applied sciences

MDPI

Article

Image Watermarking Scheme Using LSB and Image Gradient

Zaid Bin Faheem [1], Mubashir Ali [2], Muhammad Ahsan Raza [3], Farrukh Arslan [4], Jehad Ali [5,*], Mehedi Masud [6] and Mohammad Shorfuzzaman [6]

[1] Department of Computer Engineering, University of Engineering & Technology, Taxila 47080, Pakistan; zaid_fahim@yahoo.com
[2] Department of Software Engineering, Lahore Garrison University, Lahore 54000, Pakistan; mubashirali@lgu.edu.pk
[3] Department of Information Technology, Bahauddin Zakariya University, Multan 60000, Pakistan; ahsanraza@bzu.edu.pk
[4] Department of Electrical Engineering, University of Engineering and Technology, Lahore 54000, Pakistan; farrukh_arslan@uet.edu.pk
[5] Department of Computer Engineering and Department of AI Convergence Network, Ajou University, Suwon 16499, Korea
[6] Department of Computer Science, College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia; mmasud@tu.edu.sa (M.M.); m.shorf@tu.edu.sa (M.S.)
* Correspondence: jehadali@ajou.ac.kr

Abstract: In the modern age, watermarking techniques are mandatory to secure digital communication over the internet. For an optimal technique, a high signal-to-noise ratio and normalized correctional is required. In this paper, a digital watermarking technique is proposed on the basis of the least significant bit through an image gradient and chaotic map. The image is segmented into noncorrelated blocks, and the gradient of each block is calculated. The gradient of the image expresses the rapid changes in an image. A chaotic substitution box (S-Box) is used to scramble the watermark according to a piecewise linear chaotic map (PWLCM). PWLCM has a positive Lyapunov exponent and better balance property as compared to other chaotic maps. This S-Box technique is capable of producing a disperse sequence with high nonlinearity in the generated sequence. Least significant bit is a simple technique for embedding but it has a high payload capacity and direct pixel manipulation. The embedding payload introduces a tradeoff between robustness and imperceptibility; hence, the image gradient is a technique to identify the best-suited place to embed a watermark and avoid image degradation. By modifying the least significant bits of the original image, the watermark signal is embedded according to the image gradient. In the image gradient, the direction and magnitude decide how much embeding can be done. In comparison with other methods, the experimental results show satisfactory progress in robustness against several image processing and geometrical attacks while maintaining the imperceptibility of the watermark signal.

Keywords: substitution box; chaotic map; piecewise linear chaotic map; least significant bit; image gradient

Citation: Faheem, Z.B.; Ali, M.; Raza, M.A.; Arslan, F.; Ali, J.; Masud, M.; Shorfuzzaman, M. Image Watermarking Scheme Using LSB and Image Gradient. *Appl. Sci.* **2022**, *12*, 4202. https://doi.org/10.3390/app12094202

Academic Editor: Arcangelo Castiglione

Received: 29 March 2022
Accepted: 19 April 2022
Published: 21 April 2022

1. Introduction

Information technology has led to a great revolution in the field of digital communication. In addition to other benefits, it facilitates the distribution, operation, and replication of digital data, thus threatening the safe ownership of digital media. Digital image watermarking is a technique specially designed to solve these issues. In image watermarking, the owner's secret information is implanted into the image, video, and audio without effecting the acceptable quality. The embedded owner's secret information can later be extracted for authentication. The most important aspect of image watermarking is copyright safety and content authentication. Watermarking is classified into image, audio, video, and text

watermarking related to the type of data being watermarked. Image watermarking is further categorized into spatial-domain watermarking and transform-domain watermarking. Watermarks can be embedded in the spatial domain by manipulating pixel strength of the cover image, while watermarks in the transform domain are embedded by manipulating the transform coefficient [1]. Watermarking in the spatial domain is easy to implement and has high perceptual quality. The simplest method in the spatial domain is least significant bit substitution. Transform-domain techniques are more robust at the cost of computational overhead. The common methods in the transform domain are discrete wavelet transform (DWT) and discrete cosine transform (DCT), but the choice of transform depends on the complexity, cost of implementation, and speed of operation [2]. The imperceptibility and robustness of the scheme depend on the embedded watermark capacity.

In common signal operations such as filtering, JPEG compression, geometric attacks, and addition of noise, watermarking techniques have shown satisfactory progress [3]. To manipulate information is the main purpose of attack. The goal of the watermarking technique is robustness, high capacity, and imperceptibility [4,5]. Depending on the embedding purpose, the watermarking technique can be divided into robust and fragile watermarking. A fragile watermark is destroyed after a slight modification and used for authentication and tamper detection. A robust watermark is strong and has the ability to resist slight modification, which can be used for copyright protection and owner confirmation.

Base on the type of watermark insertion, techniques can be classified into visible and invisible watermarking. In visible watermarking, human eyes perceive the watermark without extraction, while, in invisible watermarking, it cannot be perceived without extraction. According to watermark detection, watermarking practices are grouped into blind, nonblind, and semi-blind. In blind watermarking, watermark is only visible by using secret key [6]; however, in semi-blind and nonblind watermarking, extra information is needed for extraction [7].

The substitution box is the counter-clockwise component used in cryptosystems, providing cryptosystems with the confusion property defined by Shannon in his famous paper [8]. The basic features of cryptography such as confusion and diffusion correspond with the features of chaos [9]. Chaotic systems have many exciting features, such as mixing property, ergodicity, and sensitivity to initial conditions; these characteristics of chaos make them ideal to design an S-Box with chaos [10]. The S-Box design using chaos is dynamic in nature, while the S-Box used in AES and DES is static in nature. The security strength of block ciphers depends upon the substitution box.

Some recent research related to digital image watermarking is summarized here. Jun et al. [11] proposed an image watermarking based on fractional Fourier transform. This scheme could withstand image handling tasks like JPEG compression, but it had high computational cost due to its complexity. Tun et al. [12] suggested a blind watermarking approach using discrete cosine and lifting wavelet transform. In this approach, the watermarked image showed high imperceptibility. The major concern of this approach is making the watermark imperceptible regardless of the robustness against attacks. Su et al. [13] suggested a spatial0domain watermarking approach relying on the distribution feature of the direct current coefficient. This technique incorporated the computational efficiency and robustness features of the spatial domain and frequency domain. The extracted watermark robustness can be compared with other image watermarking techniques. Parab [14] offered a method combining image filtering with image watermarking and improved the privacy of watermark images. Soualmi et al. [15] combined a weber descriptor, chaotic map, and DCT transform for blind medical image watermarking, where the weber descriptor was used for embedding and extraction processes. The planned method showed good results, but it had some limitations in implementation. Mittal et al. [16] proposed a method based on curvelet domain, which showed good progress in watermark embedding and watermark extraction time, but the structure similarity of the watermarked image was not good. Another technique based on all phase discrete cosine biorthogonal transform (APDCBT), DWT, and SVD was proposed by Zhou et al. [17]. This technique used DC coefficients for

embedding and extracting the watermark, because of its better perceptual capacity than AC coefficients. The PSNR and robustness against attacks were good, but the technique was computationally expensive. In [18], a digital image watermarking technique based on DCT, DWT, and SVD was recommended. This technique was robust against geometric attacks. The disadvantage of this technique was its effect on the host image. The comparative literature comparison is given in Table 1.

Table 1. Literature review of watermarking techniques.

Method	Blind	Robustness	Extraction Type
[19]	Yes	Robust to common (R2C) image processing attacks	Multi-bit
[20]	Yes	R2C, JPEG, and cropping	Single-bit
[21]	No	R2C attacks	Multi-bit
[22]	Yes	R2C attacks	Multi-bit
[23]	Yes	Robust to Rotation and Flipping attacks	Multi-bit

The remainder of the paper is arranged as follows: Section 3 proposes the methodology for watermark implanting and watermark extraction; Section 4 presents and discusses the experimental evaluation; Moreover, Section 5 provides the conclusion.

Our Contribution

In this paper, we introuduce a watermarking strategy for protecting the watermark signal, in which an original image is divided into 16 × 16 blocks, and a gradient is applied to calculate the magnitude and direction of each block. The gradient magnitude denotes image changes, while the gradient angle denotes the direction of changes. The capacity of the watermark signal is embedded according to the gradient of each block using the least significant bit technique. In image watermarking, the researcher tries to embed maximum payload without affecting the image visual quality. Greater embedding ensures more robustness; thus, spatial-domain techniques, e.g., LSB, provide a higher payload compared to frequency-domain techniques. The main concern is to balance the performance in terms of undetectability, robustness, and algorithmic complexity. LSB is computationally efficient and has high perceptual quality. To increase security, the watermark to be embedded is scrambled using a chaotic substitution box. This method shows high robustness and imperceptibility when the middle coefficient is used for embedding.

2. Preliminaries

2.1. Image Gradient

The image gradient is a core component in image processing, used to find the directional variation in the intensity of the image. The gradient magnitude and direction denote how and where variations occur. The gradient image pixel represents the change in pixel value of the original image at that point, in the relative direction. The magnitude and direction of the gradient are calculated by the equations below.

$$\mathrm{M} = \sqrt{{g_y}^2 + {g_x}^2}, \tag{1}$$

where g_y is the gradient in the y-direction, and g_x is gradient in x-direction. M is the magnitude of the gradient. The direction of the gradient is measured by λ.

$$\lambda = \tan^{-1}\left(\frac{g_x}{g_x}\right) \tag{2}$$

The image gradient in this proposed process is measured by convolving the original image block with the Prewitt operator. In gradient image, the pixels with large values indicate the edges. To visualize the direction, x- and y-direction image gradients are calculated. The filter to calculate the x- and y-direction gradients is shown below

$$M=\begin{bmatrix} -1 & 0 & 1 \\ -1 & 0 & 1 \\ -1 & 0 & 1 \end{bmatrix}\begin{bmatrix} -1 & -1 & -1 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \end{bmatrix}$$

The main concern of this approach is to classify the image into smooth and sharp portions, in order to achieve better imperceptibility of the image. For this purpose, a threshold is calculated to differentiate the local smoothness and sharpness in each block. On the basis of this threshold, a decision can be made on how many bits are to be embedded through LSB embedding.

2.2. Least Significant Bit (LSB) Embedding

The LSB is the simplest method available for watermark insertion in spatial-domain watermarking. In the LSB method, operations are directly performed on pixel values, resulting in minor changes in pixel values. By changing the LSB of the host image, a watermark is applied. The insertion and extraction principles are simple and effective. This LSB method has high perceptual quality and is mostly used in fragile watermarking. Figure 1 shows the embedding through message bytes.

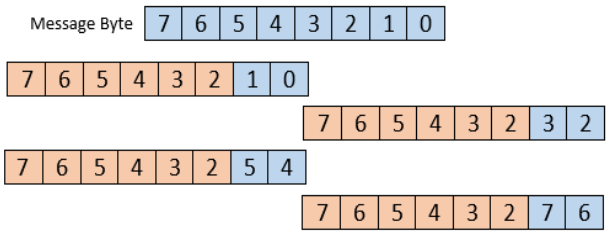


Figure 1. Embedding with message bytes.

2.3. Piecewise Linear Chaotic Map

The piecewise linear chaotic map (PWLCM) has recently gained attention because of its ease in depiction, effectiveness in application, and good vital non-linear behavior [24]. It has been proven that PWLCMs are random and have a constant density function on their classification interim. Figure 2 shows the positive values of PWLCM and the Lyapunov exponent, indicating that PWLCM is chaotic in the given range. Chaotic systems always show random behavior.

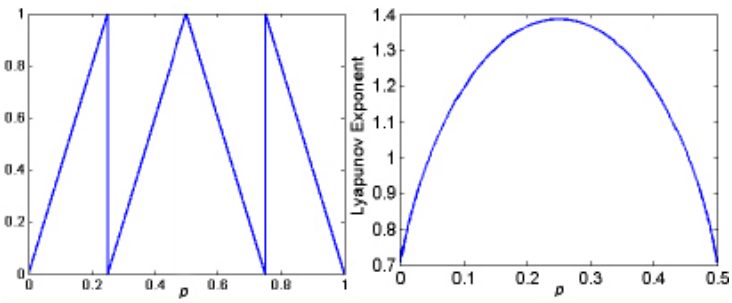


Figure 2. PWLCM plot and Lyapunov exponent [23].

A PWLCM with four intervals can be indicated by the following equation:

$$x_{n+1} = \begin{cases} \frac{x_n}{p}, & 0 \le x_n < p \\ \frac{(x_n, -, p)}{(0.5, -, p)}, & p \le x_n < 0.5 \\ \frac{(1-p-x_n)}{(0.5, -, p)}, & 0.5 < x_n < 1-p \\ (1, -, x_n)/p, & 1-p < x_n < 1.0 \end{cases} \quad (3)$$

where $x_0 \in [0, 1)$, and p is the control factor $p \in (0, 0.5)$.

2.4. Chaotic Substitution Box

A substitution box is one of the principal components in a block cipher, and it has a vital role in the substitution process. All topical ciphers follow Shannon's principal of confusion and diffusion. The S-Box used to introduce confusion in a system. The security strength of block ciphers depends upon the substitution box. Thus, it is difficult in research to assemble a strong substitution box that can pass on high nonlinearity and low differential probability values. In general, the S-Box is an auxiliary table which takes multiple input bits and randomly transforms them into output bits. Bijection cryptographic properties motivated its design, considering The nonlinearity [25], strict avalanche criterion [26], bit independence criterion [26], and linear and differential approximation probability [9,26]. Zaid et al. [27] planned a simple and efficient S-Box design based on a PWLCM map and adaptive optimization technique. Algorithm 1 shows the pseudo code of the S-Box. The proposed S-Box has few mathematical computations and shows better nonlinearity and differential probability values. The random sequence of the S-Box value is shown in Table 2.

Table 2. Generated substitution box.

-	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	179	182	224	91	159	102	75	150	151	215	234	211	145	212	85	17
2	105	95	197	147	183	181	117	188	187	255	137	9	26	41	32	83
3	189	161	52	171	93	22	223	193	236	2	228	62	227	1	172	162
4	74	166	33	126	155	140	201	63	119	149	133	191	10	25	254	167
5	99	142	207	252	176	218	40	97	232	64	199	86	131	160	190	158
6	173	23	20	19	113	129	251	165	198	70	15	237	244	128	139	61
7	122	5	130	121	214	21	30	144	48	87	170	60	68	36	163	123
8	239	37	247	235	3	110	73	206	136	81	65	107	80	219	92	229
9	100	231	50	125	24	205	96	23	230	154	72	4	57	98	146	8
10	175	152	27	249	156	28	164	55	127	177	196	116	47	216	58	124
11	115	94	169	38	108	178	148	7	253	204	54	222	203	246	217	245
12	220	157	134	242	51	106	194	45	153	78	111	18	35	118	202	114
13	0	168	238	82	31	192	59	12	180	109	208	44	221	34	49	241
14	209	135	112	104	195	67	43	76	174	225	250	11	243	69	185	29
15	16	233	210	186	56	77	6	184	120	101	84	71	79	39	248	226
16	103	138	14	240	46	66	42	88	141	200	143	90	89	13	53	132

Algorithm 1: S-Box Generation

1: **Input** x_n, p, I
2: **Output** S-BOX
3: **While** (i < 300) **Do**:
4: iterate PWLCM with x_n
5: set $x_{n+1} = x_n$
6: X ← Floor (x × 256)
7: **If** X ∉ S-Box **then**
8: Sub-Box ← X
9: i = i + 1;
10: **Else**
11: iterate PWLCM with x_n
12: **End If**
13: Optimization
14: **End-While**
15: Show Sub-Box

3. Methodology

3.1. Watermarking Scheme

In this paper, an image watermarking based on a chaotic map using LSB and image gradient is presented. The goal of this technique is to provide high capacity, imperceptibility, and robustness against attacks. The performance of our suggested approach is tested by considering well-known parameters, i.e., peak signal-to-noise ratio (PSNR) and normalized correlation (NC). The appropriate embedding positions are chosen using the gradient magnitude and direction of the individual image block. The embedding used in this technique is LSB because of its low computation cost and high perceptual capacity. This proposed framework gives high robustness against common image processing and geometrical attacks because of its embedding in edge surface areas.

3.2. Watermarking Embedding

Figure 3 shows the watermark embedding process, consisting of seven steps. Moreover, Figure 4 represents the flow diagram for extraction of watermark.

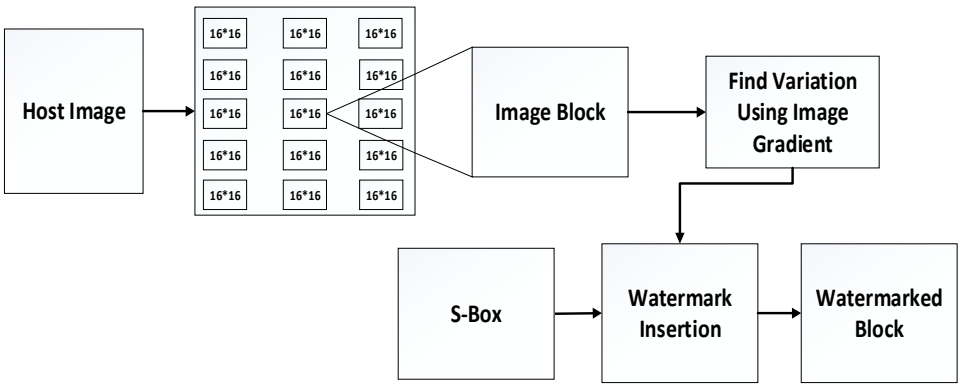


Figure 3. Watermark insertion flow diagram.

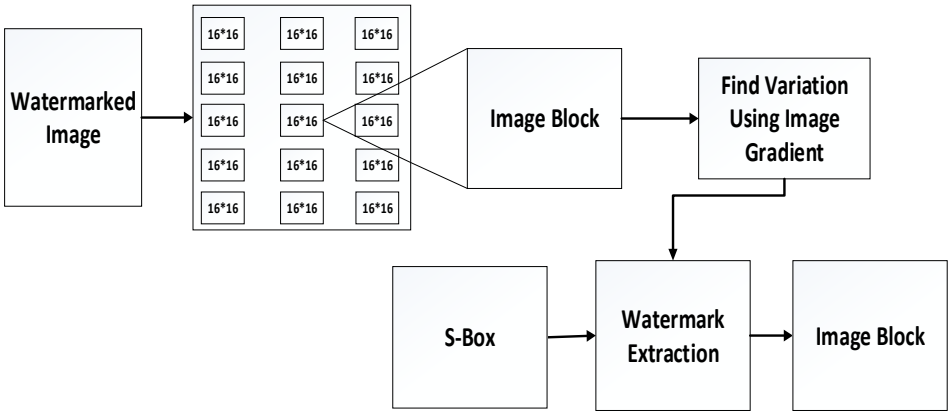


Figure 4. Watermark extraction flow diagram.

Step 1. Divide the host image into 16 × 16 nonoverlapping blocks. The nonoverlapping blocks prevent data loss.

Step 2. Calculate the gradient of each block, i.e., gradient magnitude and direction.

Step 3. Choose the central pixel of each block, and separate them into LSB and MSB.

Step 4. Watermark signals are embedded in the LSB according to the following cases:

For magnitude $M = \sqrt{{g_y}^2 + {g_x}^2}$,

For direction $\lambda = \tan^{-1}\left(\frac{g_x}{g_x}\right)$

Case 1: M ≥ (max (magnitude)/2) && $\lambda > 0$; in this case, one-bit watermark is implanted into the LSB.

Case 2: M < (max (magnitude)/2) && $\lambda < 0$; in this case, two watermark bits are implanted into the LSB.

Step 4. Select the watermark image and scramble it using the chaotic substitution box.

Step 5. Split the scrambled watermark into LSB and MSB. XOR the LSB of the watermark with the one- or two-bit LSB of the host image.

Step 6. Watermarked image can be constructed with the combination of LSB and MSB.

Step 7. To extract the watermark image, conduct all steps in reverse.

4. Experimental Results

In this section, to check the performance of proposed scheme, MATLAB-2017 software on a computer with sixth generation Windows 10 and 8 GB RAM was used to conduct tests on standard images taken from the SIPI Image Database at the University of Southern California (http://sipi.usc.edu/database/, accessed on 22 March 2022). Grayscale testing images Lena and Baboon with a standard size of 512 × 512 and a 32 × 32 grayscale logo as a watermark signal were used. To observe the imperceptibility and robustness of the testing images, several experiments were performed by varying the intensities of the image processing attacks and geometrical attacks.

4.1. Perceptual Quality Measures

To calculate the watermarked image perceptual quality, two performance metrics were calculated, i.e., PSNR and structural similarity (SSIM). PSNR measures the visual eminence between the original and watermarked image. A larger value of PSNR shows the visual equivalence of the real and watermarked image. The mathematical formula to measure peak signal to noise ratio is

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{(255)^2}{(\mathrm{MSE})}\right), \tag{4}$$

where the value 255 is the extreme image pixel strength. The term *MSE* stands for the mean squared error of image.

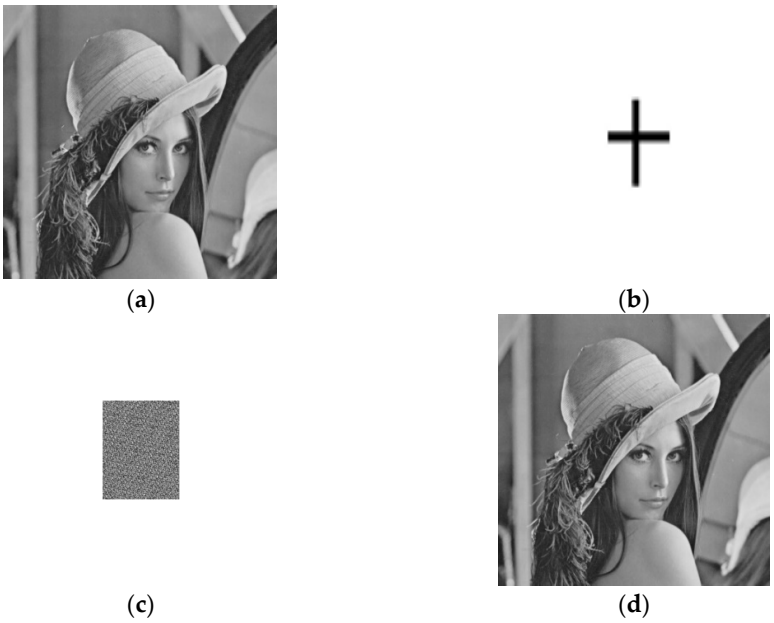
$$MSE = \frac{1}{M \times N} \sum_{m=1}^{M} \sum_{n=1}^{N} e(m,n)^2 \quad (5)$$

where $M \times N$ is the size of the image, and $e\ (m,\ n)^2$ is the difference between the watermarked and real image.

SSIM measures the similarity between two images on the basis of luminance, contrast, and structure. The mathematical formula of similarity measure is

$$\text{SSIM}\ (x,\ y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_x\sigma_y + C_2)}{(\mu_x^2\mu_y^2 + C_1)(\sigma_x^2\sigma_y^2 + C_2)} \quad (6)$$

where $\mu_x\ \mu_y$ are the averages of x and y, are the variances of x and y, and is the covariance of x and y. Figure 5 reveals various images i.e., actual image and watermark inserted image.



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

Figure 5. (**a**) Original Lena image; (**b**) watermark image; (**c**) scramble image; (**d**) watermarked Lena image.

The PSNR and SSIM of the Lena and Baboon watermarked images without any attack are shown in Table 3.

Table 3. Performance measures.

Image Quality Assessment (IQA)	Suggested Method (Lena-Image)	Suggested Method (Baboon-Image)
PSNR	57.58	53.19
SSIM	1	1

4.2. Robustness of Watermarking Algorithm

To check the robustness of the watermarking method, the normalized correlation between the real and extracted watermark was calculated. This shows its resistance against different image processing and geometrical attacks. The normalized correlation value

varies between 0 and 1; a value close to one indicates that the watermarking algorithm has strong robustness.

$$NC = \frac{\sum_i W_{ij} \sum_j W'_{ij}}{\sum_i \sum_j (W_{ij})^2} \quad (7)$$

where W_{ij}, $W_{ij}{}'$ are the inserted and withdrawal watermark strength at point (i, j). The normalized correlation values across multiple attacks i.e., image handling and geometrical are given in Table 4.

Table 4. Normalized correlation strength.

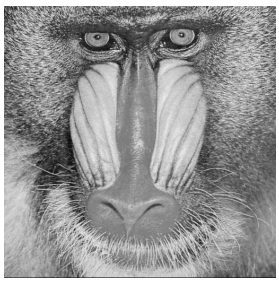
Attacks	Strengths	NC
Salt and Pepper (S&P)	0.1	0.9918
S&P	0.2	0.9850
S&P	0.5	0.9853
S&P	1.0	0.9918
Speckle	0.04	0.9937
Gaussian	0.05	0.9918
JPEG	75%	0.9976
JPEG	20%	0.9966
JPEG	10%	0.9937
Median Filter	[3 3]	0.9962
Median Filter	[5 5]	0.9966
Rotation	−50	0.9966
Translation	[50 50]	0.9955
Cropping	25%	0.9993
Cropping	50%	0.9988

4.3. Comparison with Other Paper

In this section, we compare the results of our suggested techniques with other techniques. In [28], watermarking was achieved using DWT, DCT, and image gradient. DWT separates the image into multiple bands for insertion. The gradient is used to give a topological map of the image. The method in [13] is blind, whereby the watermark is embedded in the blue component of the RGB image in the spatial domain. The imperceptibility analysis of the methods in [13,28,29] for the baboon image is shown in Table 5. Figure 6 shows different types of images.

Table 5. Imperceptibility analysis.

IQA	Suggested Technique	[28]	[13]
PSNR	53.18	42	49.89
SSIM	1	1	1



(**a**)

(**b**)

Figure 6. *Cont.*

(**c**) (**d**)

Figure 6. (**a**) Original baboon image; (**b**) watermark image; (**c**) scramble image; (**d**) watermarked baboon image.

Noise insertion, smoothening, cropping, and contrast enhancement are considered common image processing distortions. A comparison of these factors with the method suggested by Mokhnache et al. [28] is shown in Table 6. Figure 7 indicates the comparison of SSIM and PSNR.

Table 6. Normalized Correlation Against Image Processing Attacks.

Attacks	Strengths	Normalized Correlation	
		Suggested Technique	[28]
S&P	0.01	0.9970	0.6833
S&P	0.03	0.9948	0.4013
Gaussian Noise	0.001	0.9910	0.9036
Gaussian Noise	0.003	0.9904	0.6974
JPEG	60%	0.9916	0.9713

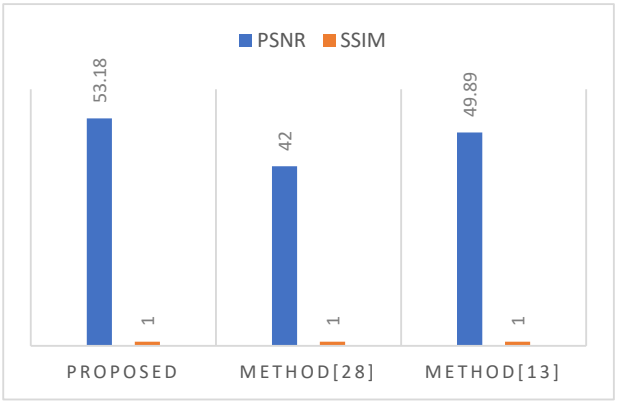


Figure 7. PSNR and SSIM comparison.

Table 7 shows that suggested method has more robustness than the method proposed by Su et al. [13].

In image watermarking, a geometric attack is basically a displacement of a pixel by a random amount. In other words, the original watermark is present, but bits are displaced. The development of such a technique is compulsory in geometric distortion correction. Table 8 illustrates the attacks and normalized correlation results.

Table 7. Normalized correlation against image processing attacks.

Attacks	Strengths	Normalized Correlation	
		Suggested Technique	[13]
S&P	0.01	0.9970	0.9032
S&P	0.02	0.9957	0.9055
Gaussian Noise	0.05	0.9875	0.9977
Gaussian Noise	0.10	0.9872	0.9816
JPEG	60%	0.9916	0.7512

Table 8. Normalized correlation against image geometrical attacks.

Attacks		Normalized Correlation		
		Suggested Technique	[28]	[13]
Image Cropping	25%	0.9975	0.2827	1.0
Median Filter	3×3	0.9940	0.3124	0.8848

5. Conclusions

In order to determine the efficiency of a watermarking technique, some important properties should be analyzed. Firstly, the effectiveness denotes whether the watermark signal embedded in the host image is properly detected. The value of normalized correlation shows the correctness of the watermark; if it is close to 1, the watermark signal is correctly detected. Secondly, imperceptibility denotes whether there is any effect on the perceptual transparency of the watermark embedded in the host image. Thirdly, the payload denotes the mass of content embedded in the digital image. Increasing the content facilitates watermark detection. Fourthly, security denotes the ability to resist against attacks. A secure cryptographic key is secure against cryptographic attacks. In this article, an LSB and image gradient-based image watermarking approach was presented. The original image was divided into nonoverlapping blocks, and the gradient of each block was calculated. In this way, the smooth and irregular areas of the image could be identified for watermark embedding. Finally, LSB was used to introduce watermarked bits. This approach functioned in the time domain, providing computational efficiency and high perceptual quality. It showed significant robustness against image processing and geometrical attacks. In the future, the proposed technique will be investigated for resistance against modern attacks, such as the boomerang attack. Moreover, this technique will be extended for color and video watermarking.

Author Contributions: Conceptualization, Z.B.F.; data curation, M.A.R.; formal analysis, M.A., F.A., M.M., J.A. and Z.B.F.; investigation, M.S. and M.A.; methodology, Z.B.F.; project administration, M.S. and M.M.; resources, M.A. and M.A.R.; software, M.A.; supervision, M.A.R., M.S. and M.M.; validation, Z.B.F.; visualization, F.A.; writing—original draft, Z.B.F., M.A. and M.A.R.; writing—review and editing, J.A., M.M., M.S. and F.A.; proofreading and writing the paper script in overleaf, M.A.R. and M.M. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Taif University Researchers Supporting Project number (TURSP-2020/79), Taif University, Taif, Saudi Arabia.

Institutional Review Board Statement: Not Applicable.

Informed Consent Statement: Not Applicable.

Data Availability Statement: Not Applicable.

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

References

1. Kalivaraprasad, B.; Prasad, M.; Babu, K.R.; Shameem, S.; Mohan, S.; Vani, V. Comparative Analysis of Watermarking Methods on CFRP Sample Thermal Images. In *Computer Communication, Networking and IoT*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 455–462.
2. Matheswaran, P.; Navaneethan, C.; Meenatchi, S.; Ananthi, S.; Janaki, K.; Manjunathan, A. Image Privacy in Social Network Using Invisible Watermarking Techniques. *Ann. Rom. Soc. Cell Biol.* **2021**, *25*, 319–327.
3. Wang, X.-Y.; Liu, Y.-N.; Xu, H.; Wang, A.-L.; Yang, H.-Y. Blind optimum detector for robust image watermarking in nonsubsampled shearlet Domain. *Inf. Sci.* **2016**, *372*, 634–654. [CrossRef]
4. Rahmani, H.; Mortezaei, R.; Moghaddam, M.E. A new robust watermarking scheme to increase image security. *EURASIP J. Adv. Signal Process.* **2010**, *2010*, 105. [CrossRef]
5. Benoraira, A.; Benmahammed, K.; Boucenna, N. Blind image watermarking technique based on differential embedding in DWT and DCT domains. *EURASIP J. Adv. Signal Process.* **2015**, *2015*, 55. [CrossRef]
6. Lam, P.; Winkelmeyer, O.; Mehdi, S.A.; Kamoosi, N. Watermarking Technologies-Analysis and Design Report. Available online: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.630.6293&rep=rep1&type=pdf (accessed on 18 April 2022).
7. Hovančák, R.; Levický, D. Comparison of watermarking methods using DCT transformation. *Watermark* **2003**, *1*, C3.
8. Shannon, C.E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **1949**, *28*, 656–715. [CrossRef]
9. Kocarev, L. Chaos-based cryptography: A brief overview. *IEEE Circuits Syst. Mag.* **2001**, *1*, 6–21. [CrossRef]
10. Khan, M.; Shah, T.; Mahmood, H.; Gondal, M.A.; Hussain, I. A novel technique for the construction of strong S-boxes based on chaotic Lorenz systems. *Nonlinear Dyn.* **2012**, *70*, 2303–2311. [CrossRef]
11. Lang, J.; Zhang, Z.-G. Blind digital watermarking method in the fractional Fourier transform domain. *Opt. Lasers Eng.* **2014**, *53*, 112–121. [CrossRef]
12. Tun, A.; Thein, Y. Digital image watermarking scheme based on LWT and DCT. *Int. J. Eng. Technol.* **2013**, *5*, 272. [CrossRef]
13. Su, Q.; Chen, B. Robust color image watermarking technique in the spatial domain. *Soft Comput.* **2018**, *22*, 91–106. [CrossRef]
14. Parab, A.V. *Improving Confidentiality of Watermark Image through Image Filtering Techniques*; National College of Ireland: Dublin, Ireland, 2019.
15. Soualmi, A.; Alti, A.; Laouamer, L. A New Blind Medical Image Watermarking Based on Weber Descriptors and Arnold Chaotic Map. *Arab. J. Sci. Eng.* **2018**, *43*, 7893–7905. [CrossRef]
16. Mittal, M.; Kaushik, R.; Verma, A.; Kaur, I.; Goyal, L.M.; Roy, S.; Kim, T.-H. Image Watermarking in Curvelet Domain Using Edge Surface Blocks. *Symmetry* **2020**, *12*, 822. [CrossRef]
17. Zhou, X.; Zhang, H.; Wang, C. A Robust Image Watermarking Technique Based on DWT, APDCBT, and SVD. *Symmetry* **2018**, *10*, 77. [CrossRef]
18. Zheng, P.; Zhang, Y. A robust image watermarking scheme in hybrid transform domains resisting to rotation attacks. *Multimed. Tools Appl.* **2020**, *79*, 18343–18365. [CrossRef]
19. Das, A.; Zhong, X. A Deep Learning-based Audio-in-Image Watermarking Scheme. In Proceedings of the 2021 International Conference on Visual Communications and Image Processing (VCIP), Munich, Germany, 5–8 December 2021; pp. 1–5.
20. Furon, T. Are Classification Deep Neural Networks Good for Blind Image Watermarking? *Entropy* **2020**, *22*, 198.
21. Sedik, A.; Hammad, M.; El-Samie, F.E.A.; Gupta, B.B.; El-Latif, A.A.A. Efficient deep learning approach for augmented detection of Coronavirus disease. *Neural Comput. Appl.* **2021**, 1–18. [CrossRef]
22. Ge, S.; Xia, Z.; Fei, J.; Sun, X.; Weng, J. A Robust Document Image Watermarking Scheme using Deep Neural Network. *arXiv* **2022**, arXiv:2202.13067.
23. Ali, M.; Ahn, C.W.; Pant, M.; Kumar, S.; Singh, M.K.; Saini, D. An optimized digital watermarking scheme based on invariant DC coefficients in spatial domain. *Electronics* **2020**, *9*, 1428. [CrossRef]
24. Ahmad, M.; Ahmad, F.; Nasim, Z.; Bano, Z.; Zafar, S. Designing chaos based strong substitution box. In Proceedings of the 2015 Eighth International Conference on Contemporary Computing (IC3), Washington, DC, USA, 20–22 August 2015; pp. 97–100.
25. Meier, W.; Staffelbach, O. Nonlinearity criteria for cryptographic functions. In *Workshop on the Theory and Application of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 1989; pp. 549–562.
26. Webster, A.; Tavares, S.E. On the design of S-boxes. In *Conference on the Theory and Application of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 1985; pp. 523–534.
27. Faheem, Z.B.; Ali, A.; Khan, M.A.; Ul-Haq, M.E.; Ahmad, W. Highly dispersive substitution box (S-box) design using chaos. *ETRI J.* **2020**, *42*, 619–632. [CrossRef]
28. Mokhnache, S.; Bekkouche, T.; Chikouche, D. A Robust Watermarking Scheme Based on DWT and DCT Using Image Gradient. *Int. J. Appl. Eng. Res.* **2018**, *13*, 1900–1907.
29. Bhalerao, S.; Ansari, I.A.; Kumar, A. Security Analysis of SVD-Based Watermarking Schemes and Possible Solutions. In *Soft Computing: Theories and Applications*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 529–537.