Palestine Journal of Mathematics

Vol 14(3)(2025) , 959–975

Blind Image Watermarking Technique Based on SHA-256, LWT and Modified Hénon Map

D. Singh, M. K. Patel, L. Chandra, H. Sharma and S. Kumar

Communicated by Manoj Patel

MSC 2020 Classifications: Primary 94A08; Secondary 68P25.

Keywords and phrases: Watermarking, modified Hénon map, sine map, encryption, lifting wavelet transformation (LWT).

The authors would like to thank the reviewers and editor for their constructive comments and valuable suggestions that improved the quality of our paper

Acknowledgement: The first author is thankful to DST, India, for support through grant no.: SR/FST/MS- 1/2021/104(C) under DST-FIST project.

Corresponding Author: S. Kumar

Abstract Many researchers are engaged to create methods to conceal digital information in another digital signal due to the rise in cyberattacks. Digital data watermarking is one of the practical approaches for data protection and verifying authenticity by hiding some key information behind some carrier information. Traditional watermarking techniques are less secure and slower in execution. This work presents a robust and efficient digital watermarking method based on the chaotic maps: sine map and modified Hénon map along with the lifting wavelet transformation (LWT). The secure SHA-256 hash function is first applied to the host image to generate the initial conditions for both the modified Hénon map and sine map. To prevent manipulation by attackers and to increase blindness, confusion and diffusion are employed to the watermark logo image before embedding it into the host image. The sine map is utilized for confusion, whereas the diffusion is completed with the help of the modified Hénon map. The LWT is employed on the host image, to split it into Low-Low (LL), Low-High (LH), High-Low (HL), and High-High (HH) bands, followed by the embedding of the ciphered watermark. Further, to increase randomness during embedding and for additional security in watermarking, confusion among frequency bands is created before embedding of bits. Thus, it becomes difficult for eavesdroppers to extract the original information. The proposed technique's robustness, efficiency, and security are verified from the results of statistical analysis such as entropy, energy, correlation, classical attacks, structure similarity index, structure dissimilarity index, and structure content.

1 Introduction

The widespread use of digital media in all facets of daily life has been one of the most significant technological developments of the past two decades. As digital pictures, videos, and multimedia sounds are becoming more and more popular, they will soon dominate the fields of entertainment, arts, education, and so forth. Open networks allow for the efficient, high-quality storage/transmission and manipulation of this digital data. Furthermore, data communication through these open networks enables the quick and affordable transmission of digital data, whereas altered digital data poses a serious risk to those who produce and disseminate information, including news organizations, museums, significant medical reports and sensitive scientific data. Sometimes, owners of copyrights seek payment each time their work is used. Moreover, they wish to guarantee that their work is not misused (e.g., altered without their consent). Nonetheless, copyright enforcement and content verification are extremely challenging responsibilities when it comes to digital data. Digital images cover most of the utilised digital data and are two-dimensional pictures with a finite number of digital values, sometimes referred to as picture elements or pixels [4, 45].

Numerous problems with data security and privacy are present in digital data. Effective security measures are required to stop unauthorized usage of data. Owing to the rapid advancement of technology, adaptable software that effectively alters digital media is now available. These alterations are imperceptible. Such circumstances make multimedia data untrustworthy. It is highly advised to protect multimedia content that is accessible online. Several methods, including cryptographic encryption & decryption, steganography, and digital watermarking, are used to provide security to digital data [16]. Using an encryption method to limit access to the data would be one way to solve the problem. Encryption does not, however, offer complete safety because once decrypted, the data can be altered or transmitted without restriction [39]. Digital watermarking uses a specific algorithm to conceal copyright information from digital material. The author's serial number, the corporate emblem, some language, or some very significant photographs can all be used embedding data or watermark data. This confidential information is incorporated into the digital data (images, audio, and video) for owner identification, data authentication, and copyright protection. The watermark might be either visible or invisible inside the digital data. In general, the following essential requirements should be fulfilled by a successful watermarking system.

Imperceptibility: It should be challenging for a human observer to identify any perceptual distinction between the original documents and those that have been watermarked; in other words, watermarks shouldn't modify the information that is being protected.

trustworthiness: A effective watermarking method should provide legitimate proof to protect ownership rights in addition to creating it harder to generate fake watermarks.

Robustness: When a document is watermarked, the watermark should to be resistant to malicious attacks as well as standard signal processing, avoiding its removal by an unauthorised individual without also making the document meaningless. More specifically, even after the watermarked image has gone through typical signal processing procedures, they ought to be observable or extractable.

Tirkel originally introduced two watermarking methods to conceal the watermark data in the original data in 1993, which gave rise to the term "digital watermarking" [7]. Over the last decades, different watermarking techniques have been introduced in the filed of digital data security [6, 8, 10, 12, 14, 27, 29, 31, 42, 46, 48, 49, 52]. There are two types of digital watermarking methods for digital images: frequency domain-based and spatial-based. Watermarking techniques in which to embeds the watermark simply altering some pixels' grey levels of the host image, comes under spatial domain watermarking [38, 55, 55]. Even with a high embedding capacity in these spatial domain techniques, computer analysis might quickly uncover any buried information. Host images have been altered in the frequency domain via transformation such as discrete wavelet transform (DWT), discrete cosine transform (DCT), lifting wavelet transformation and discrete fourier transform (DFT) to embed the watermarks to their frequency coefficients, known as frequency domain-based watermarking scheme [13, 43]. Frequency-domain watermarking is typically robust since the embedded watermarks are distributed throughout the whole spatial extent of an image. Discrete cosine transformations are a method for splitting down a signal into its most basic frequency components. It shows an image as the sum of sinusoids with different frequencies and magnitudes [40]. In Fourier analysis, wavelets are special functions that serve as fundamental functions to characterise signals such as sines and cosines [54]. Further, DWT based $2-D$ image processing is equivalent to applying $2-D$ filters to each image dimension. The filters divide the input digital image into four non-overlapping multi-resolution sub-bands (LL1, LH1, HL1, and HH1). The sub-band LL1 represents the coarse-scale DWT coefficients, whereas the sub-bands LH1, HL1, and HH1 reflect the fine-scale DWT coefficients. In [12, 29, 42], to insert the watermark, the authors utilizes the discrete cosine transform coefficients. Vahedi et al. developed a new watermarking strategy for colour photos in 2012 and used the optimisation principles of genetic algorithms to improve the performance of several current schemes. Das et al. created an effective blind picture watermarking approach in the transform domain by utilising the correlation between DCT neighbouring coefficients [14]. A secure and singular value decomposition (SVD) based watermarking technique was given in [8]. The authors in [9, 28] discovered that real-time hardware implementation issues can be reduced by employing 8×8 block-wise DCT based watermarking techniques. Moulin et al. and Mukherjee et al. have created safe watermarking systems in [32, 35], respectively. Sub-sampling and a watermarking approach based on the DWT were presented by the authors in [30]. The strategy put forth in [30] is resistant to geometric distortions. Watermarks were embedded by Zhou et al. to the mid frequencies of the Fourier Mellin Transform (FMT) in order to minimise the geometric distortion brought on by legitimate printing and scanning procedures [60]. A color image watermarking scheme based on the deep fusion theory between spatial domain and LU factorization is proposed in [47]. DWT-based image watermarking methods are presented and evaluated for enhanced robustness and imperceptibility in [53].

Chaos system is a kind of cryptosystem that is frequently employed in image encryption due to its attributes, which include high sensitivity to initial conditions and parameters [58], ergodicity [50] , and pseudo-randomness [22]. The use of chaos theory and dynamical systems in cryptography systems has grown significantly in the last 20 years [3]. Further, because of the sensitivity to the initial conditions and control parameters, a chaotic system is the best option for achieving the confusion and diffusion attributes in cryptography. The progression of chaotic sequences is sensitive to even slight modifications in the initial conditions and control parameters. One-dimensional (1D) and high-dimensional (HD) chaotic maps are the two further categories into which these can be divided [57]. One dimensional chaotic maps have very few variables and parameters, and relatively simple phase space trajectories in comparison to hyperchaotic maps, or high-dimensional (HD) chaotic maps [36]. High-dimensional chaotic map exhibit superior chaotic performance and a more intricate structure [20]. Numerous chaos-based water marking techniques have been documented in the literature [15, 18, 21, 24–26, 41, 51, 56]. Hénon maps, logistic maps, Arnold maps, Lorenz equations, skew tent maps, standard maps, and Baker map are the most widely used chaotic maps in the field of digital image watermarking. Dawei et al. converted the image into the frequency domain in order to create a chaos-based watermarking system for digital photos [15].

1.1 Motivations and proposed framework

Even though watermarking has been extensively researched for copyright protection, more research is still needed for its practical and real-world applications, particularly in online digital data privacy. For instance, YouTube is a public domain for video up-loaders and lacks the technical framework necessary to secure legitimate ownership. In the present article we have put up a uniform framework in our study to secure digital data ownership for digital images. An efficient and robust watermarking method by adding an extra layer of security in authentication with the help of encryption of watermark logo before embedding in this scheme. This extra layer of encryption of watermark logo prevents from the manipulation of the embedded data/watermark by the attackers. They can't to do so because of multiple secret keys are utilised during the encryption process. This is an integrated framework designed for protecting rightful property ownership. rest of the manuscript is divided as follows: fundamental theory behind the used maps is explained in Section 2. Demonstration for proposed algorithm including flowcharts (please refer to Figure 1 and Figure 2) of embedding and extraction of watermark is explained in Section 3. Result for all the security and statistical analysis and proposed algorithm's conclusion provided in Section 4 and Section 5, respectively.

2 Fundamental theory

2.1 Modified Hénon map (MHM)

Chaotic maps are the functions that depends on initial values and control parameters. For a specific set of system characteristics, these maps depict chaotic behaviour. Chaotic sequences that are generated undergo drastic changes even a single initial value or system parameter is changed. There are many chaotic functions in existence. Among them, one has a two-dimensionally modified Hénon map. In the proposed scheme, the initial conditions X_0 and Y_0 for the MHM are obtained by applying the SHA-256 hash function on the original host image. This map generates the two sequences $< X_n >$ and $< Y_n >$ having values lies in the interval $(0, 1)$. Mathematically, it is represented as:

$$X_{i+1} = 1 - u \times \cos(x_i) - v \times Y_i, \tag{2.1}$$

$$Y_{i+1} = -X_i, \tag{2.2}$$

where u and v are the secret key parameters and used as encryption keys. The bounded solutions for the modified Hénon map will be obtained for all values of u and $|v| < 1$. In particular, one can obtain an extensive chaotic range by selecting system parameter v = 0.3 for the MHM.

2.2 The sine map

The sine map is also a member of chaotic systems and non-linear dynamics [59]. Because of erratic behaviour and sensitivity to initial conditions, the chaotic sine map is frequently utilized in the domains of cryptography, secure communications, and image processing for purposes like watermarking and encryption. Mathematically, the sine map is expressed as:

$$Y_{n+1} = \beta * sin(\pi * Y_n), \tag{2.3}$$

where the initial condition $Y_n \in [0, 1]$, and the control parameter β satisfying the condition β > 0. Further, the sine map peak level of chaotic behaviour whenever β gets closer to 1. The advantage of the sine map, compared to certain other chaotic systems is that it is provides a higher degree of randomness and sensitivity.

3 The proposed technique's algorithm

The proposed scheme presents an efficient and robust blind watermarking by adding an extra layer of encryption to the watermark logo image. The whole process is carried out through two stages: a stage of watermark encryption by employing the modified Hénon map and the sine map and a stage of embedding the obtained ciphered watermark to the host image by utilizing the lifting wavelet transformation (LWT). Confusion and diffusion are well mentioned during the encryption of the watermark logo. Confusion among the pixel values is performed by the chaotic sequence generated from the sine map, whereas the chaotic sequence obtained from the modified Hénon map is utilized for the purpose of diffusion. Further, the modified Hénon map is also utilized to confuse the frequency elements in the bends during the embedding process to enhance the robustness and impressibility. The proposed scheme's algorithm is picturized in the Figure 1 and the detailed steps of the proposed scheme are as follows:

Step 1: Apply SHA-256 hash function to the host image P for generating the initial conditions X_0 and Y_0 utilized in the modified Hénon map.

$$H_{bits} = SHA - 256(P).$$

Produces an 64 digits hexadecimal (or binary number of 256 bit) message digest H_{bits}.

Step 2: to obtain two initial conditions, take first 128 bits out of 256 bits and convert them into a decimal number $H1_{(decimal)}$. Similarly, take the last 128 bits and convert them to another decimal number $H2_{(decimal)}$

$$H1_{(decimal)} = bi2dec(H(1 : 128)),$$

$$H2_{(decimal)} = bi2dec(H(129 : 256)).$$

Step 3: Divide decimal hash value $H1_{(decimal)}$ and $H2_{(decimal)}$ by 10^{39} to get the initial values X_0 and Y_0 in the range of $[0, 1]$, respectively

$$X_0 = \frac{H1_{(decimal)}}{10^{39}},$$

$$Y_0 = \frac{H2_{(decimal)}}{10^{39}}.$$

Step 4: Apply the modify Hénon map (please refer to Section 2.1) by considering the above generated initial conditions X_0 and Y_0 to obtain chaotic sequences $< X_n >$ and $< Y_n >$, respectively.

Step 5: Multiply the sequences $< X_n >$ and $< Y_n >$ by 10^{14} and apply the modulo 256 operation to obtain sequences $< K1 >$ and $< K2 >$ having values from 0 to 255.

Step 6: Apply the bitwise XOR in the corresponding entries of $K1$ and $K2$, resulting it will produces sequence $< K3 >$.

Step 7: Generate a square matrix $K4$ of size same as that of watermark image by reshaping the sequence $< K3 >$.

Step 8: Sorting the elements of the sequence $< X_n >$ that creates the index sequences $< I1 >$

$$< I1 >= index(SORT(< X_n >)).$$

Step 9: Apply hash function ($SHA-256$) to the watermark image W to obtain the initial condition S_0 in the range $[0, 1]$ for the sine map.

Step 10: Generate the chaotic sequence $< S_m >$ by employing the sine map (please refer to Section 2.2).

Step 11: Create the index sequence $< I2 >$ by sorting the sequence $< S_m >$

$$< I2 >= index(SORT(< S_m >)).$$

Step 12: Extract the coloured component images P_r, P_g & P_b from the original host image P, and component images W_r, W_g & W_b from the watermark image, respectively.

Step 13: Consider the red component images P_r and W_r.

Encryption of watermark

Step 14: Take the bitwise XOR among the entries of the square matrix $K3$ (obtained in Step 6) with the corresponding pixels of the watermark component image W_r. That produces the partial ciphered watermark W_{r1}

$$W_{r1} = bitXOR(W_r, K3).$$

Step 15: Confuses the entries of the partial ciphered watermark W_{r1} with the help of the index sequence $I2$, which will give the final encrypted watermark image W_{r2}

$$W_{r2} = W_{r2}(I2).$$

Embedding of cipher watermark

Step 16: Apply the LWT to the component host image P_r, which will produces four frequency subbands, viz. LL, LH, HL, and HH.

$$[LL, LH, HL, HH] = lwt2(P_r).$$

Step 17: Confuse the entries inside LH, HL, and HH bands with the help of the index sequence $< I1 >$ obtained by the modified Hénon map (please refer to Step 8). This step produces modified sub-bends LH1, HL1, and HH1

$$LH1 = LH(I1),$$

$$HL1 = HL(I1),$$

$$HH1 = HH(I1).$$

Step 18: Obtain eight bits for each pixel values of encrypted watermark image by converting them from decimal to binary numbers

$$[b_8 b_7 b_6 b_5 b_4 b_3 b_2 b_1] = dec2bin(W_{r2}).$$

Step 19: Now embed last four bits $b_4,\ b_3,\ b_2$ & b_1 inside the HH1 band, two bits b_6 & b_5 in the HL1 band and two bits b_8 & b_7 in the LH1 band, respectively. This step of embedding obtain the modified bends LH2, HL2, and HH2.

Step 20: Apply the inverse confusion in modified sub-bends LH2, HL2, and HH2 by using index sequence $< I1 >$, that followed by the inverse lifting wavelet transformation $(iLWT)$ to get the final watermarked component image P_{r1}

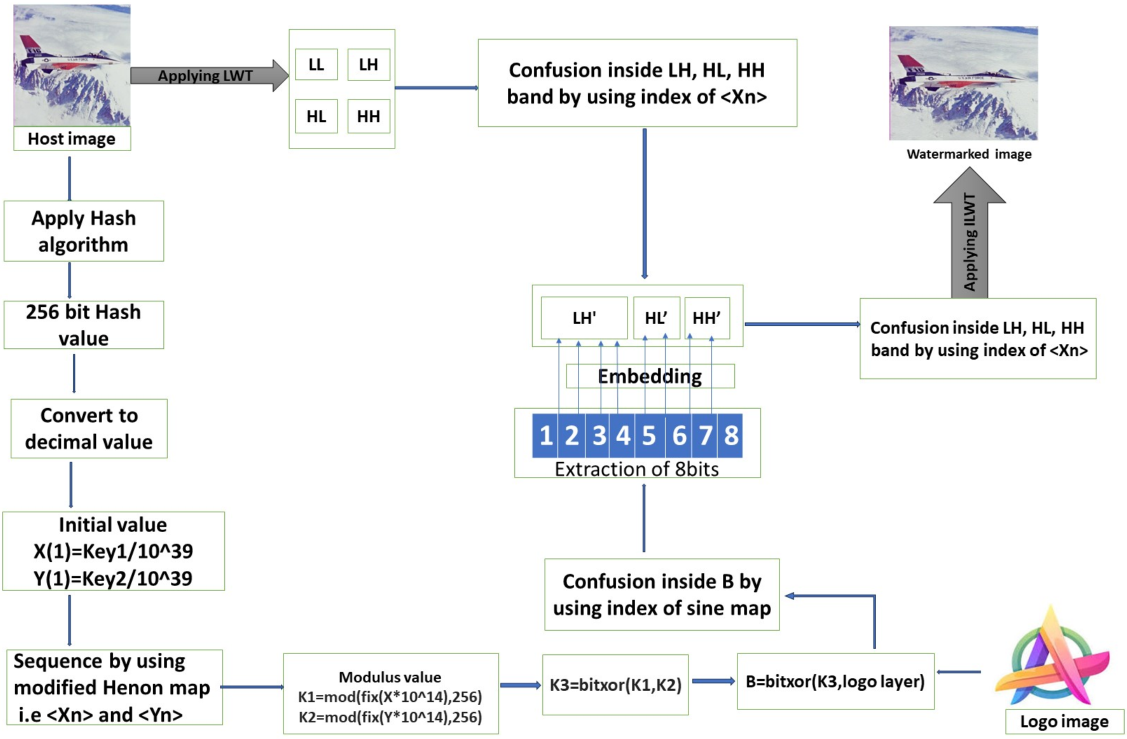
$$P_{r1} = ilwt2([LL, LH2, HL2, HH2]).$$

Concatenating the results

Step 21: Obtain watermarked component images P_{g1} and P_{b1} by repeating the Step 14 to Step 20 for green and blue channels, respectively.

Step 22: Concatenate the output images produces in Step 20 and Step 21 to obtain final coloured watermarked image D_{rgb}

$$D_{rgb} = cat(3, P_{r1}, P_{g1}, P_{b1}).$$



Host image
Applying LWT
LL
LH
HL
HH
Confusion inside LH, HL, HH band by using index of <Xn>
Watermarked image
Applying ILWT
Apply Hash algorithm
256 bit Hash value
Convert to decimal value
Initial value X(1)=Key1/10^39 Y(1)=Key2/10^39
LH'
HL'
HH'
Confusion inside LH, HL, HH band by using index of <Xn>
Embedding
1 2 3 4 5 6 7 8
Extraction of 8bits
Confusion inside B by using index of sine map
Sequence by using modified Henon map i.e <Xn> and <Yn>
Modulus value K1=mod(fix(X*10^14),256) K2=mod(fix(Y*10^14),256)
K3=bitxor(K1,K2)
B=bitxor(K3,logo layer)
Logo image

Figure 1: The flowchart for the proposed encryption and watermarking process.

3.1 The proposed technique for the decryption and extraction of watermark logo

All the above steps are applied inversely to verify the authenticity and integrity of the host image data by getting the watermark logo image back from the watermarked image. The flowchart of extraction of the deciphered logo image is illustrated in Figure 2 and step by step algorithm provided below:

Step1: Apply component-wise LWT on watermarked image D_{rgb}.

Step2: Confuse the entries inside the frequency bands obtained in previous step by the index sequence $< I1 >$.

Step3: Now, extract all eight embedded bits from the LSBs of modified sub-bands.

Step4: Compile all eight bits to produce the ciphered watermark logo image followed by the confuse using the index sequence $< I2 >$ of the sine map.

Step5: Apply the inverse diffusion by taking bitwise XOR with square matrix $K3$.

Finally, we will get final extracted watermark image or logo image and this extracted watermark image is utilizes to verify the integrity and authenticity of image data.

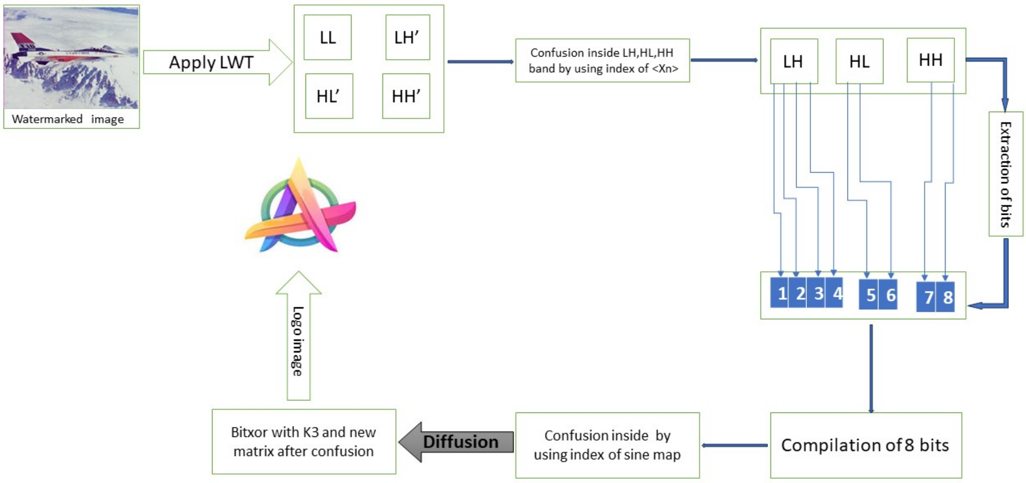

Watermarked image
Apply LWT
LL
LH'
HL'
HH'
Confusion inside LH,HL,HH band by using index of <Xn>
LH
HL
HH
Extraction of bits
1 2 3 4 5 6 7 8
Logo image
Compilation of 8 bits
Confusion inside by using index of sine map
Diffusion
Bitxor with K3 and new matrix after confusion

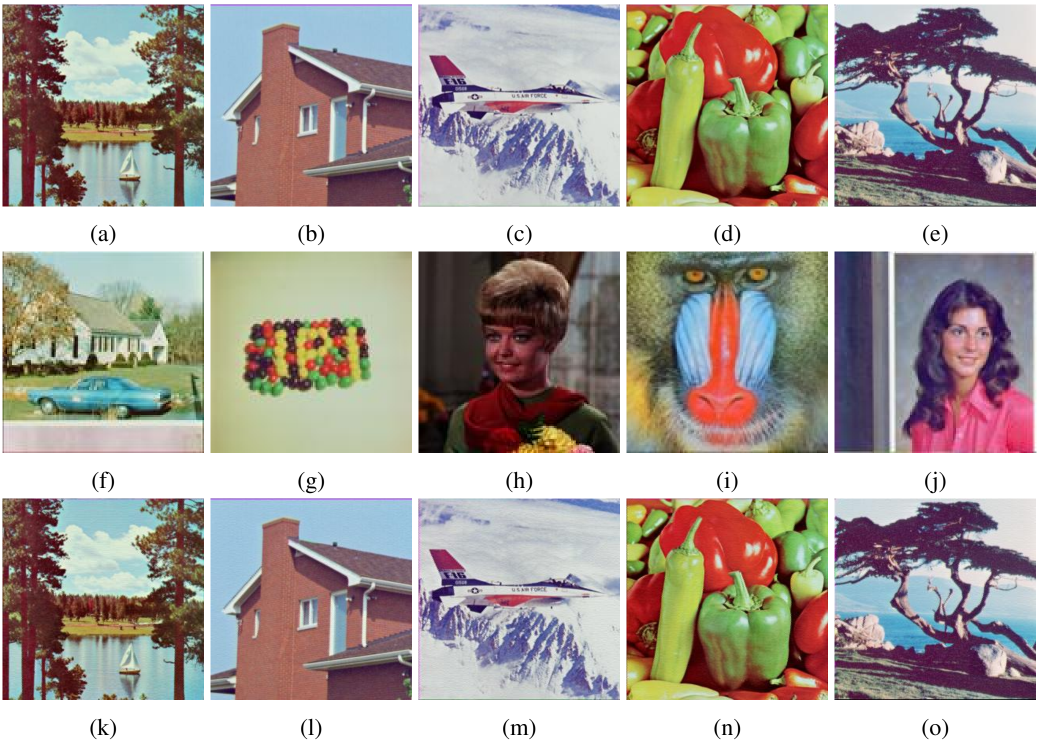
Figure 2: The flowchart of the decryption and extraction process.

4 Evaluation and simulation of results

For the verification of robustness of the proposed watermarking technique, test images of nature, house, aeroplane, peppers and tree are utilized as host images chosen from the image data base https://database.usc.edu/sipi.usc.edu.php. Whereas, the images of car, marbles, lady, baboon and a another lady chooses from the same database and used for the purpose of watermark logo. The proposed algorithm's resultant images are provided in Figure 3. Images in the top row represents the original host images, middle row's images represents watermark logo images and corresponding watermarked images obtained using proposed algorithm are presented in the last row. A system model HP laptop $15s - fq5007tu$ with a $12th$ generation $Intel(R)\ Core(TM)\ i3 - 1215U$, $1200MHz$, $6cores$, and 8 logical processors is used to evaluate the suggested watermarking approach. All the experiments have been implemented in the mathematical software $MATLAB$ $2023b$. To demonstrate the effectiveness and resilience of the suggested watermarking technique, the following tests are carried out: the structure similarity index (SSI), structure dissimilarity index (SDI), structure content (SC), energy, entropy, correlation, histogram tests, cropping and noise attack analysis. This section provides the detailed analysis of the results for the statistical and security analysis for the proposed scheme.

4.1 Structure similarity index

The structural similarity index (SSI), also called as SSIM, is a metric used in the digital image processing, that assesses the similarity between two images. Luminance, contrast, and structure are three components of image quality that are considered at the time of SSI calculation. The SSI aims to replicate how the human visual system perceives image's quality [34]. A pixel


(a) (b) (c) (d) (e)

(f) (g) (h) (i) (j)

(k) (l) (m) (n) (o)

Figure 3: Resultant images: images of the first row shows the original host images, second row shows to the watermark images and third row represents corresponding watermarked images.

interdependency relationship is shown by the SSI and mathematically, it is calculated as follows:

$$SSI(W,O) = \frac{(2\mu_W \mu_O + C_1)(\sigma_{WO} + C_2)}{(\mu_W^2 + \mu_O^2 + C_1)(\sigma_W^2 + \sigma_O^2 + C_2)}, \tag{4.1}$$

where W and O stand for the watermarked and original images, respectively. The average values of W and O are determined by the variables μ_W and μ_O, respectively. The variance of W and O are denoted by the parameters σ_W and σ_O, respectively. The covariance of pictures W and O is similarly measured by the parameter σ_{WO}. Further, $L = 2^{\#bitperpixel-1}$, $K1 = 0.01$, and $K2 = 0.03$ are used to stabilise the division with weak denominator using the parameters $C_1 = (k1L)^2$ and $C_2 = (K2L)^2$. If two images are identical, the corresponding result of SSI is 1; if not, it varies between 0 to 1. Table 1 explain structure similarity index values for the watermarked images in context to plain test host images, which illustrate that SSI values are nearly equal to 1 and hence the watermark logo is embedded efficiently by maintaining the same structure in the host image.

Watermarked image	Structure similarity
Nature	0.9779
House	0.9038
Aeroplane	0.9602
Pepper	0.9508
Tree	0.9804

Table 1: Structure similarity of watermarked images in context to the host images

4.2 Structure dissimilarity index (SDI)

The dissimilarity index in the image processing is a metric that expresses how mathematically different or dissimilar two images are from one another [2]. It is frequently used for tasks including image retrieval, picture registration, and image quality evaluation. It compares the contents of two images. Various techniques can be used to compute the dissimilarity index, depending on the particular application and the type of photos being compared. Generally, for a watermarking scheme the SDI metric is used to calculate measures the dissimilarities between two images, i.e., the host and corresponding watermarked images. Mathematically, it is calculated as follows:

$$SDI(W,O) = \frac{1 - SSI}{2}, \tag{4.2}$$

where W is obtained watermarked image corresponding to host image O, and SSI is structural similarity index (please refer to Equation (11)). The proposed watermarking approach has a modest SDI values (almost equal to zero) provided in Table 2, indicating that the watermarked images having very low dissimilarity to the corresponding original images. Hence, proposed scheme is efficient and robust as it is efficiently embeds the digital watermark.

Watermarked image	SDI values
Nature	0.0140
House	0.0481
Aeroplane	0.0199
Pepper	0.0154
Tree	0.0132

Table 2: Structure dissimilarity analysis of watermarked image

4.3 Structure content (SC)

In the field of image processing the spatial arrangement, patterns, and textures present in a given image are referred to as the image's structural content [5]. It explains how the image's pixel intensities are arranged and relate to one another. For activities like image analysis, feature extraction, and image enhancement, it is essential to comprehend the structure content of an image. Pixel intensities are arranged spatially to create patterns and textures frequently seen in images. The SC calculated for the host and corresponding watermarked image to determine the efficiency of a watermarking scheme. It can be defined mathematically as the ratio of the watermarked image's and the host image's structural information contents, and it is calculated as follows:

$$SC = \frac{\sum_{i=1}^{a} \sum_{j=1}^{b} [O(i,j)]^2}{\sum_{i=1}^{a} \sum_{j=1}^{b} [W(i,j)]^2}, \tag{4.3}$$

where $O(i,j)$ and $W(i,j)$ denotes the pixel value at the (i,j) co-ordinate position, while a and b tells the number of rows and number of columns, respectively. Table 3 has structure content value of watermarked images with reference to corresponding original host images for the proposed scheme which are nearly equal to 1. That assured the robustness of proposed scheme, and watermark logo is embedded without any disturbance in structure of the host image.

Watermarked image	Structure content
Nature	1.002
House	1.001
Aeroplane	1.003
Pepper	1.005
Tree	1.004

Table 3: Structure content analysis for watermarked image

4.4 Energy

When discussing image processing, energy is usually referred to the overall quantity of intensity variation found in a digital image [17]. It is a gauge of the overall contrast or intricacy of the picture. The energy is frequently calculated using the image's pixel intensities as a base. Image processing operations like feature extraction, compression, and enhancement can all benefit from an image's energy and it utilized to compare two images as well. Low-energy in a image implies more homogeneous or smooth, but high-energy in images typically have distinct features and contrast. Mathematically, the energy of an image is determined as follows:

$$E1 = \sum(E(i,j)^2), \tag{4.4}$$

where E(i, j) is the pixel value at position (i, j). Low energy means that the entries in the gray level co-occurrence matrix (GLCM) are almost equal, while higher energy means that some entries in the GLCM have higher magnitude. For the proposed watermarking scheme the energy value for the original and corresponding watermarked images are calculated and presented in Table 4. This table shows that the energy values of the watermarked images are low as much as energy value of original images. Further, both the energy values (i.e. the energy of host and energy of corresponding watermarked image) are similar to each other, that indicates the efficient embedding approach of the watermark logo image without any major change in the intensities of the original image.

Images	Original			Watermarked		
	R	G	B	R	G	B
Nature	1.6800×10^{-5}	2.1049×10^{-5}	2.1899×10^{-5}	1.6838×10^{-5}	2.1073×10^{-5}	2.1925×10^{-5}
House	1.7494×10^{-5}	1.6971×10^{-5}	1.9311×10^{-5}	1.7495×10^{-5}	1.6988×10^{-5}	1.9314×10^{-5}
Aeroplane	1.6184×10^{-5}	1.6507×10^{-5}	1.5674×10^{-5}	1.6195×10^{-5}	1.6521×10^{-5}	1.5681×10^{-5}
Peppers	1.6606×10^{-5}	2.1576×10^{-5}	2.1807×10^{-5}	1.6620×10^{-5}	2.1561×10^{-5}	2.1823×10^{-5}
Tree	1.8112×10^{-5}	2.0986×10^{-5}	1.8233×10^{-5}	1.8122×10^{-5}	2.0997×10^{-5}	1.8235×10^{-5}

Table 4: Energy analysis of host and corresponding watermarked images.

4.5 Entropy

Entropy is a measurement used to express the presence of randomness among the pixel values in a digital image. It is used to calculate the degree of disorder or uncertainty in the pixel values of an image [44]. In image processing, entropy can be applied to several tasks, including segmentation and compression. Digital image's entropy is calculated by taking the summation of probabilities of all possible pixel values and the formula to evaluate it is provided as follows

$$H = \sum[p(x_i)log(\frac{1}{p(x_i)})], \tag{4.5}$$

where $p(x_i)$ is the probability of i^{th} pixel value. For an efficient watermarking scheme the entropy of the host image and corresponding watermarked image must have almost same values. Table 5 explains component wise (viz., R for red, G for green and B for blue) entropy value of original and corresponding watermarked images for the proposed watermarking technique. Slight difference in entropy values of original and corresponding watermarked images, shows the proposed watermarking scheme robustness, efficiency and almost same maintenances of pixel distribution during embedding.

Images	Host			Watermarked		
	R	G	B	R	G	B
Nature	7.2587	7.6143	7.1892	7.2982	7.6985	7.3584
House	7.6058	7.3581	7.6856	7.6274	7.3815	7.6665
Aeroplane	7.7254	7.8253	7.3768	7.8425	7.9636	7.2078
Peppers	7.3009	7.5570	7.0929	7.3465	7.6261	7.1719
Tree	7.3104	7.4136	7.9207	7.2910	7.5373	7.5098

Table 5: Entropy analysis of host and watermarked image

4.6 Correlation analysis

Correlation analysis is an examination of the link or a relation between the adjacent pixel values inside an image or between multiple images. This analysis is employed in the domains like computer vision, remote sensing, and image processing. The correlation coefficient determines the similarity between variables [11]. Correlation in three perspectives diagonal, vertical, and horizontal analysis.

Diagonal analysis: An image's diagonal correlation is a particular kind of correlation analysis that looks at the relationship between pixel values along the image's diagonal. It describes the analysis of diagonally oriented features or patterns in a picture.

Vertical analysis: In image processing, vertical correlation analysis looks at the relationship between pixel values in an image's vertical columns. Vertically oriented patterns, textures, or characteristics within the image can be identified through this analysis.

Horizontal analysis: In image processing, horizontal correlation analysis looks at the relationship between the pixel values in a picture's horizontal rows. Horizontal correlation analysis aims to find a correlation coefficient between the pixel values in an image's horizontal rows. Mathematically, correlation coefficient is calculated as follows:

$$CC = \frac{Cov(O,W)}{\sqrt{D(O)D(W)}}, \tag{4.6}$$

$$Cov(O,W) = E[O - E(O)] \times [W - E(W))],$$

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) stands for the covariance of the corresponding elements in the sequence of pixels O and W. From Table 6 it is observed that the correlation values for all the test images and corresponding watermarked images in all three directions (viz., diagonal, vertical and horizontal direction) are almost similar. Hence, correlation among adjacent pixel values is well maintained during the watermark embedding and proves the proposed algorithm's robustness and efficiency.

Images		Host			Watermarked		
		R	G	B	R	G	B
Nature	D	0.9274	0.9225	0.9369	0.9274	0.9191	0.9338
	V	0.9539	0.9527	0.9645	0.9539	0.9430	0.9561
	H	0.9563	0.9558	0.9603	0.9563	0.9498	0.9552
House	D	0.9034	0.7925	0.8763	0.9028	0.7935	0.8771
	V	0.9208	0.8380	0.9139	0.9171	0.8333	0.9083
	H	0.9474	0.8728	0.9216	0.8720	0.8720	0.9198
Aeroplane	D	0.8738	0.8814	0.8800	0.8638	0.8731	0.8615
	V	0.9239	0.9343	0.9089	0.9029	0.9121	0.8809
	H	0.9389	0.9309	0.9503	0.9283	0.9192	0.9383
Peppers	D	0.9369	0.9466	0.9369	0.9278	0.9426	0.9278
	V	0.9680	0.9570	0.9680	0.9510	0.9648	0.9510
	H	0.9558	0.9698	0.9646	0.9563	0.9637	0.9563
Tree	D	0.9451	0.8956	0.8754	0.9278	0.8845	0.8654
	V	0.9564	0.9421	0.8832	0.8712	0.8862	0.8845
	H	0.9523	0.9387	0.9578	0.9687	0.9754	0.9621

Table 6: Correlation analysis of host and watermarked image.

4.7 Histogram analysis

In digital image processing, histogram analysis involves examining the distribution of pixel intensities in an image. A histogram is a graphical representation of the frequency of occurrence of each intensity value in a given digital image. It helps to understand an image's overall brightness or color characteristics and it is a fundamental tool for various image-processing tasks [23]. Histogram analysis can provide valuable insights into an image, such as brightness distribution, contrast enhancement, thresholding, image equalization and noise Analysis. Overall, histogram analysis is a powerful tool in digital image processing that provides valuable information about the characteristics of an image and is used in a wide range of applications to enhance and analyze images. Figure 4 provide the proposed scheme's histogram analysis: images in second row are the histogram of corresponding test images provided in first row, fourth row's images are the histograms of the watermark images (provided in the second row), further histograms of corresponding watermarked images are presented in the last row. Presence of almost same peaks in the original host image's histogram and in the watermarked image's histogram, proves the efficiency and the robustness of the proposed watermarking scheme. Further, identical histograms of watermark and corresponding extracted watermark images (not shown here) shows the extraction process done without any data loss and verification of watermark process completed smoothly.

4.8 Classical attack analysis

Hackers exploit the weakness in the algorithm and try to retrieve the secret keys utilized in the given system by analysis for some given particular set, such as a set of known plaintext or a set of pairs of plaintext-ciphertext, etc. These types of activities are performed by hackers and are known as classical attacks. Dependency of the secret keys utilized in the proposed algorithm on the original host and watermark images due to the use of secure $SHA-256$ hash function during key generation, the output corresponded to the slight changes in input produces totally different output. Hence, hackers can not access the secret keys, and the proposed scheme is robust and efficiently defends against all types of classical attacks.

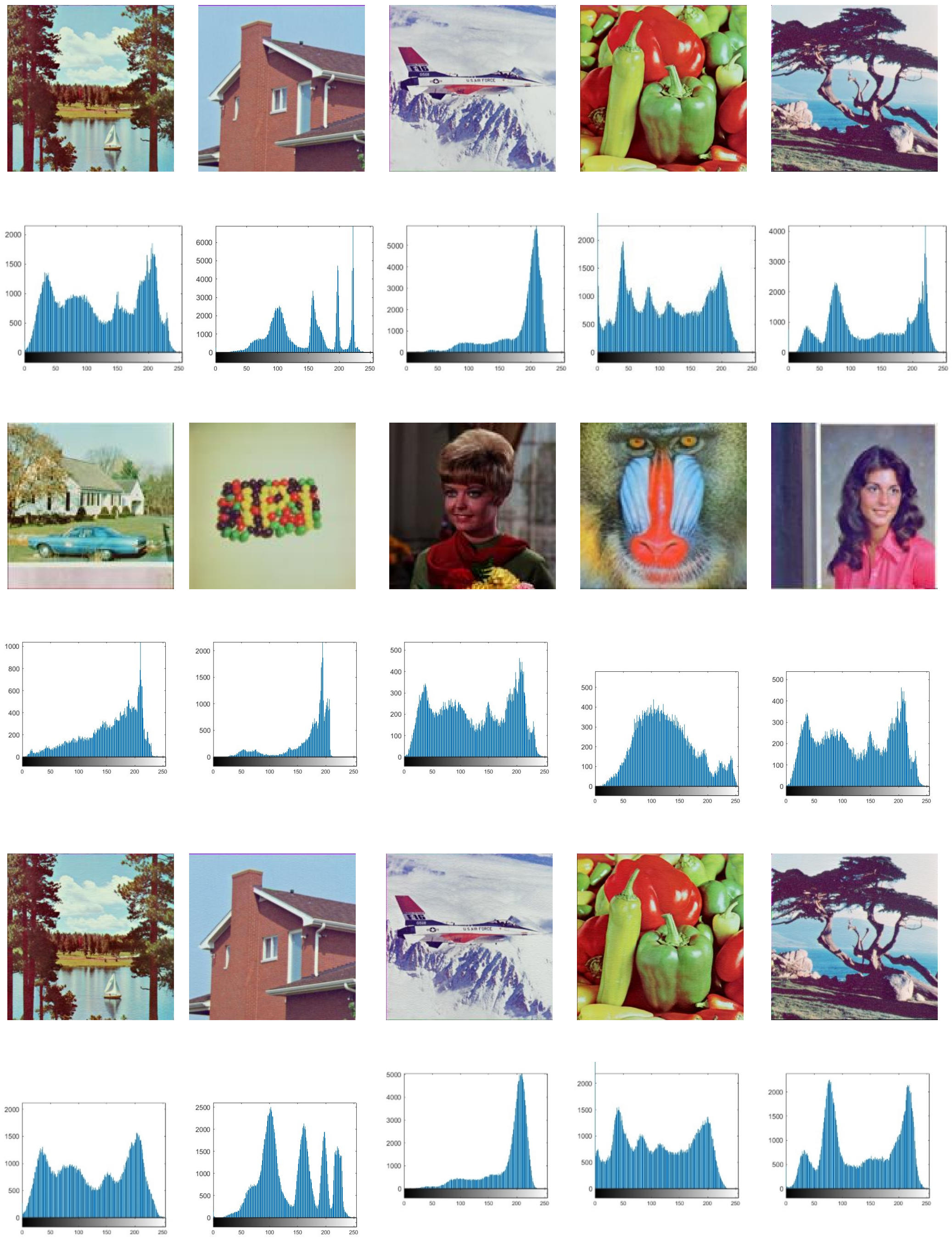
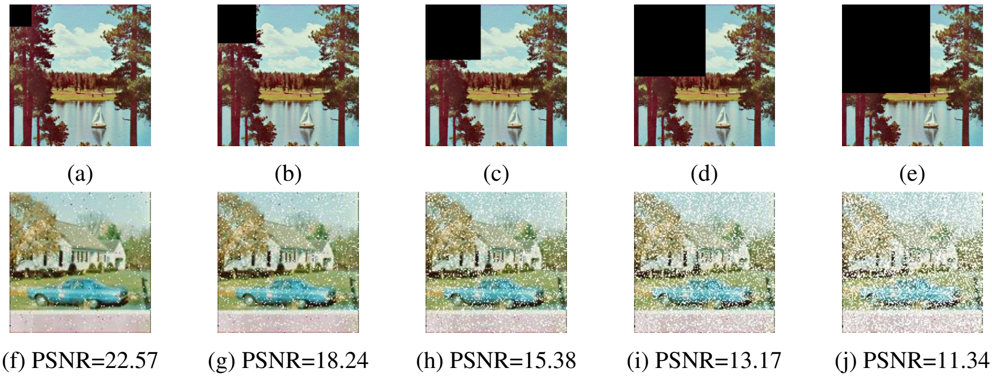


Figure 4: Histogram analysis: first row represents the original images & second row represents the corresponding histograms, third & forth represents the watermark images & their histograms, and last two rows represents the histograms of watermarked images.



(a) (b) (c) (d) (e)

(f) PSNR=22.57 (g) PSNR=18.24 (h) PSNR=15.38 (i) PSNR=13.17 (j) PSNR=11.34

Figure 5: Cropping attack analysis: Watermarked image of nature with (a) 2.44%, (b) 7.47%, (c) 15.25%, (d) 25.78% & (e) 39.06% of the crop, and images in second row are corresponding extracted images.

4.9 Cropping attack analysis

A cropping attack in image processing is a type of manipulation where a portion of an image is intentionally removed/cropped out or data loss during transmission over open networks [1]. Data manipulation can be done for various purposes, such as altering the context of the image, hiding certain details, or focusing attention on specific elements. A watermarking scheme is robust only if it is capable to efficiently extract and verifying the watermark even in case of cropped watermarked image. Now, to analyzing the proposed scheme's robustness, watermarked image of nature containing image of car as watermark is cropped by 2.44%, 7.47%, 15.25%, 25.78% & 39.02% and presented in the first row of Figure 5, and corresponding extracted logo images are provided in second row, respectively. All the extracted logos are visible by human eye shows the robustness. Further, for the quantitative analysis the calculated $PSNR$ between original and extracted logo images is calculated and provided in the corresponding caption of extracted images in Figure 5. All the $PSNR$ values are greater than 10.

4.10 Noise attack analysis

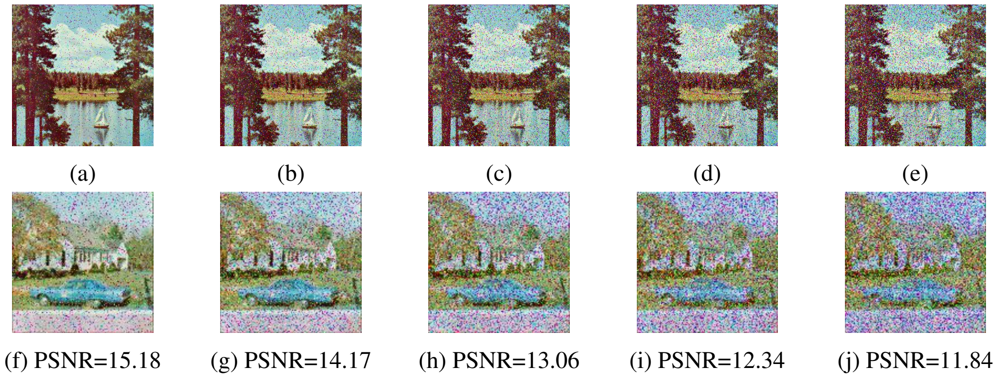
In image processing, a noise attack refers to the introduction of unwanted or random variations in the pixel values of a digital image during the transmission over open networks. This can degrade the quality of the image and make it harder to analyze or interpret [37]. Various factors, such as electronic interference in the image capture process, transmission errors in digital communication, and imperfections in the image sensor, can cause noise. There are several types of noise available in the domain of image processing including:

Gaussian noise: This type of noise follows a Gaussian (normal) distribution and is often used to simulate random variations in intensity levels [19].

Salt and pepper noise: This type of noise manifests as randomly occurring black and white pixels, resembling grains of salt and pepper sprinkled on the image [33].

Speckle noise: Speckle noise is caused by interference patterns and appears as grainy artefacts in the image.

A watermarking scheme is robust only if it is capable to efficiently extract and verifying the watermark even in presence of noise in the watermarked image. Now, to analyzing the proposed scheme's robustness, $salt$ & $pepper$ noise is added to the watermarked image of nature containing image of car as watermark with 4%, 8%, 12%, 16% & 20%, and are presented in the first row of Figure 6, and second row provides corresponding extracted logo images, respectively. Visibility of all the extracted logo images shows the efficiency and robustness of the proposed scheme in case of noise attack. Further, PSNR grater than 10 for all the extracted images (provided in the corresponding caption of extracted images in Figure 6), quantitatively verifies the the robustness.



(a) (b) (c) (d) (e)

(f) PSNR=15.18 (g) PSNR=14.17 (h) PSNR=13.06 (i) PSNR=12.34 (j) PSNR=11.84

Figure 6: Noise attack analysis: Watermarked image of nature containing (a) 4%, (b) 8%, (c) 12%, (d) 16%, & (e) 20% of $salt$ & $pepper$ noise, and images in second row are corresponding extracted images.

5 Conclusion

This paper proposes an efficient and robust watermarking method by adding an extra layer of security in authentication with the help of encryption of watermark logo before embedding. This encryption of watermark logo prevents from the manipulation of the embedded data by the attackers. They can't to do so because of multiple secret keys are utilised during the encryption process. Further, the proposed watermarking method uses the sine and modified Hénon map (2D-MHM) along with the bends obtained from the lifting wavelet transformation (LWT) for the purpose of encryption and embedding of watermark logo. The used 2D-MHM has more dynamic in nature and exhibits a wide range of chaotic behaviour for the system parameter than that of Hénon map. The confusion and diffusion among the pixel values of watermark logo image is significantly maintained. The 2D-MHM is used for diffusion, whereas the sine map is utilised for the confusion. Further, to enhance the randomness/blindness in watermarking, the chaotic sequence obtained from the same 2-D MHM will be utilised to permute the elements in the frequency bands before substituting the bits of ciphered watermark logo. The proposed scheme is significantly robust and capable to resist all types of statistical attacks including classical attacks. Results for all the included test highlights the proposed scheme's efficiency and robustness.

In the future, we will extend the proposed technique to multidimensional digital data, including digital videos and 3D images. This expansion aims to broaden the technique's applicability across diverse media formats.

Declarations

Conflict of interest/Competing interest All authors declare that they have no conflict of interest.

References

[1] Aggarwal, A. and Singla, M. (2011). Robust watermarking of color images under noise and cropping attacks in spatial domain. *image*, 6(9):11.

[2] Akl, A. and Yaacoub, C. (2019). Image analysis by structural dissimilarity estimation. In *2019 Ninth International Conference on Image Processing Theory, Tools and Applications (IPTA)*, pages 1–4. IEEE.

[3] Alvarez, G. and Li, S. (2009). Cryptanalyzing a nonlinear chaotic algorithm (nca) for image encryption. *Communications in Nonlinear Science and Numerical Simulation*, 14(11):3743–3749.

[4] Basha, S. A., & Khan, A. (2023). Image Thresholding Using Discrete Wavelet Transform with Retention of Possible Edge Contour. *Palestine Journal of Mathematics*, 12(3).

[5] Bell, P. (2012). Content analysis of visual images. *SAGE visual methods: Interpretation and classification*, 3:31–57.

[6] Chamlawi, R., Khan, A., and Usman, I. (2010). Authentication and recovery of images using multiple watermarks. *Computers & Electrical Engineering*, 36(3):578–584.

[7] Chandrakar, N., Bagga, J., et al. (2013). Performance comparison of digital image watermarking techniques: a survey. *International Journal of Computer Applications Technology and Research*, 2(2):126–130.

[8] Chang, C.-C., Tsai, P., and Lin, C.-C. (2005). Svd-based digital image watermarking scheme. *Pattern Recognition Letters*, 26(10):1577–1586.

[9] Chau, L.-P. and Siu, W.-C. (2003). Efficient multiplier structure for realization of the discrete cosine transform. *Signal Processing: Image Communication*, 18(7):527–536.

[10] Chen, L., Chen, J., Zhao, G., and Wang, S. (2019). Cryptanalysis and improvement of a chaos-based watermarking scheme. *IEEE Access*, 7:97549–97565.

[11] Chu, T., Ranson, W., and Sutton, M. A. (1985). Applications of digital-image-correlation techniques to experimental mechanics. *Experimental mechanics*, 25:232–244.

[12] Chu, W. C. (2003). Dct-based image watermarking using subsampling. *IEEE transactions on multimedia*, 5(1):34–38.

[13] Cox, I. J., Kilian, J., Leighton, F. T., and Shamoon, T. (1997). Secure spread spectrum watermarking for multimedia. *IEEE transactions on image processing*, 6(12):1673–1687.

[14] Das, C., Panigrahi, S., Sharma, V. K., and 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.

[15] Dawei, Z., Guanrong, C., and Wenbo, L. (2004). A chaos-based robust wavelet-domain watermarking algorithm. *Chaos, Solitons & Fractals*, 22(1):47–54.

[16] Dixit, A. and Dixit, R. (2017). A review on digital image watermarking techniques. *International Journal of Image, Graphics and Signal Processing*, 9(4):56.

[17] Dua, S., Acharya, U. R., Chowriappa, P., and Sree, S. V. (2011). Wavelet-based energy features for glaucomatous image classification. *Ieee transactions on information technology in biomedicine*, 16(1):80–87.

[18] Fan, M. and Wang, H. (2009). Chaos-based discrete fractional sine transform domain audio watermarking scheme. *Computers & Electrical Engineering*, 35(3):506–516.

[19] Fan, W., Sun, G., Su, Y., Liu, Z., and Lu, X. (2019). Integration of statistical detector and gaussian noise injection detector for adversarial example detection in deep neural networks. *Multimedia Tools and Applications*, 78:20409–20429.

[20] Gao, X. (2021). Image encryption algorithm based on 2d hyperchaotic map. *Optics & Laser Technology*, 142:107252.

[21] Ghebleh, M., Kanso, A., and Own, H. S. (2014). A blind chaos-based watermarking technique. *Security and Communication Networks*, 7(4):800–811.

[22] Hilborn, R. C. (2000). *Chaos and nonlinear dynamics: an introduction for scientists and engineers*. Oxford university press.

[23] Holub, O. and Ferreira, S. T. (2006). Quantitative histogram analysis of images. *Computer physics communications*, 175(9):620–623.

[24] Jamal, S. S., Khan, M. U., and Shah, T. (2016). A watermarking technique with chaotic fractional s-box transformation. *Wireless Personal Communications*, 90:2033–2049.

[25] Khan, M. and Shah, T. (2015). A copyright protection using watermarking scheme based on nonlinear permutation and its quality metrics. *Neural Computing and Applications*, 26:845–855.

[26] Khan, M., Shah, T., and Batool, S. I. (2017). A new approach for image encryption and watermarking based on substitution box over the classes of chain rings. *Multimedia Tools and Applications*, 76:24027–24062.

[27] Lian, S., Chen, X., and Wang, J. (2012). Content distribution and copyright authentication based on combined indexing and watermarking. *Multimedia Tools and Applications*, 57:49–66.

[28] Liang, J. and Tran, T. D. (2001). Fast multiplierless approximations of the dct with the lifting scheme. *IEEE transactions on signal processing*, 49(12):3032–3044.

[29] Lin, S. D. and Chen, C.-F. (2000). A robust dct-based watermarking for copyright protection. *IEEE Transactions on Consumer Electronics*, 46(3):415–421.

[30] Lu, W., Sun, W., and Lu, H. (2012). Novel robust image watermarking based on subsampling and dwt. *Multimedia tools and applications*, 60(1):31–46.

[31] Lu, Z.-M., Zheng, H.-Y., and Huang, J.-W. (2007). A digital watermarking scheme based on dct and svd. In *Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 2007)*, volume 1, pages 241–244. IEEE.

[32] Moulin, P. and Mihcak, M. K. (2002). A framework for evaluating the data-hiding capacity of image sources. *IEEE Transactions on Image Processing*, 11(9):1029–1042.

[33] Mousavi, S. M., Naghsh, A., Manaf, A. A., and Abu-Bakar, S. (2017). A robust medical image watermarking against salt and pepper noise for brain mri images. *Multimedia Tools and Applications*, 76:10313–10342.

[34] Mudeng, V., Kim, M., and Choe, S.-w. (2022). Prospects of structural similarity index for medical image analysis. *Applied Sciences*, 12(8):3754.

[35] Mukherjee, D. P., Maitra, S., and Acton, S. T. (2004). Spatial domain digital watermarking of multimedia objects for buyer authentication. *IEEE Transactions on multimedia*, 6(1):1–15.

[36] Natiq, H., Al-Saidi, N., Said, M., and Kilicman, A. (2018). A new hyperchaotic map and its application for image encryption. *The European Physical Journal Plus*, 133:1–14.

[37] Nguyen, H. P., Delahaies, A., Retraint, F., and Morain-Nicolier, F. (2019). Face presentation attack detection based on a statistical model of image noise. *IEEE Access*, 7:175429–175442.

[38] Nikolaidis, N. and Pitas, I. (1998). Robust image watermarking in the spatial domain. *Signal processing*, 66(3):385–403.

[39] Nikolaidis, N. and Pitas, I. (1999). Digital image watermarking: an overview. In *Proceedings IEEE International Conference on Multimedia Computing and Systems*, volume 1, pages 1–6. IEEE.

[40] Rao, K. R. and Yip, P. (2014). *Discrete cosine transform: algorithms, advantages, applications*. Academic press.

[41] Rawat, S. and 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.

[42] Seo, J. S. and Yoo, C. D. (2006). Image watermarking based on invariant regions of scale-space representation. *IEEE Transactions on Signal Processing*, 54(4):1537–1549.

[43] Shih, F. Y. and Wu, S. Y. (2003). Combinational image watermarking in the spatial and frequency domains. *Pattern Recognition*, 36(4):969–975.

[44] Silva, L. E., Duque, J. J., Felipe, J. C., Murta Jr, L. O., and Humeau-Heurtier, A. (2018). Two-dimensional multiscale entropy analysis: Applications to image texture evaluation. *Signal Processing*, 147:224–232.

[45] Singh, D., Patel, M. K., Mukesh (2025). COLOR IMAGE ENCRYPTION SCHEME BASED ON RC4A AND CHAOTIC MAPS. *Palestine Journal of Mathematics*, 14(1).

[46] Singhal, N., Lee, Y.-Y., Kim, C.-S., and Lee, S.-U. (2009). Robust image watermarking using local zernike moments. *Journal of Visual Communication and Image Representation*, 20(6):408–419.

[47] Su, Q., Sun, Y., Xia, Y., & Wang, Z. (2024). A robust color image watermarking scheme in the fusion domain based on LU factorization. *Optics & Laser Technology*, 174, 110726.

[48] Thakur, S., Singh, A. K., Ghrera, S. P., and 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.

[49] Thakur, S., Singh, A. K., Ghrera, S. P., and Mohan, A. (2020). Chaotic based secure watermarking approach for medical images. *Multimedia Tools and Applications*, 79(7):4263–4276.

[50] Thompson, J. M. T. and Stewart, H. B. (2002). *Nonlinear dynamics and chaos*. John Wiley & Sons.

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

[52] Vahedi, E., Zoroofi, R. A., and 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.

[53] Venkatesha, G. G., Kansal, S., Ilamurugan, P. K., Kumar, K., Marella, V., & Khan, S. (2024). Blind Image Watermarking Scheme Utilizing 3-Level Discrete Wavelet Transform (DWT) for Enhanced Security. *In 2024 13th International Conference on System Modeling & Advancement in Research Trends (SMART)* pages 151-155. IEEE.

[54] Vetterli, M. and Kovacevic, J. (1995). *Wavelets and subband coding*. Prentice-hall.

[55] Wong, P. W. (1998). A public key watermark for image verification and authentication. In *Proceedings 1998 international conference on image processing. ICIP98 (Cat. No. 98CB36269)*, volume 1, pages 455–459. IEEE.

[56] Wu, X. and Guan, Z.-H. (2007). A novel digital watermark algorithm based on chaotic maps. *Physics Letters A*, 365(5-6):403–406.

[57] Wu, X., Hu, H., and Zhang, B. (2004). Parameter estimation only from the symbolic sequences generated by chaos system. *Chaos, Solitons & Fractals*, 22(2):359–366.

[58] Xiaofu, W., Songgeng, S., et al. (1999). A general efficient method for chaotic signal estimation. *IEEE Transactions on signal processing*, 47(5):1424–1428.

[59] Yosefnezhad Irani, B., Ayubi, P., Amani Jabalkandi, F., Yousefi Valandar, M., & Jafari Barani, M. (2019). Digital image scrambling based on a new one-dimensional coupled Sine map. *Nonlinear Dynamics*, 97(4), 2693-2721.

[60] Zhou, J. and Pang, M. (2010). Digital watermark for printed materials. In *2010 2nd IEEE InternationalConference on Network Infrastructure and Digital Content*, pages 758–762. IEEE.

Author information

D. Singh, (Deep Singh) School of Undergraduate Studies, Dr. B. R. Ambedkar University Delhi, Delhi 110006, and Department of Mathematics and Statistics, Central University of Punjab, Bathinda, 151401, India.
E-mail: deepsinghspn@gmail.com

M. K. Patel, (Manoj Kumar Patel) Department of Mathematics, National Institute of Technology, Nagaland, India.
E-mail: mkpitb@gmail.com

L. Chandra, (Lal Chandra) Department of Mathematics and Statistics, Central University of Punjab, Bathinda, 151401, India.
E-mail: chandra18cutn@gmail.com

H. Sharma, (Harshit Sharma) Department of Mathematics and Statistics, Central University of Punjab, Bathinda, 151401, India.
E-mail: harshit220596@gmail.com

S. Kumar, (Sandeep Kumar) Department of Mathematics and Statistics, Central University of Punjab, Bathinda, 151401, India.
E-mail: sandeepkumarsvr@gmail.com, Corresponding Author

Received: 2024-11-01
Accepted: 2025-06-26