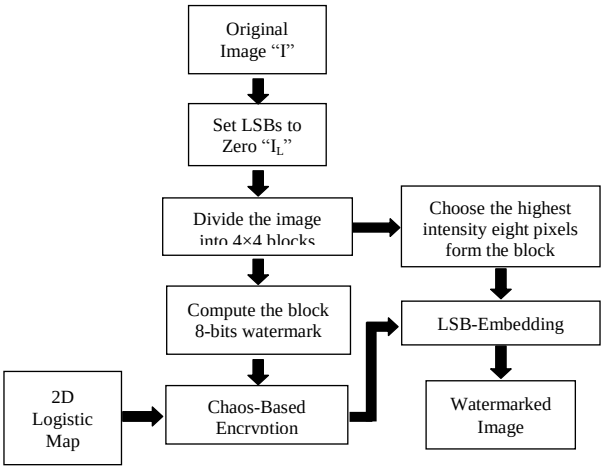


Fig.1: The embedding process block diagram of the first proposed scheme

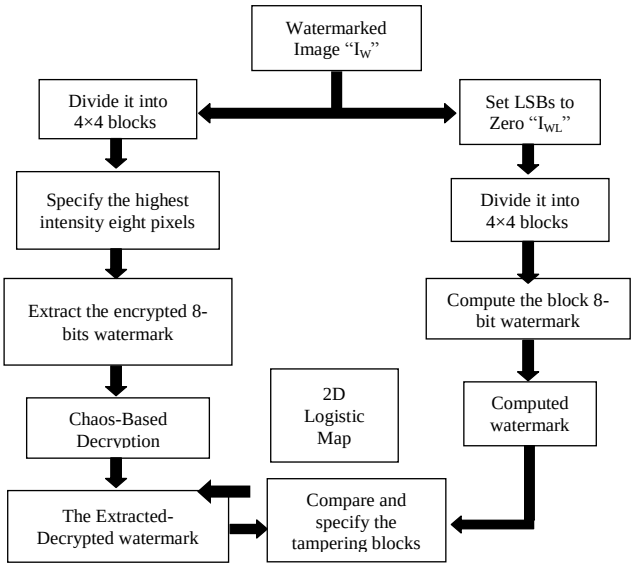


Fig.2: The extraction process block diagram of the first proposed scheme

3.1.2 Tamper Detection and Extraction Process

(i) Read the watermarked image "I_W" and then set its LSBs to zero. Let we call the resultant image as "I_{WL}".

(ii) Divide "I_{WL}" into 4×4 non-overlapping blocks and then reshape each block to be a vector of 16 elements, P_k, since $k = 1,2,..,16$.

(iii) Calculate the 8-bits authentication watermark "W_C", for each block, just as step (iii) in the embedding process.

(iv) Select the highest intensity eight pixels of the "I_{WL}" 4×4 block, starting from the upper-left pixel and moving, row by row, towards lower-right pixel of that block.

(v) Extract the 8-bits encrypted watermark "W_{EXE}" from the LSBs of the selected pixels of the watermarked image "I_W" block.

(vi) Decrypt the extracted encrypted watermark "W_{EXE}" to get the extracted decrypted watermark "W_{EXD} " of the "I_W" block.

(vii) For each "I_W" block: compare the extracted decrypted watermark "W_{EXD}" with the calculated authentication watermark "W_C" using the following equation to identify the tampered blocks:

$$BT = W_{EXD} \oplus W_C \tag{7}$$

The "I_W" block is considered to be authentic if the *BT* is equal to '0'; otherwise, it is marked as a tampered block.

The first proposed scheme can be also used for color images by, simply, repeating all pervious steps for each color component of the image.

3.2 The Second Proposed Watermarking Scheme

The second proposed watermarking scheme considered as a modified version of Wu et al. [32] scheme. We notice that the imperceptibility performance and tamper detection accuracy of Wu et al. scheme are good, but still needed to be improved. For the second proposed scheme, we use: (i) the proposed chaos-based encryption algorithm to improve the tamper detection accuracy and the security of the scheme, and (ii) watermark embedding strategy in wavelet domain to improve the imperceptibility performance of the scheme. Experimental results demonstrate that the second proposed scheme improves the tamper detection accuracy and the imperceptibility performance over the Wu et al. scheme. The block diagrams of embedding and extracting process of the first proposed are shown in Fig.3 and Fig.4, respectively.

3.2.1 The Embedding Process

(i) Use DWT to decompose the cover image "*I*" into LL, HL, LH and HH sub-bands.

(ii) Select a secret watermark "*W*" and reformulate it to be of the same size of LL sub-band.

(iii) Encrypt the watermark using the chaos-based encryption algorithm. Let us call the encrypted watermark as "W_E".

(iv) Round the LL sub-band coefficients to the nearest integer value and then select a number "*n*" of the LSBs of these coefficients to embed the watermark. Robustness and imperceptibility performances of this scheme are guaranteed by the number "*n*".

(v) Use the encrypted watermark "W_E" to update the "n" LSBs of LL sub-band coefficients as follows:

$$\text{n LSBs} = \begin{cases} \text{ones in binary format} & \text{if } W_E = 1 \\ \text{zeros in binary format} & \text{if } W_E = 0 \end{cases} \tag{8}$$

(vi) Use Inverse DWT (IDWT) of the watermarked LL sub-band "LL_W", HL, LH and HH sub-bands to obtain the watermarked image "I_W".

3.2.2 The Extraction and Tamper Detection Process

(i) Apply DWT on the watermarked image "I_W" to determine the watermarked LL sub-band "LL_W".

(ii) Extract the "*n*" LSBs from the LL_W sub-band coefficients and represent these bits in decimal format. We can determine the extracted encrypted watermark image "W_{EXE} " using the following equation:

$$W_E = \begin{cases} 1 & \text{if } \text{dec}(\text{n LSBs}) \geq T \\ 0 & \text{if } \text{dec}(\text{n LSBs}) < T \end{cases} \tag{9}$$

Where T is the threshold value and it is simply given by: $T = n/2$.

(iii) Decrypt the extracted encrypted watermark "W_{EXE}" to determine the extracted decrypted watermark image "W_{EXD}".

(iv) Resize the secret watermark "W" and the extracted decrypted watermark "W_{EXD}" to be of the same size of the cover image and then round their values to be binary values (0s or 1s).

(v) Compare "W_{EXD}" with the secret watermark "W" to identify the tampered regions in the image using the following equation:

$$WT = W_{EXD} \oplus W_C \quad (10)$$

Where "WT" is a binary image that shows the tampered pixels within the image. Black regions of the "WT" image are considered to be authentic while white regions represent the tampered regions of the watermarked image.

The second proposed scheme can be also used for color images by, simply, repeating all pervious steps for each color component of the image.

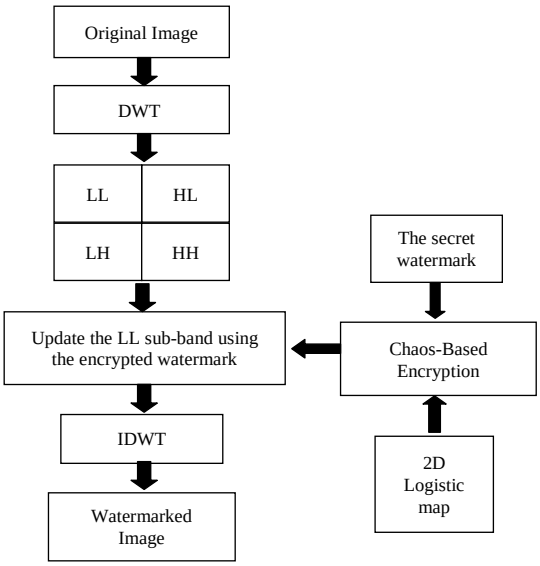


Fig.3: The embedding process block diagram of the second proposed scheme

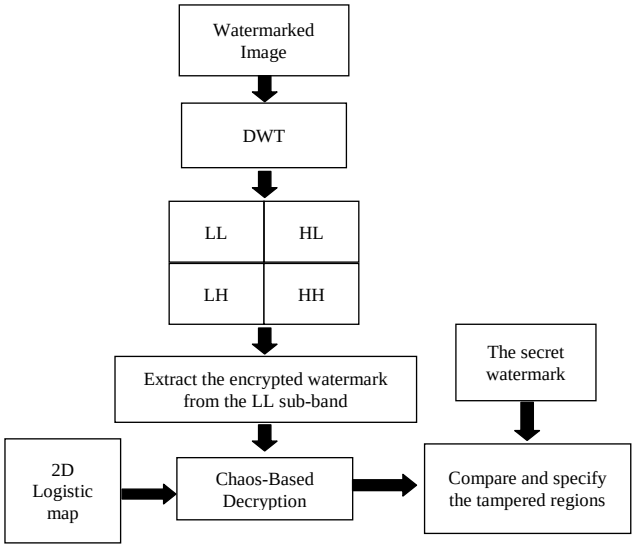


Fig.4: The extraction process block diagram of the second proposed scheme

4. RESULTS AND DISCUSSIONS

In this section, we carry out various experiments to evaluate the performance of the proposed watermarking schemes. We use the nine images shown in Fig. 5 to perform these experiments. The first seven images of Fig. 5 are greyscale images in BMP format, uncompressed and of 8 bits/pixel depth. The last two images are RGB color images in TIFF format, uncompressed and each color component has 8 bits/ pixel depth.

The nine cover images shown in Fig.5 are watermarked using the two proposed schemes. For the first scheme, there is no external watermark. The authentication watermark is generated based on the image contents. The watermarked images of the nine cover images for the first proposed schemes are shown in Fig.6. For the second proposed scheme, we select a 32×64 secret watermark logo in BMP format as shown in Fig.7 (a). We generate the authentication watermark by, periodically, repeating this logo until reach the size of LL sub-band of the cover image as shown in Fig.7 (b). The authentication watermark is encrypted using the proposed chaos-based encryption algorithm and the encrypted watermark is shown in Fig.7 (c). The encrypted watermark is now used to update the LL sub-band coefficients of the nine cover images shown in Fig.5 and the watermarked images are shown in Fig.8. Performance tests for the second proposed scheme show that the best value for n is 2. Then, we use the 2 LSBs of the LL sub-band coefficients for the watermark

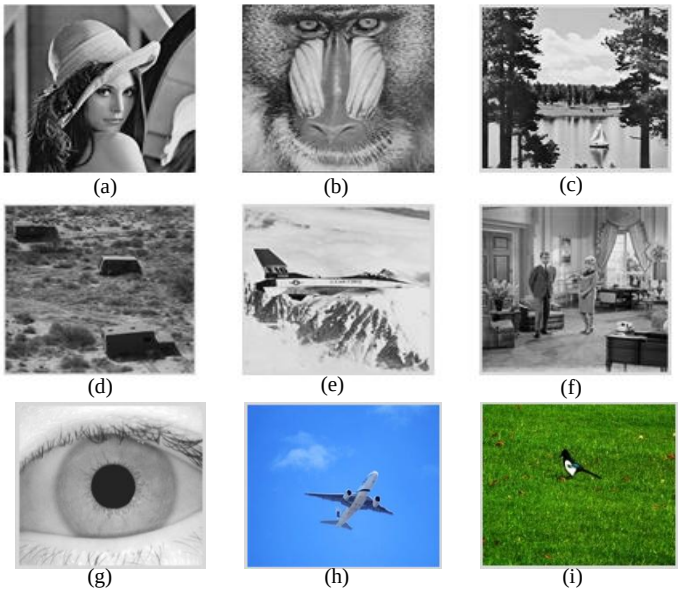


Fig.5: Nine cover images (a) Lena, (b) Baboon, (c) Lake, (d) Trucks, (e) Jetplane, (f) Living room, (g) Iris, (h) Plane, and (i) Bird.

4.1 Imperceptibility Performance of The Two Proposed Schemes

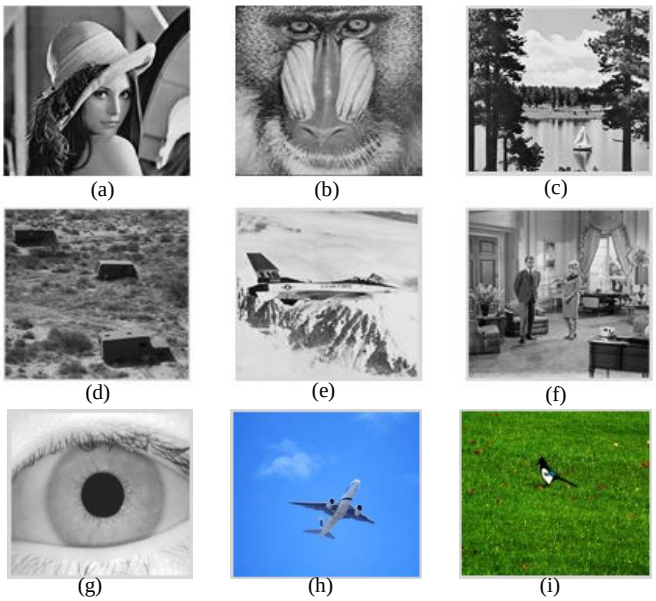
We evaluate the imperceptibility performance of the two proposed schemes using Peak signal to Noise Ratio (PSNR) and Mean squared Error (MSE) performance measures. In ideal case PSNR should be infinite and MSE should be zero. But it is not possible for watermarked image. Therefore, large PSNR and small MSE are desirable [33]. PSNR is defined as:

$$\text{PSNR} = 10 \log_{10} \left(\frac{\text{Max}_I^2}{\text{MSE}} \right) \text{dB} \quad (11)$$

Where Max_I is the maximum possible pixel value of the image ($Max_I = 255$ for 8 bits/pixel grayscale image). MSE is defined as:

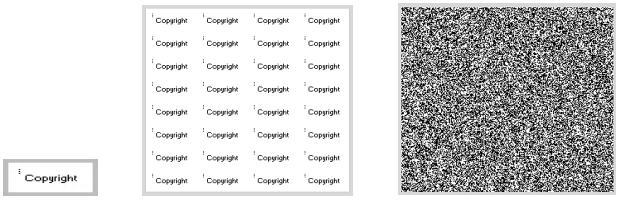
$$\text{MSE} = \frac{1}{\text{M}\times\text{N}\times\text{f}}\sum_{\text{k}=1}^{\text{f}}\sum_{\text{i}=1}^{\text{M}}\sum_{\text{j}=1}^{\text{N}}[\text{I}(\text{i},\text{j},\text{k}) - \text{I}_\text{w}(\text{i},\text{j},\text{k})]^2 \quad (12)$$

Where "I" is the cover image, "I_W" is the watermarked image, "M", "N", and "f" are the number of cover image rows, columns, and frames, respectively.



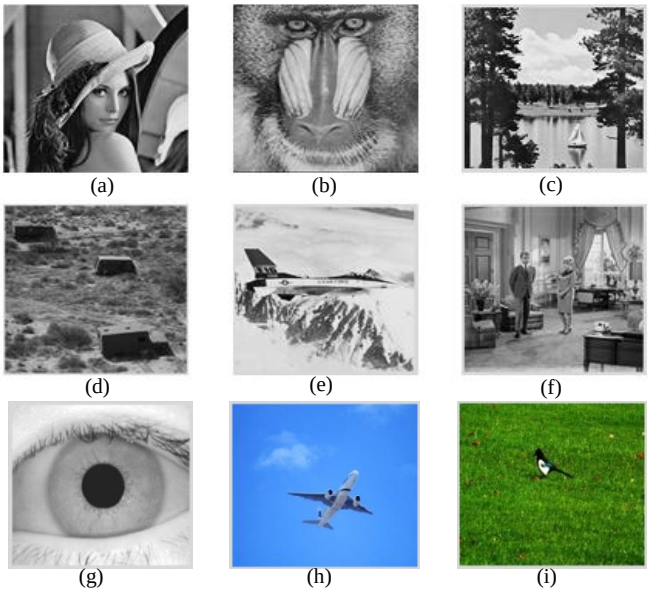
(a) (b) (c) (d) (e) (f) (g) (h) (i)

Fig.6: Watermarked images using the first proposed scheme.



(a) (b) (c)

Fig.7: (a) The watermark logo, (b) the authentication watermark, (c) the encrypted watermark of the second proposed watermarking scheme.



(a) (b) (c) (d) (e) (f) (g) (h) (i)

Fig.8: The watermarked images of the second proposed scheme.

As shown in Fig.6 and Fig. 8, naked eye cannot distinguish between the cover images shown in Fig.5 and the corresponding watermarked images shown in Fig.6 and Fig.8. To quantify the imperceptibility performance of the two proposed schemes, we calculate the PSNR values of the nine watermarked images shown in Fig.6 and Fig. 8 and list these values in Table.1. From Table.1, we can notice that the first proposed scheme shows better PSNR values than the second proposed scheme.

4.2 Performance of the Two Proposed Schemes under Tampering Attacks

Powerful publicly available image processing software packages enable unknown users to tamper with any image easily. Feathered cropping enables replacing or adding features to an image without causing detectable edges. Tamper localization and detection accuracy are two important aspects of the authentication watermarking schemes. The two proposed schemes will now be tested under tampering attacks of different sizes. Fig.9 shows that, tampering attacks can be detected and localized accurately using the first proposed scheme. Figs.9 (a) are the watermarked images of the nine cover images shown in Fig.5, Figs.9 (b) are the tampered watermarked images, Figs.9 (c) are the detected tampered regions in the watermarked images and in Figs.9 (d) we allocate the tampered regions in the watermarked images.

Table 1. The PSNR Values of the two proposed schemes

Image	Size	First Proposed Scheme	Second Proposed Scheme
Lena	[512×512]	53.8573	50.8185
Baboon	[256×256]	53.7208	50.6148
Lake	[256×256]	53.7232	50.6164
Trucks	[512×512]	53.9370	50.8915
Jetplane	[256×256]	53.3499	50.2594
Living Room	[512×512]	54.1713	51.1068
Iris	[256×256]	54.1281	51.1138
Plane	[256×256]	54.1328	52.0835
Bird	[256×256]	55.0154	52.8670

Fig.10 shows that, tampering attacks can also be detected and localized accurately using the second proposed scheme. Figs.10 (a) are the watermarked images of the nine cover images shown in Fig.5, Figs.10 (b) are the tampered watermarked images, Figs.10 (c) are the extracted-decrypted watermark images, (d) are the detected tampered regions in the watermarked images and in Figs.10 (e) we allocate the tampered regions in the watermarked images.

Now, we will compare the performance of the first proposed scheme with other existing schemes like Chang et al. [34] scheme, Lin et al. [35] scheme, Bravo-Solorio et al. [36] scheme and Sumalatha et al. [31] scheme. The comparison is based on the main quality factors of fragile watermarking scheme which are the imperceptibility performance that is evaluated using PSNR measure and the tamper detection accuracy which is measured using the tamper detection rate as shown in Table.2.

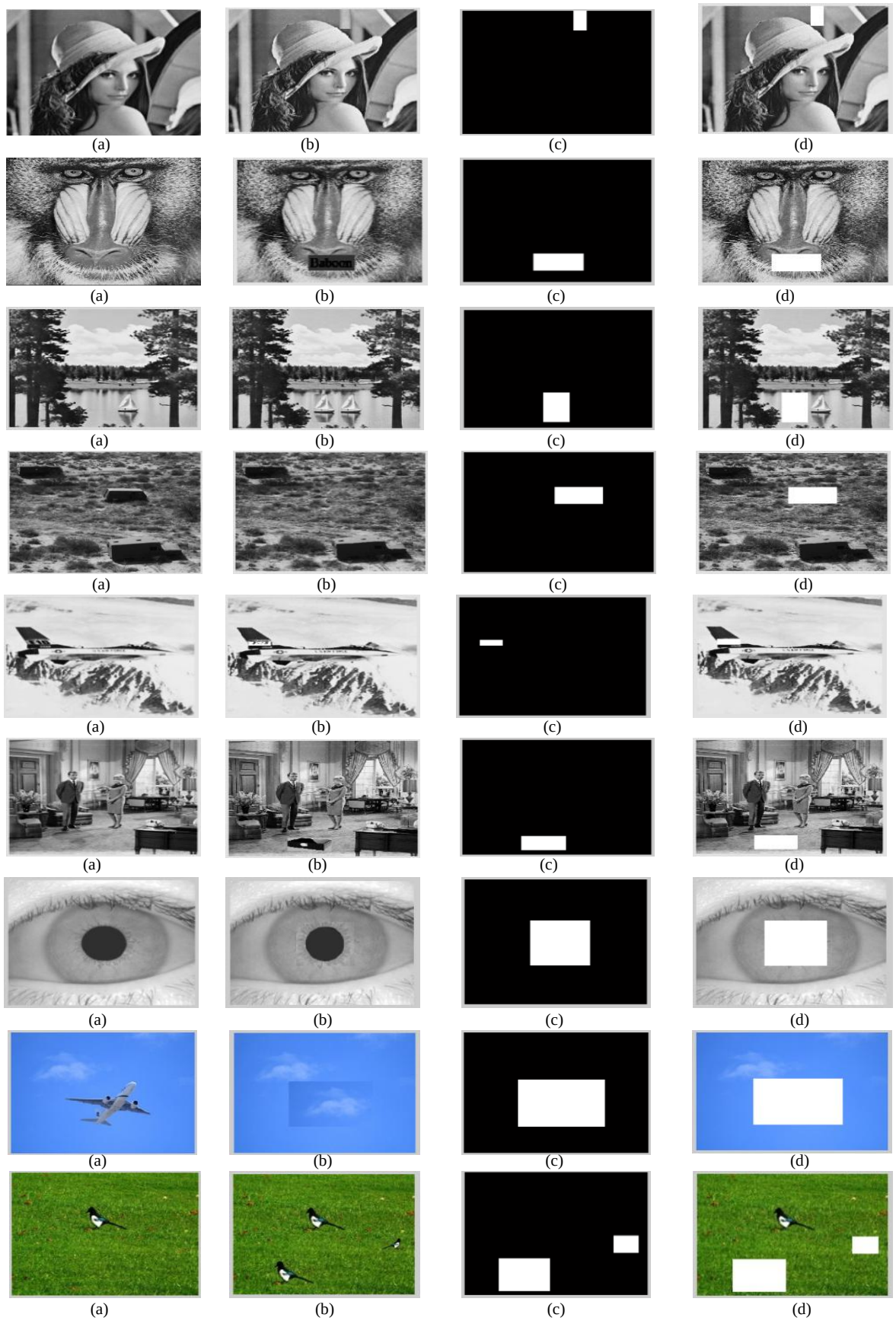


Fig.9: First Proposed Scheme: (a) watermarked images, (b) tampered watermarked images, (c) localization of tampered areas, and (d) allocation of tampered regions in the images.

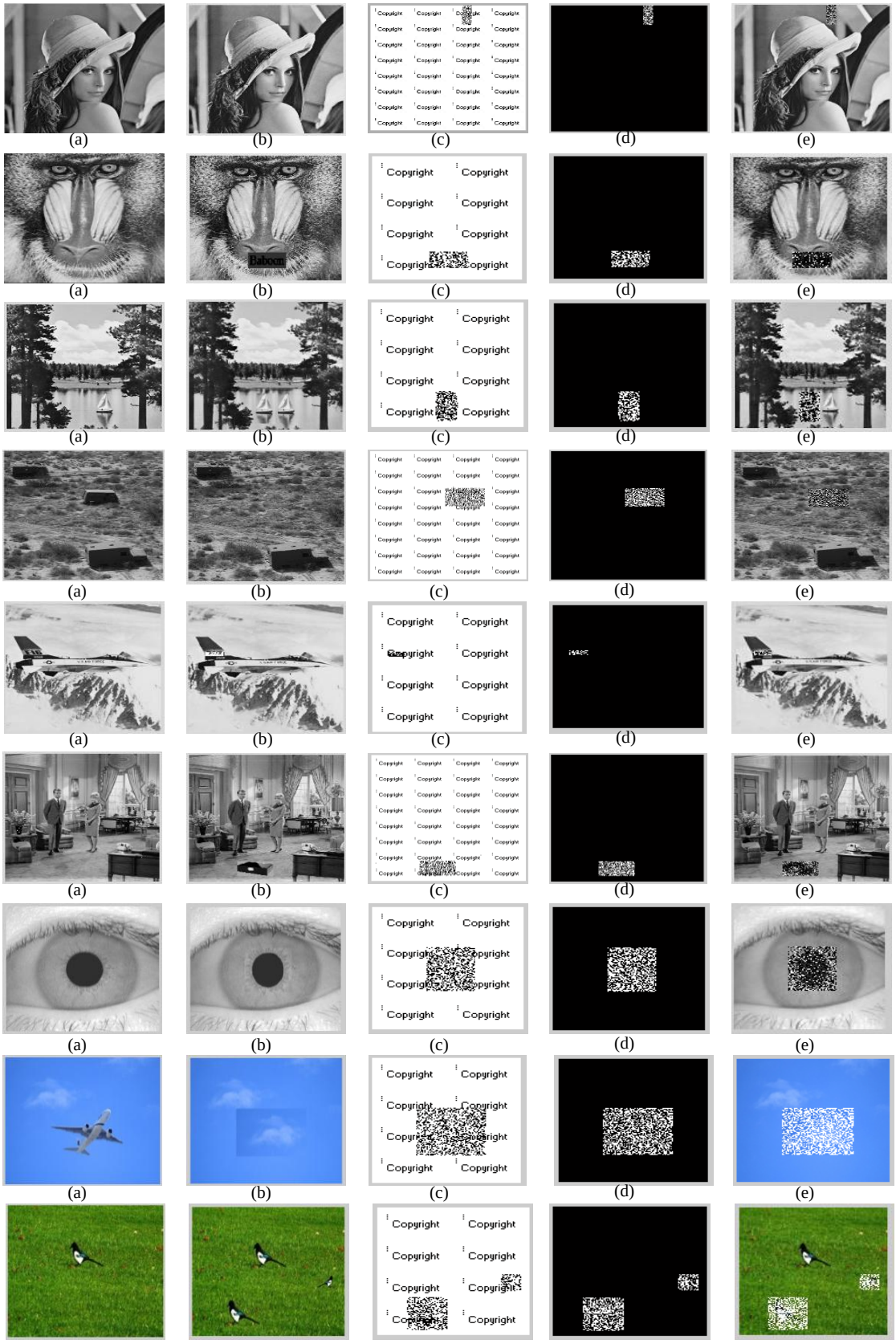


Fig.10: Second Proposed Scheme: (a) watermarked images, (b) tampered watermarked images, (c) tampered extracted-decrypted watermark, (d) localization of tampered areas and (e) allocation of tampered regions in the watermarked images.

The tamper detection rate is given by:

$$TR = \frac{N_{td}}{N_t} \times 100\% \quad (13)$$

Where TR is tamper detection rate, "N_t" is the number of tampered blocks, and "N_{td}" is the number of detected tampered blocks. We can see from Table.2 that, the tamper detection rate of all schemes are almost the same, however, the PSNR value of the first proposed scheme is better than other schemes.

Table 2. Comparison of the first proposed scheme with existing algorithms [31], [34-36]

Schemes	PSNR (dB)	Tamper Detection Rate
Chang et al. [34]	48.44	100%
Lin et al. [35]	44.37	100%
Bravo-Solorio et al. [36]	41	99%
Sumalatha et al. [31]	52.71	100%
First Proposed Scheme	53.85	100%

As the first proposed scheme is a modified version of Sumalatha et al. scheme, we should perform a performance comparison between the two schemes. Table.3 and Table.4 show the improvement of the first proposed scheme over Sumalatha et al. scheme with respect to: (i) PSNR; (ii) Normalized Correlation (NC), and (iii) TR. On the other hand, Sumalatha et al. algorithm advantage over the first proposed scheme is that it can recover the tampered regions.

Table 3. The PSNR and NC of the first proposed scheme and Sumalatha et al. algorithm

Image	Sumalatha et al. scheme		First Proposed Scheme	
	PSNR	NC	PSNR	NC
Lena	52.61	1	53.86	1
Cameraman	52.64	0.98	54.08	1
Peppers	52.65	0.98	54.12	1
Baboon	52.62	0.98	53.72	1
Jet Plane	52.64	0.97	53.35	1
Living Room	52.65	1	54.17	1

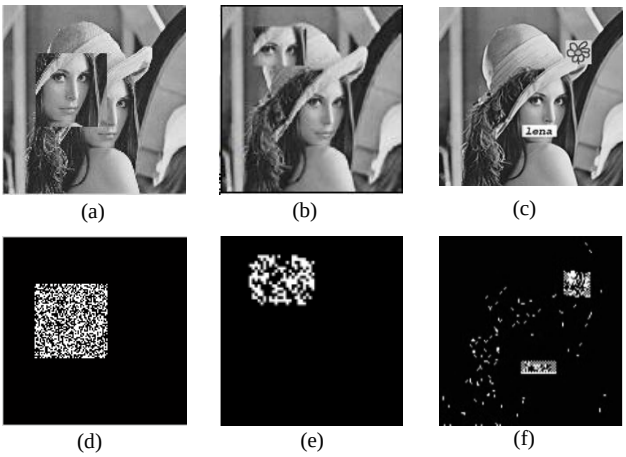
Table 4. The Tamper detection rate (TR) of the first proposed scheme and Sumalatha et al. algorithm

Image	Tampered Blocks Number	TR of Sumalatha et al. Scheme	TR of The First Proposed Scheme
Baboon	100	99%	100%
Lena	225	99%	100%
Jet Plane	155	99%	100%
Living Room	25	99%	100%

The performance of the second proposed scheme is compared with Wu et al. [32] scheme and Kommini et al. [37] scheme. Table.5 shows the improvement of the second proposed scheme over the Wu et al. and Kommini et al. schemes with respect to PSNR measure. We compare the tamper detection accuracy of the three schemes as shown in Fig.11. Lena image is used in this experiment. The tampered watermarked Lena images of the second proposed scheme, Wu et al. scheme, and Kommini et al. scheme are shown in Fig. 11 (a), (b) and (c), respectively. The tampered regions are detected using the second proposed scheme, X. Wu et al. algorithm, and C. Kommini et al. algorithm as shown in Fig. 11 (d), (e) and (f), respectively. We can notice that, the second proposed scheme shows better tamper detection accuracy than the other two schemes. On the other hand, the advantage of the other two schemes over the second proposed algorithm is that, they can resist JPEG compression much better than second proposed scheme.

Table 5. The PSNR (dB) of the second proposed scheme and Xiaoyun et al. scheme

Image	Kommini et al. [37] algorithm	Wu et al. [32] algorithm	Second Proposed Scheme
lena 512×512	34.16	42.26	50.8185
Baboon 256×256	33.96	42.11	50.6148



(a) (b) (c)

(d) (e) (f)

Fig. 11 (a), (b), (c) watermarked images and (d), (e), (f) tampered areas of second proposed scheme, X. Wu et al. [32] algorithm, and C. Kommini et al. [37] algorithm, respectively

5. CONCLUSION

Two fragile watermarking schemes for image authentication have been proposed. The first scheme is a block-based watermarking scheme and the other one is a wavelet-based watermarking scheme. The performances of the two proposed schemes were quantitatively compared with their original algorithms. These schemes are highly secure and efficient. Experiment results have demonstrated that the two proposed schemes are capable of accurate tamper detection and localization when the image has been suffered from malicious tampering attack with respect to their original algorithms. The second proposed scheme has an advantage to be faster than the first proposed scheme, but the first proposed scheme shows better imperceptibility performance and tamper detection accuracy than the second proposed scheme, which are considered to be the main quality factors of fragile watermarking scheme.

6. REFERENCES

[1] H. Y. Kim and A. Afif, "Secure authentication watermarking for binary images," In Computer Graphics and Image Processing, 2003.SIBGRAPI 2003, XVI Brazilian Symposium on IEEE, 199-206, 2003.

[2] A. Guru, H. Damecha, "Digital Watermarking Classification: A Survey," International Journal of Computer Science Trends and Technology (IJCST) vol. 5, pp. 8-13, Oct 2014.

[3] J. Fridrich and M. Goljan, "Images with Self-Correcting Capabilities," IEEE: International Conference of Image Processing, Vol.3, pp. 792-796, 1999.

[4] H. He, J. Zhang, F. Chen, "Block-wise Fragile Watermarking Scheme Based on Scramble Encryption," IEEE on International Conference on Bio-Inspired Computing: Theories and Applications, pp. 216-220, 2007.

[5] H. He, J. S. Zhang, and H. M. Tai, "Self-recovery Fragile Watermarking Using Block- Neighborhood Tampering Characterization," Springer-Verlag Berlin Heidelberg, Vol. 5806, pp. 132-145, 2009.

[6] X. Zhao, A.T. Ho, H. Treharne, V. Pankajakshan, C. Culnane and W. Jiang, "A Novel Semi-Fragile Image Watermarking, Authentication and Self-restoration Technique Using the Slant Transform," Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Vol. 1, pp. 283 – 286, 2007.

[7] C. C. Lo and Y. C. Hu, "A novel reversible image authentication scheme for digital images," Signal processing, Vol. 98, pp. 174-185, 2014.

[8] J. C. Chuang, Y. C. Hu, C. C. Lo and W. L. Chen, "Grayscale image tamper detection and recovery based on vector quantization," International journal of security and its applications, Vol. 7, No. 6, pp. 209-228, 2013.

[9] R. Chacko and W. Jebrson "Fragile Pixel-Wise Watermarking using Neighborhood Location Based Technique," International Journal of Current Engineering and Technology, Vol. 3, No. 5, pp. 1871-1877, 2013.

[10] Y. Lim, C. Xu, and D. D. Feng, "Web based Image Authentication Using Invisible Fragile Watermark," Proceedings of the Pan-Sydney area workshop on Visual information processing (VIP2001), Vol. 11, 2001.

[11] X. Zhang and S. Wang, "Statistical Fragile Watermarking Capable of Locating Individual Tampered Pixels," IEEE Signal processing letters, Vol. 14, No.10, 2007.

[12] S. Che, B. Ma, Z. Che, "An Adaptive and Fragile Image Watermarking Algorithm Based on Composite Chaotic Iterative Dynamic System," IIHMSP '08 International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 159-162, 2008.

[13] X. Zhang and S. Wang, "Fragile watermarking scheme using a hierarchical mechanism," Signal Processing, Vol. 4, No. 89, pp. 675-679, 2009.

[14] P. MeenakshiDevi, M. Venkatesan and K. Duraiswamy, "A Fragile Watermarking Scheme for Image Authentication with Tamper Localization Using Integer Wavelet Transform," Journal of Computer Science, Vol. 5, No. 11, pp. 831-837, 2009.

[15] D. Kundur and D. Hatzinakos, "Digital watermarking for telltale tamper proofing and authentication," Proceedings of the IEEE: Special Issue on Identification and Protection of Multimedia Information, pp. 1167–1180, 1999.

[16] G. Yu, C. Lu and H. Liao, "Mean quantization-based fragile watermarking for image authentication," Opt. Eng. Vol. 40, No. 7, pp. 1396–1408, 2001.

[17] X. Zhou, X. Duan and D. Wang, "A semi-fragile watermarking scheme for image authentication," Proceedings of the 10th International Conference on Multimedia Modeling, pp. 374–377, 2004.

[18] H. Kang and J. Park, "A semi-fragile watermarking using JND," Proceedings of STEG, pp. 127–131, 2003.

[19] Y. Hu and D. Han, "Using two semi-fragile watermarks for image authentication," Proceedings of the Fourth International Conference on Machine Learning and Cybernetics, pp. 5484–5489, 2005.

[20] H. Liu, J. Lin and J. Huang, "Image authentication using content based watermark," Proceedings of IEEE International Symposium on Circuits and Systems, pp. 4014–4017, 2005.

[21] Y. Zhu, C. Li and H. Zhao, "Structural digital signature and semi-fragile fingerprinting for image authentication in wavelet domain," Proceedings of IAS, pp. 478-483, 2007.

[22] H. Yang and X. Sun, "Semi-fragile watermarking for image authentication and tamper detection using HVS model" Proceedings of International Conference on Multimedia and Ubiquitous Engineering, pp. 1112–1117, 2007.

[23] S. Che, B. Ma and Z. Che, "Semi-fragile image watermarking algorithm based on visual features" Proceedings of International Conference on Wavelet Analysis and Pattern Recognition, pp. 382–387, 2007.

[24] C. Cruz, R. Reyes and M. Nakano, H. Perez, "Image content authentication system based on semi-fragile watermarking," Proceedings of the 51st Midwest Symposium on Circuits and Systems, pp. 306–309, 2008.

[25] Z. Dawei, C. Guanrong, L. Wenbo, "A chaos-based robust wavelet-domain watermarking Algorithm," Chaos Solitons and Fractals, Vol.22, No. 1, pp. 47–54, 2004.

[26] S. Rakesh, A. Ajitkumar, B. Shadakshari, and B. Annappa, "Image Encryption Using Block Based Uniform Scrambling and Chaotic Logistic Mapping," International Journal on Cryptography and Information Security (IJCIS), Vol. 2, No. 1, pp. 49-57, 2012.

[27] F. Dachselt and W. Schwarz, "Chaos and Cryptography," IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications, Vol. 48, pp. 1498-1501, 2001.

[28] T. S. Parker and L. O. Chua, "Chaos: A Tutorial for Engineers," Proceedings of the IEEE, Vol. 75, No. 8, pp. 982–1008, 1995.

[29] M. S. Baptista, "Cryptography with Chaos," Physics Letters A, Vol. 240, pp. 50-54, 1998.

[30] H. Liu, Z. Zhu, H. Jiang and B. Wang, "A Novel Image Encryption Algorithm Based on Improved 3D Chaotic Cat Map," In The 9th International Conference for Young Computer Scientists (ICYCS 2008), pp. 3016-3021, 2008.

[31] L. Sumalatha, G. R. Nesa, and V. V. Kumar, "A Simple Block Content Watermarking Scheme for Image Authentication and Tamper Detection," International Journal of Soft Computing & Engineering, Vol. 2, No. 4, pp. 113 – 117, 2012.

[32] X. Wu, J. Hu, Z. Gu, and J. Huang, "A Secure Semi Fragile Watermarking for Image Authentication Based on Integer Wavelet Transform with Parameters," Proceedings of the Australasian Information security workshop (AISW 2005) on Grid computing and e-research, Vol. 44, pp. 75-80, 2005.

[33] E. D. Aggarwal, E. S. Kaur and E. Anantdeep, "An Efficient Watermarking Algorithm to Improve Payload and Robustness without Affecting Image Perceptual Quality," JOURNAL OF COMPUTING, Vol. 2, No. 4, pp.105-109.

[34] C. C. Chang, Y. S. Hu, T. C. Lu, "A watermarking-based image ownership and tampering authentication scheme", Pattern Recognition Letters, Vol. 27, No. 5, pp. 439-446, 2006.

[35] C. H. Lin, W. S. Hsieh, "Applying projection and B-spline to image authentication and remedy," IEEE Transactions, Consumer Electronics, Vol. 49, No. 4, pp. 1234-1239, 2003.

[36] S. Bravo-Solorio, A. K. Nandi, "Fragile watermarking with improved tampering localization and self-recovery capabilities," In 18th European Signal Processing Conference (EUSIPCO), pp. 820-824, 2010.

[37] C. Kommini, K. Ellanti and E. H. Chowdary, "Semi-Fragile Watermarking Scheme based on Feature in DWT Domain," International Journal of Computer Applications, Vol. 28, No. 3, pp.42-46, 2011.