Wireless Personal Communications (2022) 125:513–530
https://doi.org/10.1007/s11277-022-09562-9

Dynamic S-Box and PWLCM-Based Robust Watermarking Scheme

Jan Sher Khan[1] · Sema Koç Kayhan[1] · Saygin Siddiq Ahmed[2] · Jawad Ahmad[3] · Hafza Ayesha Siddiqa[4] · Fawad Ahmed[5] · Baraq Ghaleb[3] · Ahmed Al Dubai[3]

Accepted: 31 January 2022 / Published online: 25 February 2022

Abstract
Due to the increased number of cyberattacks, numerous researchers are motivated towards the design of such schemes that can hide digital information in a signal. Watermarking is one of the promising technologies that can protect digital information. However, traditional watermarking schemes are either slow or less secure. In this paper, a dynamic *S-Box* based efficient watermarking scheme is presented. The original image was extracted at the receiver's end without any loss of sensitive information. Firstly, the Secure Hash Algorithm is applied to the original image for the generation of the initial condition. Piece Wise Linear Chaotic Map is then used to generate 16 $\times$ 16 dynamic Substitution Box (*S-Box*). As an additional security feature, the watermark is substituted through dynamic *S-Box*. Hence, it is hard for the eavesdroppers to attack the proposed scheme due to the dynamic nature of *S-Box*. Lastly, lifting wavelet transform is applied to the host image and the High Low and High High blocks of host image are replaced with least significant bits and most significant bits of the substituted watermark, respectively. Robustness, efficiency and security of the proposed scheme is verified using Structure Similarity Index, Structure Dissimilarity Index, Structure Content, Mutual Information, energy, entropy, correlation tests and classical attacks analysis.

Keywords Watermarking · Chaos · PWLCM · LSBs · MSBs · Random numbers

✉ Jawad Ahmad
j.ahmad@napier.ac.uk

[1] Department of Electrical and Electronics, University of Gaziantep, 27310 Gaziantep, Turkey

[2] Technical College of Kirkuk-Northern Technical University, Kirkuk, Iraq

[3] School of Computing, Edinburgh Napier University, Edinburgh, UK

[4] Department of Electrical Engineering, Fudan University, Yangpu, China

[5] Department of Cyber Security, Pakistan Navy Engineering College, NUST, Karachi, Pakistan

1 Introduction

Transmission of multimedia data such as images, videos and audios has significantly increased in the last decade. However, such a massive usage of the Internet also provided some opportunities for the eavesdropper. Eavesdropper apply different attacks and can access private and secret information. Therefore, to secure the information from illegal access and distribution, information hiding has recently become a major area of research. Intruders apply various attacks such as changing meaningful information through modifying the content or decipher the actual information. Steganography, cryptography, and watermarking have one thing in common: they all transmit secret information in such a way that only the receiver can decrypt. Steganography and cryptography are two separate approaches for keeping data secure. The goal of steganography is to conceal hidden messages in media files in such a way that no one can detect the existence of a secret message. A watermark is a type of marking that is hidden within a noise-tolerant signal like audio, video, or image data. It is commonly used to determine who owns the copyright to a signal with the main purpose of watermarking is to ensure proof of ownership. In watermarking, secret data is embedded in the original image in the form of text or image to shield the ownership of original image against unlawful copies. Watermarking can be mainly classified into blind, semi-blind and non-blind watermarking. Blind watermarking extracts the watermark without any knowledge of the original and watermarked images. The semi-blind watermarking extracts the original image knowing the watermarked image while the non-blind watermarking extracts the original image knowing original image, watermarked image and watermark [5, 20].

Over the last decade, various watermarking schemes have been proposed [6, 7, 9, 11, 12, 21, 23, 25, 28, 31, 32, 34, 35, 37]. For instance, a secure and Singular Value Decomposition (*SVD*) based watermarking method was proposed in [7, 25]. However, due to greater complexity and higher computational complexity, *SVD* based watermarking schemes are not suitable for hardware implementation. In [11, 23, 28], authors modified Discrete Cosine Transform (*DCT*) coefficients to embed the watermark. In 2012, Vahedi et al. improved the performance of some existing schemes by utilizing genetic algorithm optimization principles and proposed a new watermarking scheme for colour images [37]. Das et al. utilized the correlation among *DCT* adjacent coefficients and designed a blind efficient image watermarking scheme in the transform domain [12]. Authors in [8, 22] found that using 8×8 block-wise *DCT* based watermarking schemes can decrease real-time hardware implementation problem. In [26, 27], Moulin et al. and Mukherjee et al. designed secure watermarking schemes, respectively. Authors in [24], presented sub-sampling and Discrete Wavelet Transform (*DWT*) based watermarking scheme in the frequency domain. The proposed scheme in [24] resist geometric distortions. Zhou et al. inserted watermark in mid frequencies of Fourier Mellin Transform (*FMT*) for the minimization of the geometric deformation caused by lawful printing and scanning processes [41].

Since the last decade, a close relationship between chaos and cryptography has been proved. Due to the initial key sensitivity, non-periodicity, deterministic pseudo randomness, and larger keyspace, chaos-based watermarking schemes have received a lot of attention from the research community. In literature, a number of chaos-based watermarking schemes are available [13–16, 18, 19, 29, 36, 40]. The most commonly used chaotic maps are Henon map, Logistic map, Arnold map, Lorenz equations, Skew Tent map, Standard map and Baker map. Dawei et al. designed a chaos-based watermarking scheme for still images by transforming the image into the frequency domain. Dawei

et al. applied wavelet transformation locally and inserted the chaos-based watermark into sub-band coefficients [13]. Authors in [40] presented a new watermarking scheme using two chaotic maps. Embedded indexes of the host images were encrypted by one chaotic map while the second chaotic map was used to locate the pixel bit of the host image. Fan et al. proposed a novel watermarking scheme for speech data copyright protection via Discrete Fractional Sine Transform (*DFRST*) [14]. The security of the watermarking scheme [14] was improved through adopting chaotic sequences. In [29], a novel chaos-based fragile watermarking scheme for image authentication and tamper detection was presented. This watermarking scheme can identify the modification in an image and can also detect the exact location that has been modified. For security enhancement, two chaotic maps were employed in the presented algorithm [29].

Self-recovery and tamper detection fragile watermarking scheme were presented by Tong et al. [36]. Blocks of the original image were confused by using the cross chaotic map. The recovery after tampering was improved through a novel method known as sister block embedding scheme [36]. Ghebleh et al. proposed blind frequency domain watermarking scheme using Logistic and Arnold chaotic maps [15]. According to [15], the proposed wavelet transform based algorithm inserts a white and black watermark logo in the mid-band component of the host image. Two copies of watermark were embedded in two distinct subbands of the host image. The computational complexity was reduced by using only the least significant bits of the image [18]. Furthermore, Khan et al. [19] utilized classes of finite chain rings for designing of substitution Box (*S-Box*). The authors developed image encryption and watermarking schemes using the aforementioned *S-Box*. Jamal et al. embedded watermark in the frequency domain of the original image [16]. The embedded indexes were generated through random numbers that were obtained from Chaotic Fractional Rössler System [16]. Su et al. [33] utilized Hessenberg transform and designed a blind colour image watermarking algorithm. The security of the proposed watermarking scheme was increased via Arnold transform and *MD*5 hashing. Roy et al. developed a *DCT*-based blind colour watermarking scheme for inserting multiple watermarks simultaneously [30].

1.1 Contributions

Following are the main contributions of this paper.

1. For higher security, *SHA*-256 is applied on the original image and initial condition is generated for *PWLCM* chaotic map.
2. A dynamic 16×16 *S-Box* is generated from the random data obtained using *PWLCM*. Due to the dynamic nature of substitution, the presented scheme resist a number of statistical attacks.
3. The final watermark image is obtained using dynamic *S-Box* and the *HH* and *HL* block of the lifting wavelet transformed image.

The rest of paper is structured as follows: Sect. 2 presents the fundamental knowledge. Section 3 discusses the proposed scheme. Sections 4 and 5 presents simulation results and conclusion, respectively.

2 Fundamental Knowledge

2.1 PWLCM

Due to the random-like nature and sensitivity to initial conditions, a number of researchers have used *PWLCM* map in image encryption schemes [10]. From previous research [3, 38], it is evident that *PWLCM* has good dynamical behavior, uniform invariant density, and ergodicity. Mathematically, *PWLCM* map can be written as [39]:

$$z = f(z_{m-1}, \alpha) = \begin{cases} \frac{z_{m-1}}{\alpha}, & 0 \le z_{m-1} < \alpha \\ \frac{(z_{m-1})}{(1-\alpha)}, & 0 \le z_{m-1} < 0.5 \\ 0, & z_{m-1} = 0.5 \\ f(1 - z_{m-1}, \alpha). & 0.5 < z_{m-1} < 1 \end{cases} \tag{1}$$

where $\alpha \in (0, 0.5)$ is the control parameter and $z_0 \in (0, 1)$ is initial condition. These two parameters serve as a secret key in the proposed watermarking scheme. Figure 1 shows the key sensitivity of *PWLCM* for a small change in initial condition. In Fig. 2, 5000 random numbers are generated for $z_0 = 0.4999$ and $\alpha = 0.2120$. From these figures, one can conclude that *PWLCM* is highly sensitive to initial conditions and all random numbers are different.

2.2 Substitution Box (*S-Box*)

S-Box is used to induce non-linearity in a cryptosystem. In order to develop an efficient and robust watermarking scheme, *S-Box* should be part of it. *S-Box* decreases correlation between original/plaintext data. High non-linearity in a cryptosystem is always of great interest. *S-Box* is fundamentally vector boolean function that maps n input bits to m output bits which means $n \times m$ *S-Box* always produces m bits for a given number of n bits. In cryptographic theory, *S-Box* is a function of the form [2]:

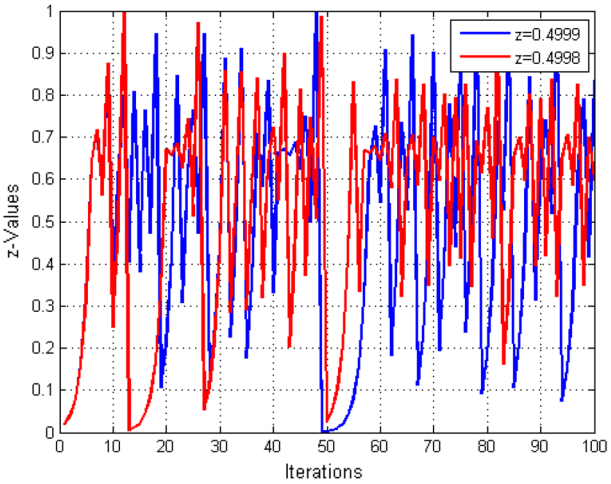

Fig. 1 Plots of *PWLCM* against number of iterations for slightly different values of z_0

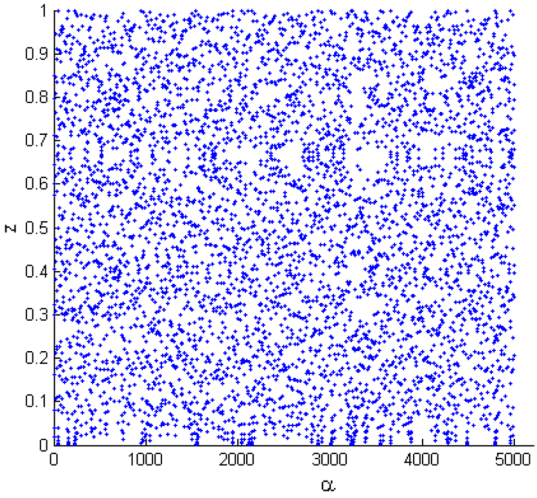

Fig. 2 Distribution of z against iterations

$$S - Box : GF(B)^n \rightarrow GF(B)^m. \tag{2}$$

Where $B = 0, 1$. As $S - Boxes$ are nonlinear components, therefore, it determines security strength against differential and linear attacks.

3 The Proposed Scheme

Flowchart of the proposed image watermarking scheme is shown in Fig. 3. The presented scheme consists of two main steps: (1) dynamic *S-Box* generation using *PWLCM* chaotic map (2) embedding watermark in the original image. Detail steps of the proposed image watermarking scheme are as follows:

Step1: Apply $SHA - 256$ on the original image P and generate the initial condition z_0 for the *PWLCM*.

$$H_{bits} = SHA(P). \tag{3}$$

Step2: Convert 256 bit (64 byte hexadecimal) hash value to decimal format.

$$H_{decimal} = bi2de(H_{bits}). \tag{4}$$

Step3: Divide decimal hash value $H_{decimal}$ by 2^{48} to ensure that the value of initial condition z_0 is between 0 and 1.

$$z_0 = \frac{H_{decimal}}{2^{48}}. \tag{5}$$

Step4: Set maximum number of iterations i.e., 356 for *PWLCM*. To avoid the transient effect, the first 100 random numbers were ignored and the remaining 256 random numbers were considered.

Step5: Multiply random numbers vector z with 10^{14} and apply modulus 256 operation.

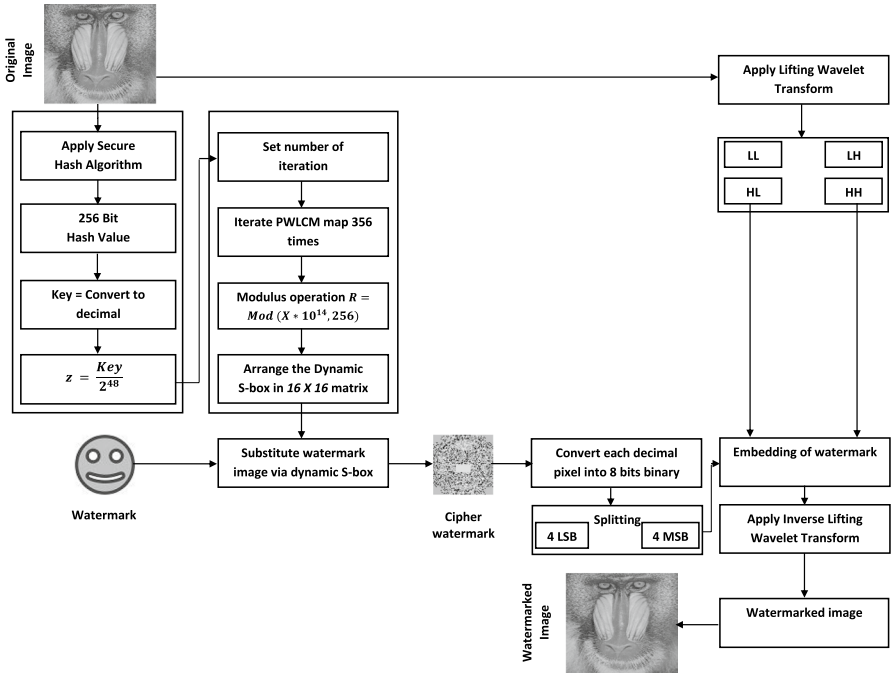

Fig. 3 Flow chart of proposed scheme

$$R = Mod(z \times 10^{14}, 256). \tag{6}$$

Step6: Arrange decimal random numbers in 16×16 matrix form and obtain dynamic *S-Box*.

$$\begin{pmatrix} S_{11} & S_{12} & \dots & S_{1n} \\ S_{21} & S_{22} & \dots & S_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ S_{m1} & S_{m2} & \dots & S_{mn} \end{pmatrix} \tag{7}$$

Step7: To get a substituted watermark W', substitute each pixel of the watermark with the value of dynamic *S-Box*.

Step8: Convert each decimal pixel of substituted watermark W' to binary 8 bits at index i and j.

$$W'_{bits} = decimal2binary(W'). \tag{8}$$

Step9: Split the 8 bit binary pixel values into 4 *LSBs* and 4 *MSBs*.

$$\begin{aligned} LSBs &= W'_{bit}(1 : 4), \\ MSBs &= W'_{bit}(5 : 8). \end{aligned} \tag{9}$$

Step10: Apply *LWT* on the original image *P*.

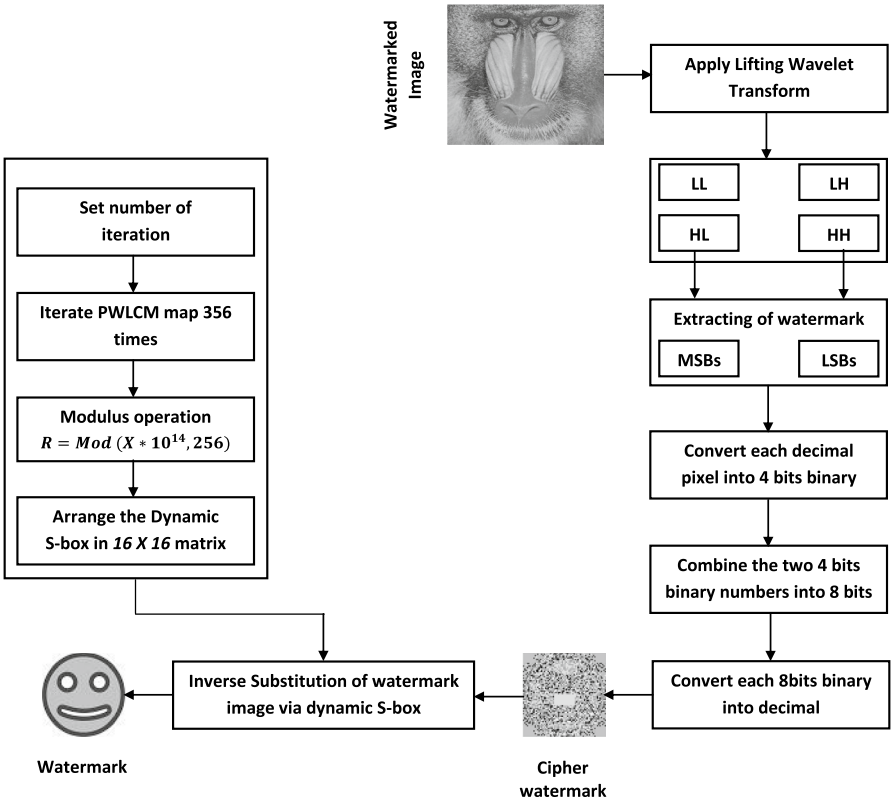

Fig. 4 Flow chart of watermark extraction

$$[LL, LH, HL, HH] = lwt2(P). \tag{10}$$

Step11: Replace *H*L and *HH* blocks of the host image with the *LSBs* and *MSBs* of the substituted watermark.

$$[LL, LH, HL, HH] = [LL, LH, LSBs, MSBs]. \tag{11}$$

Step12: Apply inverse lifting wavelet transform on the new blocks of host image to get the final watermarked image *W*.

$$W = ilwt2([LL, LH, LSBs, MSBs]). \tag{12}$$

To obtain the watermark and original image P from the watermarked image W, all the above steps are applied in reverse order. The step-wise flowchart of the watermark extraction algorithm is illustrated in Fig. 4. As the initial condition, z_0 serve as a secret key in the proposed scheme, therefore, at the receiver end, the receiver must know this key. Due to this reason, the flow chart in Fig. 4 does not have key generation steps.

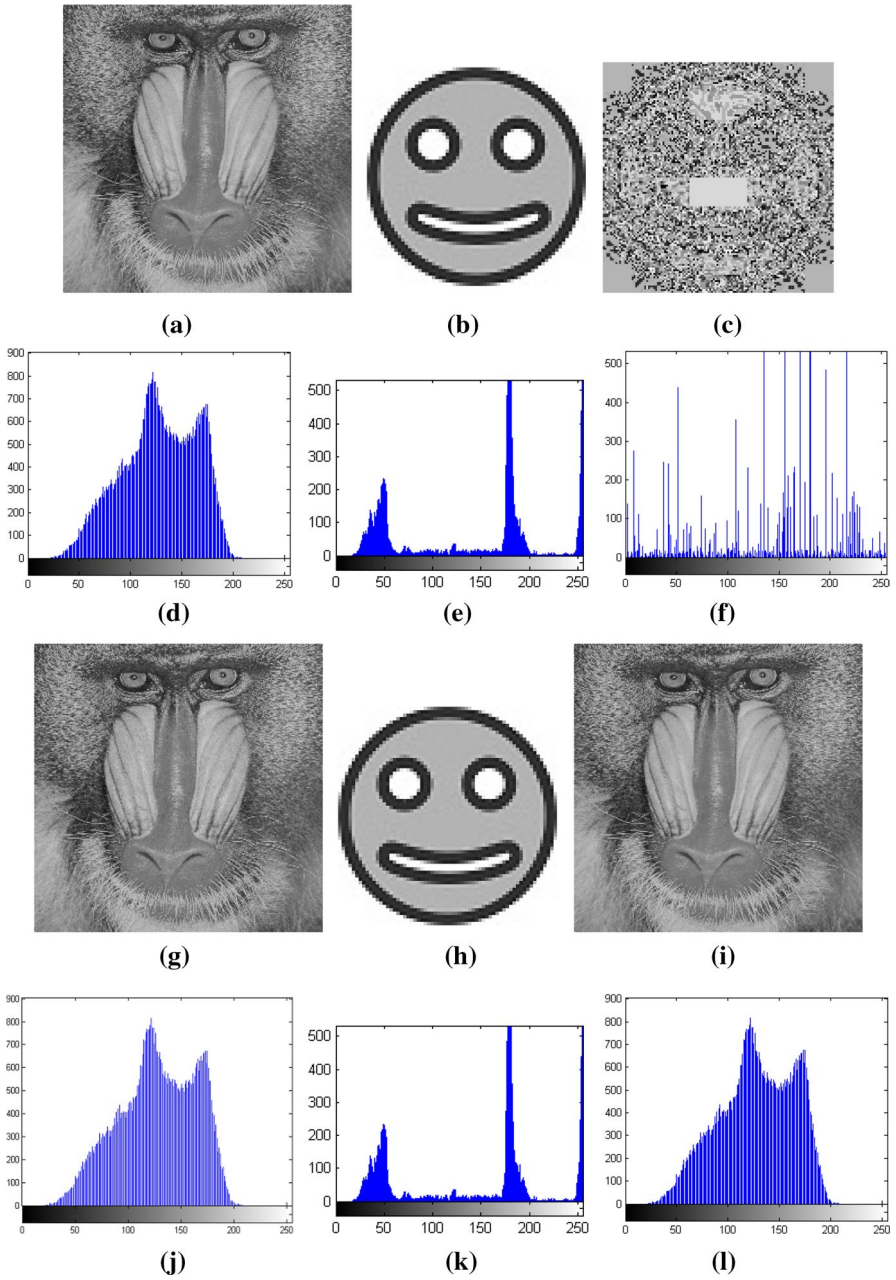

Fig. 5 Visual results of proposed watermarking scheme for Baboon image **a** Original Baboon image. **b** Watermark imagem. **c** Substitute watermark image. **d** Histogram of original Baboon image. **e** Histogram of watermark image. **f** Histogram of substitute watermark image. **g** Watermarked Baboon image. **h** Extracted watermark image. **i** Recovered original Baboon image. **j** Histogram of watermarked Baboon image. **k** Histogram of extracted watermark image. **l** Histogram of recovered original Baboon image

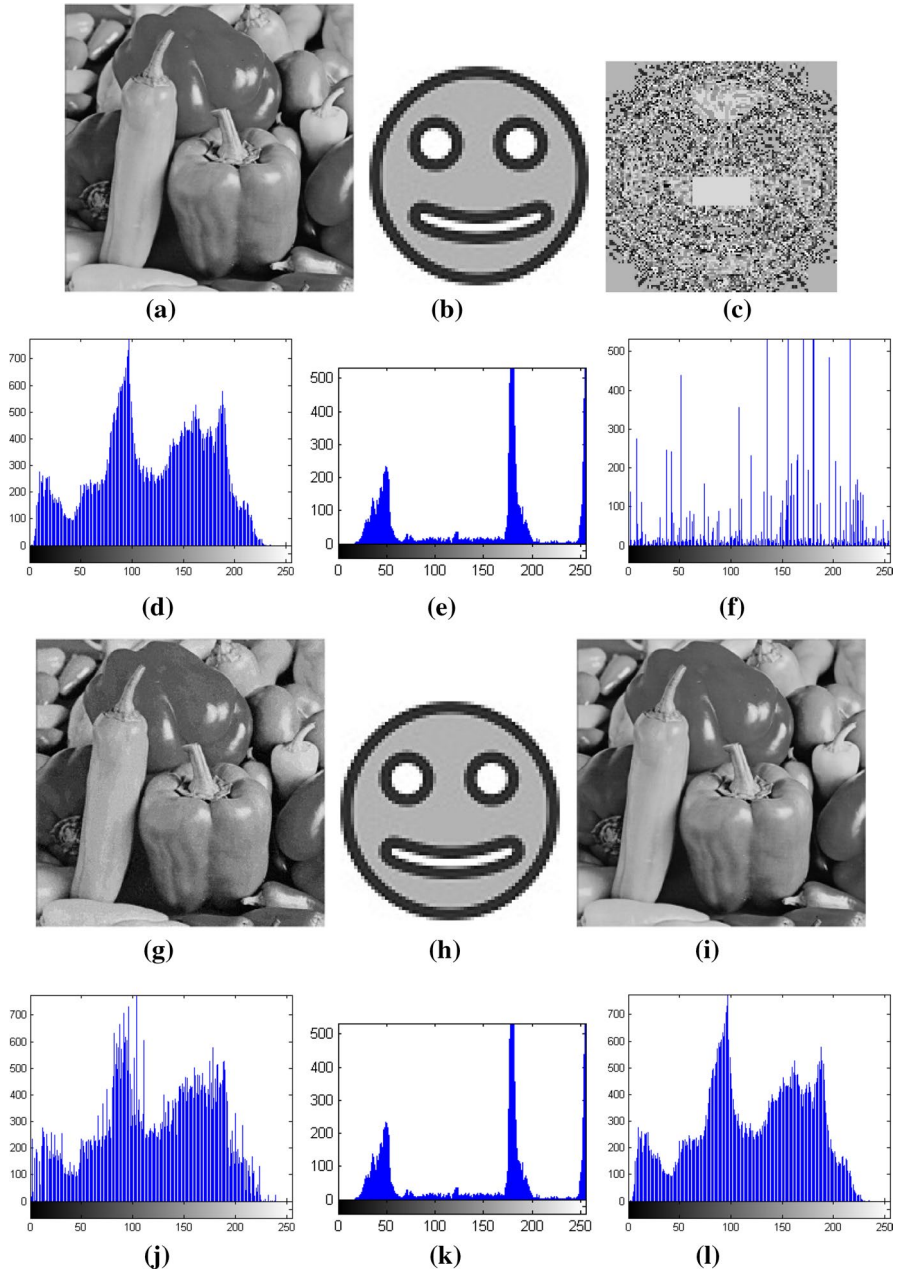

Fig. 6 Visual results of proposed watermarking scheme for Pepper image **a** Original Pepper image. **b** Watermark image. **c** Substitute watermark image. **d** Histogram of original Pepper image. **e** Histogram of watermark image. **f** Histogram of substitute watermark image. **g** Watermarked Pepper image. **h** Extracted watermark image. **i** Recovered original Pepper image. **j** Histogram of watermarked Pepper image. **k** Histogram of extracted watermark image. **l** Histogram of recovered original Pepper image

4 Simulation Results and Evaluation

Original Baboon image, watermark image, ciphered watermarked image, watermarked Baboon image, recovered watermark and recovered Baboon image are illustrated in Fig. 5a, b, c, g, h and i, respectively. Similarly, original Pepper image, watermark image, ciphered watermarked image, watermarked Pepper, recovered watermark and recovered Pepper image are shown in Fig. 6a, b, c, g, h and i, respectively. To prove the robustness and efficiency of the designed watermarking scheme, Structure Similarity Index (*SSI*), Structure Dissimilarity Index (*SDI*), Structure Content (*SC*), Mutual Information (*MI*), energy, entropy, correlation, histogram tests, and classical attacks analysis are carried out for the proposed scheme. All these parameters are discussed in the following subsections along with obtained results.

4.1 Structure Similarity Index (SSI)

SSI test is used to compute similarity between two variables or (in our case) two images. The results of *SSI* primarily reveals pixel inter dependency relationship. Mathematically, it is computed as [1]:

$$SSI(W,R) = \frac{(2\mu_W\mu_R + C1)(\sigma_{WR} + C2)}{(\mu_W^2 + \mu_R^2 + C1)(\sigma_W^2 + \sigma_R^2 + C2)} \tag{13}$$

where W represent watermarked image and R represents recovered image, respectively. The variables μ_W and μ_R compute the average values of W and R, respectively. The parameters σ_W and σ_R calculate variance of W and R, respectively. Similarly, the parameters σ_{WR} quantifies the covariance of image W and R. Likewise, the parameters $C1 = (K1L)^2$ and $C2 = (K2L)^2$ are utilized to stabilize the division with weak denominator, where $L = 2^{\#bitsperpixel} - 1$, $K1 = 0.01$ and $K2 = 0.03$. The resultant *SSI* is 1 if two images are identical, otherwise it is between 0 and 1. From Table 1, *SSI* value of the proposed image watermarking is near to the ideal value 1. Hence, SSI test confirms that the watermarked image is closer to the original image.

4.2 Structure Dissimilarity Index (SDI)

SDI computes dissimilarities between two images i.e., host and watermarked image. Mathematically it is calculated as [4]:

Table 1 Experimentally computed values

Experiment type	Watermarked Baboon	Watermarked Pepper
Structure Similarity Index	0.9503	0.9660
Structure Dissimilarity Index	0.0258	0.0170
Structure content	1.0022	1.0010
Mutual information	0.2541	0.2633

$$SDI(W,R) = \frac{1 - SSI}{2} \tag{14}$$

From Table 1, one can see that the *SDI* value of the proposed image watermarking scheme is considerably small, which again confirms that the watermarked image is closer to the original image.

4.3 Structure Contents (SC)

SC is the measure of information content in an image. Mathematically, it is written as the ratio of the structural information contents of the original and watermarked images. *SC* is calculated as [4]:

$$SC = \frac{\sum_{i=1}^{a} \sum_{j=1}^{b} [O(i,j)]^2}{\sum_{i=1}^{a} \sum_{j=1}^{b} [W(i,j)]^2} \tag{15}$$

In the above equation, $O(i; j)$ represents original image and $W(i; j)$ represents the watermarked image at index i and j while a and b illustrates the number of rows and columns, respectively. From Table 1, one can see that the values of *SC* is close to 1 for the proposed watermarking scheme that confirms the robustness of the proposed scheme.

4.4 Mutual Information (MI)

The statistical dependence between two random variables is determined by *MI* test. *MI* can also be used to quantify robustness efficiency against various image degradation [4]. Mathematically, *MI* can be computed as follows [4]:

$$MI = \sum \sum p(O,W) \log\left(\frac{p(O,W)}{p(O)p(W)}\right). \tag{16}$$

where $p(O, W)$ computes the joint probability distribution function of original and watermarked images while $p(O)$ and $p(W)$ computes the probability density functions in the individual images, respectively. The lower values of *MI* in Table 1 is a proof of good watermarking.

4.5 Energy

The disorder in texture can be computed via energy of an image. Energy of an image determines the information in an image in terms of the sum of squared values [4].

$$E = \sum (E(i,j)^2) \tag{17}$$

where $E(i, j)$ is pixel value at position i and j. Low energy means that the entries in Gray Level Co-occurrence Matrix (*GLCM*) are almost equal while higher energy means that some entries in the *GLCM* have higher magnitudes. A lower value of energy is required in image watermarking. The computed value in Table 2 proves that the proposed watermarking scheme has small value of energy.

Table 2 Experimentally computed values

Experiment type	Original Baboon	Watermarked Baboon	Original Pepper	Watermarked Pepper
Energy	0.1022	0.0898	0.0938	0.0692
Entropy	7.1273	7.0892	7.6170	7.5691
Horizontal	0.7287	0.7465	0.9371	0.9116
Vertical	0.6690	0.7034	0.9686	0.9678
Diagonal	0.6744	0.6520	0.9189	0.8800

4.6 Entropy

Entropy test is used to calculate the degree of randomness of digital images. In watermarking, entropy is of great interest to approximate whether the watermarked image is similar to the original image or not. By assuming that an algorithm which output 2^8 symbols, its ideal entropy should be 8 bits. For a good watermarking scheme, entropy value of the watermarked image should be near to the original image entropy value. Mathematically entropy can be calculated as [17]:

$$H = \sum \left[p(x_i) \log_2 \left(\frac{1}{p(x_i)} \right) \right] \tag{18}$$

In the above equation, $p(x_i)$ represents the probability of random variable x at i^{th} position. The calculated entropy for the proposed watermarking scheme is shown in Table 2. From Table 2, one can see that entropy values for watermarked and host images are approximately equal. Thus the proposed watermarking scheme can resist entropy attacks.

4.7 Correlation Analysis

Correlation coefficient determine similarity between variables. Mathematically, the correlation coefficient is written as [17]:

$$Cov(O, W) = E[O - E(O)] \times [W - E(W)] \tag{19}$$

$$CC = \frac{Cov(O, W)}{\sqrt{D(O)D(W)}} \tag{20}$$

where

$$E(O) = \frac{1}{1000} \sum_{x=1}^{1000} (O(x))$$

$$D(O) = \frac{1}{1000} \sum_{x=1}^{1000} (O(x) - E(O))^2$$

The variable $Cov(O, W)$ represents the covariance of adjacent pixels between original image O and watermarked image W, respectively. Correlation coefficient values in horizontal, vertical and diagonal directions are highlighted in Table 2. From Table 2, one can see that the correlation coefficient values in all direction are almost same which confirms the similarity between watermarked and original images.

4.8 Histogram Analysis

The histogram shows the pixel distribution of a digital image. From Figs. 5d, e, f, j, k and l and 6d, e, f, j, k and l, it is evident that the histogram of the watermarked image is similar to the original image histogram. Furthermore, the histograms of the recovered watermark and recovered plaintext original images are also exactly similar to the original watermark and original plaintext images histograms. Hence, the histogram plot confirms that an intruder cannot detect any differences between original and watermarked images.

4.9 Classical Attacks Analysis

SHA-256 and plaintext image are utilized to produce the initial values of *PWLCM* chaotic maps (z_0). This makes the proposed watermarking dependable on the plaintext image. For a single pixel change in the original plaintext image, the proposed scheme will produce a totally different random number. Therefore, during extraction and inverse substitution of the watermark image, instead of generating the original watermark image, the algorithm will produce a totally different cipher watermark. As a result, the proposed watermarking scheme can resist ciphertext-only, chosen-plaintext and known-plaintext attack.

5 Conclusion

In this paper, a dynamic *S-Box* based efficient watermarking scheme is presented and statistically evaluated. The dynamic *S-Box* and *PWLCM* strengthen the security of the proposed scheme due to the dynamic nature. The initial condition for *PWLCM* was generated from the $SHA - 256$. The watermark is substituted with the values of dynamic *S-Box*. Due to the dynamic nature of *S-Box*, it is hard for the eavesdroppers to launch an attack on the proposed scheme. Lastly, *LWT* is applied on the host image and *HL* and *HH* blocks of host image were replaced with Least Significant Bits (*LSBs*) and Most Significant Bits (*MSBs*) of the substituted watermark. The efficiency and robustness of the presented watermarking scheme are tested against numerous security parameters which confirmed that the scheme is highly secure. Furthermore, at the receiver's end, the proposed scheme can recover the original image without loss of any sensitive information. In future, we intend to optimize the proposed scheme by targeting the colored images rather than only gray-scale ones and we will also evaluate the scheme under numerous types of attacks.

Funding The authors have not disclosed any funding.

Data Availability Enquiries about data availability should be directed to the authors.

Declarations

Conflict of interest There is no conflict of interest.

References

1. Abbas, N. A. (2015). Image watermark detection techniques using quadtrees. *Applied Computing and Informatics, 11*(2), 102–115.
2. Ahmad, J., & Hwang, S. O. (2015). Chaos-based diffusion for highly autocorrelated data in encryption algorithms. *Nonlinear Dynamics*, *82*(4), 1–12 .
3. Baranovsky, A., & Daems, D. (1995). Design of one-dimensional chaotic maps with prescribed statistical properties. *International Journal of Bifurcation and Chaos, 5*(06), 1585–1598.
4. Batool, S. I., Shah, T., & Khan, M. (2014). A color image watermarking scheme based on affine transformation and s 4 permutation. *Neural Computing and Applications, 25*(7), 2037–2045.
5. Benhocine, A., Laouamer, L., Nana, L., & Pascu, A. C. (2013). New images watermarking scheme based on singular value decomposition. *Journal of Information Hiding and Multimedia Signal Processing, 4*(1), 9–18.
6. Chamlawi, R., Khan, A., & Usman, I. (2010). Authentication and recovery of images using multiple watermarks. *Computers and Electrical Engineering, 36*(3), 578–584.
7. Chang, C. C., Tsai, P., & Lin, C. C. (2005). Svd-based digital image watermarking scheme. *Pattern Recognition Letters, 26*(10), 1577–1586.
8. Chau, L. P., & Siu, W. C. (2003). Efficient multiplier structure for realization of the discrete cosine transform. *Signal Processing: Image Communication, 18*(7), 527–536.
9. Chen, L., Chen, J., Zhao, G., & Wang, S. (2019). Cryptanalysis and improvement of a chaos-based watermarking scheme. *IEEE Access, 7,* 97549–97565.
10. Chen, Y., Tang, C., & Yi, Z. (2020). A novel image encryption scheme based on pwlcm and standard map. *Complexity*, *2020*, 3026972. https://doi.org/10.1155/2020/3026972.
11. Chu, W. C. (2003). Dct-based image watermarking using subsampling. *IEEE Transactions on Multimedia, 5*(1), 34–38.
12. Das, C., Panigrahi, S., Sharma, V. K., & Mahapatra, K. (2014). A novel blind robust image watermarking in dct domain using inter-block coefficient correlation. *AEU-International Journal of Electronics and Communications, 68*(3), 244–253.
13. Dawei, Z., Guanrong, C., & Wenbo, L. (2004). A chaos-based robust wavelet-domain watermarking algorithm. *Chaos, Solitons and Fractals, 22*(1), 47–54.
14. Fan, M., & Wang, H. (2009). Chaos-based discrete fractional sine transform domain audio watermarking scheme. *Computers and Electrical Engineering, 35*(3), 506–516.
15. Ghebleh, M., Kanso, A., & Own, H. S. (2014). A blind chaos-based watermarking technique. *Security and Communication Networks, 7*(4), 800–811.
16. Jamal, S. S., Khan, M. U., & Shah, T. (2016). A watermarking technique with chaotic fractional s-box transformation. *Wireless Personal Communications, 90*(4), 2033–2049.
17. Khan, J. S., Ahmad, J., Ahmed, S. S., Siddiqa, H. A., Abbasi, S. F., & Kayhan, S. K. (2019). Dna key based visual chaotic image encryption. *Journal of Intelligent and Fuzzy Systems, 37*(2), 2549–2561.
18. Khan, M., & Shah, T. (2015). A copyright protection using watermarking scheme based on nonlinear permutation and its quality metrics. *Neural Computing and Applications, 26*(4), 845–855.
19. Khan, M., Shah, T., & Batool, S. I. (2016). A new approach for image encryption and watermarking based on substitution box over the classes of chain rings. *Multimedia Tools and Applications*, *76*(22), 24027–24062.

20. Wang, R., Shaocheng, H., Zhang, P., Yue, M., Cheng, Z., & Zhang, Y. (2020). A novel zero-watermarking scheme based on variable parameter chaotic mapping in NSPD-DCT domain. In *IEEE Access*, *8*, 182391–182411. https://doi.org/10.1109/ACCESS.2020.3004841.
21. Lian, S., Chen, X., & Wang, J. (2012). Content distribution and copyright authentication based on combined indexing and watermarking. *Multimedia Tools and Applications, 57*(1), 49–66.
22. Liang, J., & Tran, T. D. (2001). Fast multiplierless approximations of the dct with the lifting scheme. *IEEE Transactions on Signal Processing, 49*(12), 3032–3044.
23. Lin, S. D., & Chen, C. F. (2000). A robust dct-based watermarking for copyright protection. *IEEE Transactions on Consumer Electronics, 46*(3), 415–421.
24. Lu, W., Sun, W., & Lu, H. (2012). Novel robust image watermarking based on subsampling and dwt. *Multimedia Tools and Applications, 60*(1), 31–46.
25. Lu, Z. M., Zheng, H. Y., & Huang, J. W. (2007). A digital watermarking scheme based on dct and svd. In *Intelligent Information Hiding and Multimedia Signal Processing, 2007. IIHMSP 2007. Third International Conference on* (Vol. 1, pp. 241–244). IEEE.
26. Moulin, P., & Mihcak, M. K. (2002). A framework for evaluating the data-hiding capacity of image sources. *IEEE Transactions on Image Processing, 11*(9), 1029–1042.
27. Mukherjee, D. P., Maitra, S., & Acton, S. T. (2004). Spatial domain digital watermarking of multimedia objects for buyer authentication. *IEEE Transactions on Multimedia, 6*(1), 1–15.
28. Patra, J. C., Phua, J. E., & Bornand, C. (2010). A novel dct domain crt-based watermarking scheme for image authentication surviving jpeg compression. *Digital Signal Processing, 20*(6), 1597–1611.
29. Rawat, S., & Raman, B. (2011). A chaotic system based fragile watermarking scheme for image tamper detection. *AEU-International Journal of Electronics and Communications, 65*(10), 840–847.
30. Roy, S., & Pal, A. K. (2017). A blind dct based color watermarking algorithm for embedding multiple watermarks. *AEU-International Journal of Electronics and Communications, 72,* 149–161.
31. Seo, J. S., & Yoo, C. D. (2006). Image watermarking based on invariant regions of scale-space representation. *IEEE Transactions on Signal Processing, 54*(4), 1537–1549.
32. Singhal, N., Lee, Y. Y., Kim, C. S., & Lee, S. U. (2009). Robust image watermarking using local zernike moments. *Journal of Visual Communication and Image Representation, 20*(6), 408–419.
33. Su, Q., & Chen, B. (2017). A novel blind color image watermarking using upper hessenberg matrix. *AEU-International Journal of Electronics and Communications, 78,* 64–71.
34. Thakur, S., Singh, A. K., Ghrera, S. P., & Elhoseny, M. (2019). Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications. *Multimedia Tools and Applications, 78*(3), 3457–3470.
35. Thakur, S., Singh, A. K., Ghrera, S. P., & Mohan, A. (2020). Chaotic based secure watermarking approach for medical images. *Multimedia Tools and Applications, 79*(7), 4263–4276.
36. Tong, X., Liu, Y., Zhang, M., & Chen, Y. (2013). A novel chaos-based fragile watermarking for image tampering detection and self-recovery. *Signal Processing: Image Communication, 28*(3), 301–308.
37. Vahedi, E., Zoroofi, R. A., & Shiva, M. (2012). Toward a new wavelet-based watermarking approach for color images using bio-inspired optimization principles. *Digital Signal Processing, 22*(1), 153–162.
38. Wang, X., & Jin, C. (2012). Image encryption using game of life permutation and pwlcm chaotic system. *Optics Communications, 285*(4), 412–417.
39. Wang, X., & Xu, D. (2014). A novel image encryption scheme based on brownian motion and pwlcm chaotic system. *Nonlinear Dynamics, 75*(1–2), 345–353.
40. Wu, X., & Guan, Z. H. (2007). A novel digital watermark algorithm based on chaotic maps. *Physics Letters A, 365*(5), 403–406.
41. Zhou, J., & Pang, M. (2010). Digital watermark for printed materials. In *2010 2nd IEEE international conference on network infrastructure and digital content* (pp. 758–762). IEEE.

Jan Sher Khan has recently completed his master in Electrical and Electronics Engineering (with highest distinction) from the Department of Electrical and Electronics Engineering, Gaziantep University, Turkey. He obtained his bachelor of science degree in Electrical Engineering (with highest distinction), from HITEC University Taxila, Pakistan. As an exchange student, he completed his fourth year of undergraduate studies in the Department of Electric and Electronics Engineering at Istanbul Technical University (ITU), Turkey. His research interest includes chaos based encryption, cryptography, compressive sensing, machine learning and medical imaging.

Sema Koç Kayhan received M.Sc. and Phd degrees in Electrical and Electronic Engineering from the University of Gaziantep, Turkey. Currently, she is an Associate Professor in Electrical and Electronic Engineering Department at the University of Gaziantep Turkey, and working on signal and image processing.

Saygin Siddiq Ahmed received his PhD in Bio-electronics from the University of Gaziantep, Turkey. He obtained his Master of Science degree in Electrical and Electronics Engineering from the same university in 2003. He has taught a number of computer science and engineering courses for more than 10 years in several colleges. His research interest includes security, compression, machine learning and robotics.

Jawad Ahmad is an experienced researcher with more than 10 years of cutting-edge research and teaching experience in prestigious institutes including Edinburgh Napier University (UK), Glasgow Caledonian University (UK), Hongik University (South Korea) and HITEC University Taxila (Pakistan). He has co-authored more than 100+ research papers, in international journals and peer-reviewed international conference proceedings. He has taught various courses both at Undergraduate (UG) and Postgraduate (PG) levels during his career. He regularly organizes timely special sessions and workshops for several flagship IEEE conferences. He is an invited reviewer for numerous world-leading high impact journals (reviewed 100+ journal papers to date). His area is cybersecurity, multimedia encryption, machine learning, and application of chaos theory in cybersecurity.

Hafza Ayesha Siddiqa is currently pursuing her PhD in Biomedical Engineering, Fudan University, China. She recently completed her master of Electrical Engineering in the Department of Electrical Engineering, HITEC University, Pakistan. She received her B.Sc. degree in Electrical Engineering in 2015 from HITEC University, Pakistan. Her research interest includes machine learning, fuzzy, control and chaos.

Fawad Ahmed graduated in Industrial Electronic Engineering from NED University of Engineering and Technology, Pakistan in 1994. He did his MS from UNSW, Australia in 1998 and Ph.D. from NTU, Singapore in 2010. From 1998 to 2010 he replaced as a lecturer and then as an Assistant Professor at Pakistan Navy Engineering College, National University of Sciences and Technology, Pakistan. From 2010 to 2021 he was working as an Associate Professor in the Department of Electrical Engineering, HITEC University Taxila. He has recently joined the Department of Cyber Security, Pakistan Navy Engineering College, NUST, Pakistan. His research interests include image hashing, image encryption and bio-hashing.

Baraq Ghaleb (Student Member, IEEE) received the B.Sc. degree in computer science from the University of Jordan, Amman, Jordan, in 2009, and the M.Sc. degree from the Jordan University of Science and Technology, Irbid, Jordan, in 2013, and the Ph.D. degree in applied computing from Edinburgh Napier University, Edinburgh, U.K. His current research interests include routing protocols in low-power and lossy networks and the Internet of Things (IoTs), security of LLNs, and the IoT in addition to data mining. He holds one patent in the field of the IoT Routing.

Ahmed Al Dubai received the Ph.D. degree in computing from the University of Glasgow, Glasgow, UK, in 2004. In 2004, he joined the University of West London, London, UK In 2005, he joined Edinburgh Napier University, Edinburgh, UK, where he became a Professor and the Programme Leader of the Post-Graduate Research degrees with the School of Computing.He is currently the Head of the Networks Research Group. He has been published in world leading journals and in prestigious international conferences. He has also been involved with research in the area of group communication algorithms,smart spaces, and high-performance networks. He is a Fellow of the Higher Academy, UK He was a recipient of the several academic awards and recognitions, and a member of several Editorial Boards of scholarly journals. He has served as a Guest Editor for more than 20 special issues in scholarly journals and chaired and co-chaired more than 30 international conferences/workshops.