Enhancing Image Security: A Hybrid Encryption Approach Incorporating Bogdanov and Duffing Maps with DWT

Ramakant Parida[1, 2*], Binod Kumar Singh[1], Chittaranjan Pradhan[2]

[1] *Department of Computer Science and Engineering, NIT Jamshedpur, 831014, Jharkhand, India*

[2] *Kalinga Institute of Industrial Technology, Bhubaneswar, 751024, Odisha, India*

Abstract: **-** In this study, a novel and robust double image encryption method is introduced by combining the Bogdanov map and the Duffing map chaotic algorithms for image encryption, ensuring both copyright protection and image integrity. This approach also incorporates image watermarking techniques using two distinct images, a message image and a cover image of varying sizes. The message image is initially encrypted using a double encryption method, and at the receiver's end, double decryption is applied to recover the original message while removing the watermarking component. By leveraging a discrete wavelet transform (DWT), the message image is merged with the cover image to create a watermark image, enhancing security and unpredictability through the utilization of multiple key values.This method also effectively deters potential attackers from recognizing the presence of a message image within a cover image, as it exhibits both a high correlation and entropy value. To assess the image encryption's effectiveness, various metrics, including NPCR, UACI, MSE, PSNR, entropy, and correlation coefficient, are employed to measure subtle pixel changes.

Keywords: *double encryption, decryption, watermarking, cover image, message image.*

1. Introduction

The development of new gadgets and the transformation in communication technology are the driving forces of the modern world. In a situation where ordinary communication is buried under a flood of data traffic and used by handheld embedded devices, data protection is obviously essential. New techniques, while providing safe transmission over open networks, must overcome challenging barriers against malware, Trojans, and persistent hacking attempts. Many strategies have been created and put into use to improve computer security to fight these vulnerabilities. The mainstays of information security are cryptography, steganography, and watermarking, which all significantly contribute to the secure transmission of data. Many industries, such as the military, navy, space programme, and news transmission, value image encryption. Increasing the qualities of records authentication, integrity, non-repudiation, and harmful attack resistance requires the use of image encryption. Image encryption is used to transmit digital photos securely in a variety of formats including .bmp, .tiff, .png, .jpeg etc. The two techniques that are most typically employed while encrypting these images are confusion and diffusion. Diffusion and confusion alter the pixel values and positions, respectively to making detection challenging [1, 2]. The Arnold cat map is one of the widely utilised techniques for producing efficient pixel scrambling chaotic map technique used for image encryption [3, 4]. Watermarking is a crucial step in providing authenticated access to digital images. In the most recent designs proposed by various academics, watermarks of both the visible and invisible varieties are used. Many watermarking methods, such as fragile watermarking, least-significant bit substitution, pixel alteration, and bit shifting, are built on the foundation of spatial-domain embedding. By dividing the bigger digital image into the Region of Interest (ROI) and the Region of Non-Interest (RONI), watermarking can be done successfully in the spatial domain. These methods, however, do not provide much defence against attacks involving image processing, such as rotation, shifting, or scaling. In contrast, attacks are defended against via transform domain approaches to picture compression and filtering [5].

Using watermarking techniques, a watermark is injected into high-frequency components to increase the robustness and imperceptibility [6]. One of the crucial transformations used in encryption and compression techniques is the discrete cosine transform (DCT). Discrete Wavelet Transform (DWT) and DCT were combined to present a digital watermarking technology for

Improved authentication proposed by Zhu et al. [7]. A window function with adjustable size is needed to evaluate the image's finer elements. DWT is therefore included in a number of picture encryption and authentication techniques [8, 9]. Wavelets have been employed by Ibrahim et al. to isolate the smooth pixels in photographs and place the watermark in them [10]. Cetinel and Cerkezi [11] proposed a better watermarking method based on DWT and singular value decomposition to reduce the size of the watermark and generate low Mean Square Errors (MSEs). A novel multiple watermarking techniques for photograph were proposed by Liu et al. to improve ownership authentication. Their strategy gives demonstrable defence against local attacks on image [12]. Another strategy uses DNA-based dispersion and chaos-based confusion [13]. To shuffle, scramble, and authenticate the DICOM picture in a different way, a trilayer cryptic system built on the Latin square image cypher, the Rubik's cube, and the discrete Gould transform has been designed [14]. This three-layer cryptic method provides demonstrable defence against brute-force and tamper-proofing attacks. Furthermore, Hu and Han's method for encryption relies heavily on real random numbers as a source [15]. For scrambling medical photos, this technique appears to be a hundred times faster than the Advanced Encryption Standard (AES). AES is one of the most widely used methods for text data encryption in general. Due to its shortcomings in achieving low correlations, which are necessary to fend off statistical attacks on images, it is not frequently chosen for the encryption of images. The key space of the approach is 2^{510}, while it is 2^{256} for AES [16]. The first method also uses a True-Random-Number Generator for key generation that is based on a multiscroll chaotic oscillator, substantially boosting security. Some methods for encrypting medical images have used chaotic cat maps [17].

2. Objectives

The main motivation of considering water marking technique using DWT is that it provides better solution in both the form like spatial as well as transform domain. We are using DWT using for cover image which act like a carrier of our encrypted message image so that many will treat this as a normal cover image because if its appearance like the normal cover image to avoid attacker. This study has further concentrated on the following issues to enhance authentication and encryption quality in light of the various factors:

- A new and improved double encrypted chaotic map technique which consists up two chaotic maps to ensure increased authentication and security for digital image.
- Security analysis like different variety of image with different size of image taken into account.
- Comparison of results with other well knows existing techniques to demonstrate the improvement.
- Water marking technique is used to hide out double encrypted message image.
- Big size cover image is being used to hide our encrypted message image

Section 3 gives brief information about Bogdanov and Duffing map. The proposed method for encrypting and decrypting for both colour and grayscale images is described in Section 4. The outcome analysis is in Section 5, while the conclusion and the future focus are in Section 6.

3. Chaotic System and Watermarking

3.1 Bogdanov Map

In 2017, V. J. Subashini and S. Poornachandra put out a method for image encryption that entailed applying chaos to an image representing pixel values. An unremarkable cypher image can be produced by changing or modifying the image's pixel position value, which can then be reversed to produce plain text. The Bogdanov map bears the name of Soviet Russian mathematician Rifkat Ibragimovich Bogdanov. The Bogdanov-Takens bifurcation is depicted in a disorganised 2D map that was provided by the [18] author:

$$\begin{cases} x_{p+1} = x_p + y_{p+1} \\ y_{p+1} = y_p + \in y + kx_p(x_p - 1) + \mu x_p y_p \end{cases} \quad (1)$$

where ϵ, k and μ are control parameters and values are 0, 1.2 and 0 respectively.

This approach relies on the replacement of the old pixel position in the original image with a new pixel position by scrambling the pixels in the image. The same key (k) that is used to scramble data is also used to recover the original image. Images of any dimension can be scrambled using a Bogdanov map without being divided into chunks. There is therefore no restriction on the size of photographs. The Bogdanov algorithm restores the original image after a certain number of rounds. The period of the Bogdanov map is the number of iterations required to recover the original location pixels.

3.2 Duffing Map

Borislav Stoyanov et al. [19] suggested a brand-new image encryption technique based on the Chebyshev polynomial and the Duffing map. Similar to that, Amina Mahdi et al. suggested using Duffing Maps for voice encryption [20]. Bhavna Sinha et al. [21] present a comparative examination of image encryption using 3D chaotic maps. The discrete-time dynamical system known as the “Holmes map” or the “Duffing map” exhibits chaotic behaviour [6]. A 2D Duffing map represented by (xa, ya) in a plane by equation 2 is as follows:

$$\begin{cases} x_{p+1} = y_p \\ y_{p+1} = -bx_p + ay_p - y_p^3 \end{cases} \quad (2)$$

where the control parameters for equation 2 are a and b. The start or initial pixel is represented by xp and yp is shifted to xp+1 and yp+1 are new pixel positions. The following is the quantization equation that produces a random integer in binary format:

$$N(x) = \begin{cases} 0, & 0 < M(x,y) \leq 0.5 \\ 1, & 0.5 < M(x,y) \leq 1 \end{cases} \quad (3)$$

For grayscale image encryption, we first use equation 1 to generate pseudo random numbers, which are then quantized using equation 2 in binary format. The encrypted image is then created by XORing each bit with the quantized numbers of a grayscale image with a size of M × M. Read the encrypted image once again for decoding purposes, and then create random sequence numbers using the decryption key. The original image is created by XORing each bit of the M × M encrypted image with this sequence after it has been quantized to binary format.

3.3 Encryption Process

Pseudorandom numbers are first generated using equation 1 and control parameter values, after which they are quantized using equation 2, producing a binary matrix. The encrypted image is created by XORing each bit with the M × M grayscale image and quantization matrix.

3.4 Decryption Process

The first phase in the decryption involves employing an Arnold cat map with a secret key, which will once more move each pixel to a different spot in the image. The obtained decrypted image passes through still another decryption process in the very next step to recover the final derived image after two successive steps of decryption.

3.5 Watermarking

Embedding a message image into another image through image watermarking is a common practise. This embedded information, which may or may not be visible, can be used to prove who the rightful owner of the original image is or to deter unlawful duplication of the original image. There are two types of image watermarking techniques, i.e. transform domain techniques and spatial domain techniques. The attributes of imperceptibility and robustness are excellent for a digital watermarking technology. Additionally, spatial or transform domains can be used for watermarking [22].

Using the intensity data from the original cover image, the watermark is implanted in this method of watermarking. The watermark is often added by changing the least significant bits (LSB) of intensity values picked at random. The intensity values of the image are directly altered using the spatial domain watermarking method. These computationally efficient methods are straightforward [23]. These systems, however, cannot be used in real-time applications due to their significant susceptibility to typical attacks, noise, and signal processing approaches. In this case, the original cover image's transform or frequency coefficients contain the watermark's encoding. Compared to straightforward spatial domain watermarking systems, transform domain based watermarking techniques are more reliable [24]. Invertible transformations are employed for these purposes [25], such as the discrete wavelet transform (DWT), discrete Fourier transforms (DFT), and discrete cosine transforms (DCT). The most common 8 by 8 and 16 by 16 pixel sizes for these modifications are the complete image or smaller sections of it. To insert the watermark image, the frequency coefficients are modified. The watermarked embedded image can be obtained. After inverse transformation, the watermark is applied unevenly to the image pixels using transform domain watermarking, making it invisible and impervious to unauthorized alterations. It can therefore withstand common image modification processes including scaling, Gaussian noise, cropping, and JPEG compression attack. When the watermark is present in perceptually important areas of the image, the resistance to image distortion is more effectively obtained [26]. The middle frequency band of the cover image is where the watermark is placed. These methods demand greater complexity.

3.5.1 Discrete Fourier Transform (DFT)

In order to translate the spatial intensity image into its frequency domain, the Fourier transform first decomposes a spatial image function into a collection of orthogonal functions. The DFT embeds signals using phase modulation as opposed to magnitude components because phase modulation has less of an impact on visual perception. Additionally, phase modulation is more noise attack resistant [27]. Applying DFT requires a certain amount of calculations, which is directly proportional to N2. The computation is carried out using the rapid fourier transform method, whose decomposition can lead to a Nlog2N proportional amount of arithmetic operations. It is impossible for the fourier transform to identify local frequency content. The representation of oscillatory functions is challenging.

3.5.2 Discrete Cosine Transform (DCT)

Numerous image compression methods, like JPEG compression, use the discrete cosine transform (DCT) to transform images and quantize data from the spatial to frequency domain. This method divides the image into smaller parts and computes the DCT of each block separately [28]. A matrix with low, middle, and high frequency bands is created from each block. The most energy is present in the low frequency range. Therefore, any changes to this area lower the quality of the cover media and make the watermark evident. Any changes to this region won't have an impact on the image's quality because the high frequency has less energy than the low frequency. However, watermark removal using image processing techniques is simple. Consequently, the middle frequency range is typically where the watermarking is embedded. The main drawbacks of DCT are:

- It only takes into account the spatial connection between the pixels within of a single 2-D block while ignoring the correlation between the pixels in adjacent blocks.
- The DCT function cannot be adjusted to the input data.
- Binary images are not efficiently handled by it.

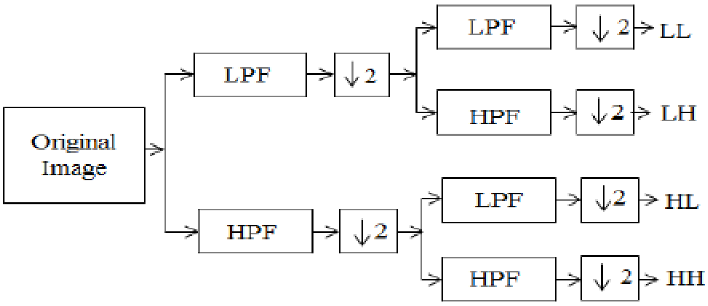

Fig. 1: Using high pass and low pass filter in one level decomposition

3.5.3 Discrete Wavelet Transform (DWT)

The discrete wavelet transform (DWT) is another quick and simple method for translating an image from the spatial to the frequency domain. In contrast to DFT and DCT, which only represent a signal in one of the spatial or frequency domains, DWT is able to provide a representation for both spatial and frequency interpretations concurrently. The discrete wavelet transform (DWT) is created by first applying sequential low-pass and high-pass filters to the discrete time domain signal [29]. The image is separated into four bands following wavelet decomposition: horizontal, vertical, diagonal, and low frequency component, which can be further, decomposed [30]. We may sum up DWT by saying that it is nothing more than a system of filters. The "wavelet filter" and the "scaling filter" are the two filters that are engaged. The scaling filter (also known as the average filter) is a low pass filter, whereas the wavelet filter (also known as the details filter) is a high pass filter. Fig. 1 shows the filters used for both the breakdown and reconstruction. The following are the main benefits:

- It does not require input coding to be divided because it displays better compression ratios.
- Better localisation is possible in the time and frequency domains.
- The alteration of the entire image results in inherent scaling.
- With the truncation of minor frequency coefficients, the reconstructed image exhibits less mistakes.
- The wavelet function can be selected at will.

4 Proposed Methodology

In this section, our proposed methodology will discuss under two heading i.e. proposed methodology for grayscale image and proposed methodology for color image.

4.1 Proposed Methodology for Grayscale Image

A Digital is nothing but a pixel values in a matrix. Pixel value is an integer positive number between 0-255 signifies the brightness of image where 0 means black and 255 means write and all values within the range represent shades of gray [31].

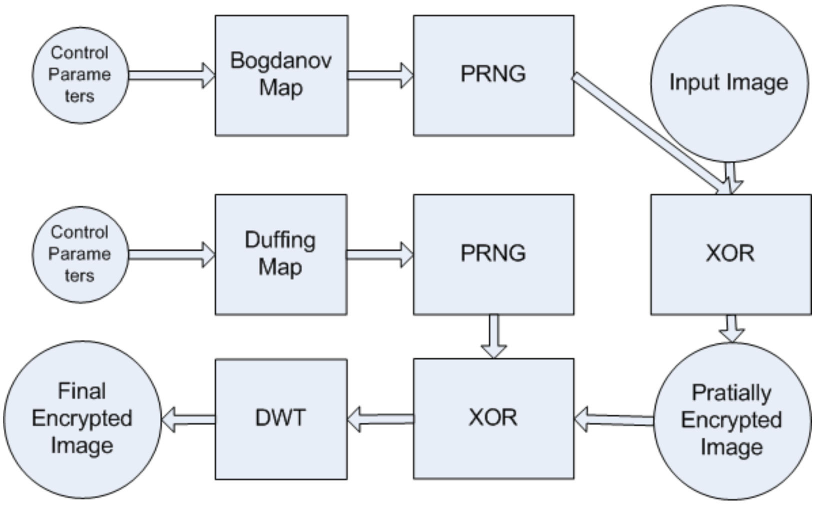

Fig. 2: Process diagram for grayscale image encryption of proposed work.

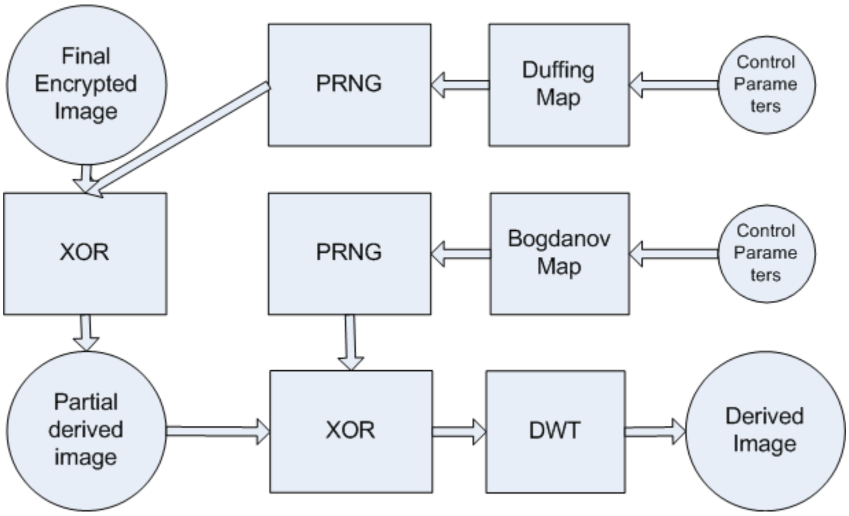

Fig. 3: Process diagram for grayscale image decryption of proposed work.

In the proposed methodology, we proposed a methodology which consists up two different chaotic systems made up of Bogdanov map and Duffing map to produce a final encrypted image, which will be the encrypted message image, which is merged into a cover image using DWT to produce a watermark image for data transmission, as shown in Fig. 2 and Fig. 3. The steps include are following:

Step 1: Take a input message image and represent it in a matrix form.

Step 2: Generate PRNG values using Bogdanov map.

Step 3: Modify the LSB of each pixel of the input message image by the help of PRNG sequences to produce from Step 2 to get a partially encrypted message image.

Step 4: Generate PRNG values using Duffing map.

Step 5: Modify the LSB of each pixels of partially encrypted message image produced from Step 4 to generate double encrypted message image, called final encrypted message image.

Step 6: Final encrypted message image is now merged into a big size cover image using DWT to produce a watermarked image for data transmission.

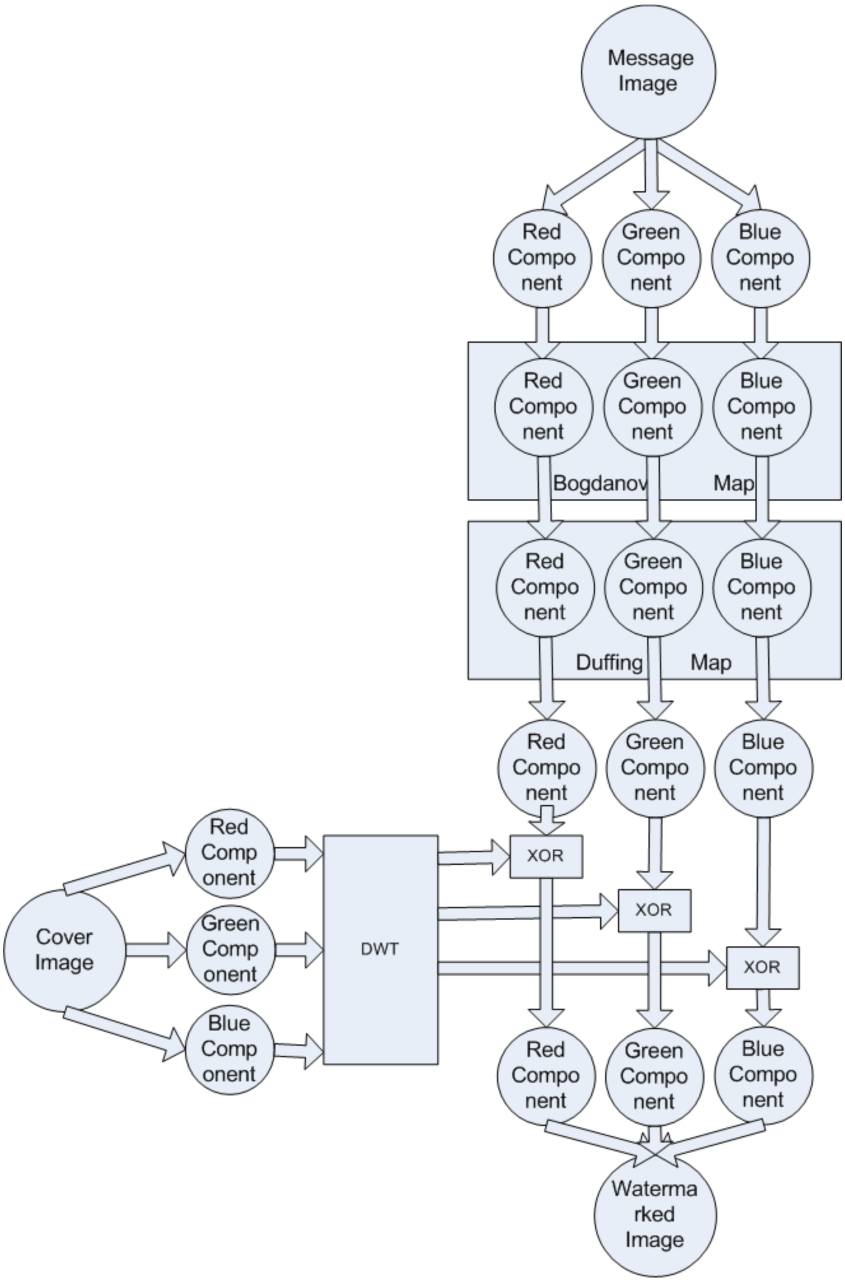

Fig. 4: Proposed diagram for color image encryption technique.

Similarly, the steps needed for decryption process are as follows:

Step 1: Take watermarked cover image as an input to extract a hidden double encrypted message image out of it using reverse of DWT.

Step 2: Generate PRAN using Duffing map.

Step 3: Modify the LSB of each pixels of double encrypted message image to get back partially encrypted message image.

Step 4: Generate the PRNG value using Bogdanov map.

Step 5: Modify the LSB of each pixels of the partial encrypted message image received from Step 3 to get back derived message image[32–35].

4.2 Proposed Methodology for Color Image

A digital color image differs from a grayscale image in that more additional information is not present. A color image can be represented using a variety of standard models, including RGB, CMY, YIQ, or image processing software (HSI). Of these, RGB depicts a color image as a three-by-three matrix, hence the name [36, 37]. The steps include are as follows:

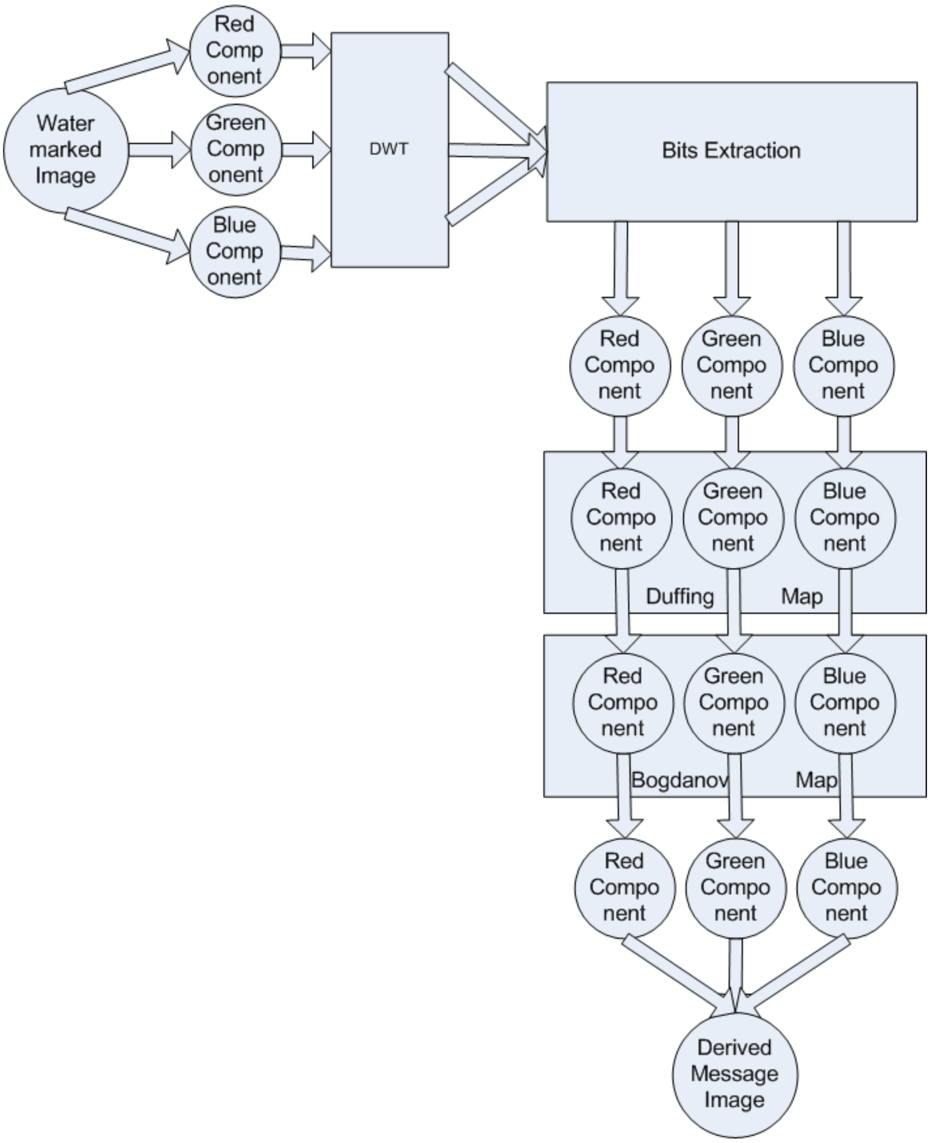

Fig. 5: Proposed diagram for color image decryption technique.

Step 1: Find Red, Green and Blue components of a color message image.

Step 2: Generate PRNG value using Bogdanov map.

Step 3: Modify the LSB of each pixels of the all Red, Green and Blue components of input message image using PRNG sequences generated in Step 2 to get partially encrypted all Red, Green and Blue components of message image.

Step 4: Generate PRNG value using Duffing map.

Step 5: Modify the LSB of each pixels of all Red, Green and Blue components of partially encrypted message image produced from Step 4 to generate double encrypted all Red, Green and Blue components of message image, called final all Red, Green and Blue components of encrypted message image.

Step 6: Find Red, Green and Blue components of a cover image.

Step 7: Apply DWT and IDWT on each Red, Green and Blue components of it.

Step 8: Applying the XOR operation of selected region obtained from step 5 and step 7.

Step 9: Combine all three components of cover image to get watermarked color cover image.

Similarly, the steps needed for decryption process are as follows:

Step 1: Take a color watermarked image as an input to find out Red, Green and Blue components of it.

Step 2: APPLY DWT and IDWT on each components.

Step 3: Apply XOR operation on selected area obtained from step 2 to get back Red, Green and Blue components of double encrypted message image.

Step 4: Generate PRNG value using Duffing map.

Step 5: Modify the LSB of each pixels of all Red, Green and Blue components of double encrypted message image produced from Step 4 to generate partially encrypted all Red, Green and Blue components of message image.

Step 6: Generate PRNG value using Bogdanov map.

Step 7: Modify the LSB of each pixels of partially encrypted message image

to get back derived message image.

Step 8: Combining all three components of derived message image to get derived color image.

All these steps are explained in Fig. 4 and Fig. 5 by experimenting using various message images with higher size cover images, by taking initial values xp = 0.5, yp = 0.5 along with appropriate control parameters for both Encryption and Decryption processes.

5 Performance Analysis

5.1 NPCR and UACI

A new encryption method was created by combining the chaotic map encryption techniques based on the Bogdanov map and the Duffing map. Due to the unique method’s chaotic nature, which is sensitive to initial conditions and control variables, even minor changes may have a significant effect on the results. As a result, pixel analysis is performed on both the original and encrypted images with a focus on the NPCR (Number of Pixel Changing Rate) and UACI (Unified Average Chang Index) [38] values. Equations 4 and 5 can be used to calculate the NPCR and UACI values, and each matrix’s dimensions should be similar.

$$NPCR = \frac{\sum_{p,q} K(p,k)}{m*n} * 100\% \quad (4)$$

$$UACI = \frac{\sum_{p,q}\left\{\frac{|M(p,q) - M'(p,q)|}{255}\right\}}{m*n} * 100\% \quad (5)$$

Larger NPCR values are better for digital image encryption, according to a number of studies, because they may be used to compare the pixel counts of two images (in this case, the original image and the encrypted image) and figure out how much they differ from one another. To determine how many pixels divide two images from one another, NPCR and UACI are helpful tools.

Table 1, which displays the typical values for the encryption and decryption operations, is used to determine the NPCR and UACI values for a variety of images with varying dimensions. A graphic representation of these times is shown in Fig. 6. The NPCR and UACI values of five current techniques are contrasted with those of our proposed method in Table 2.

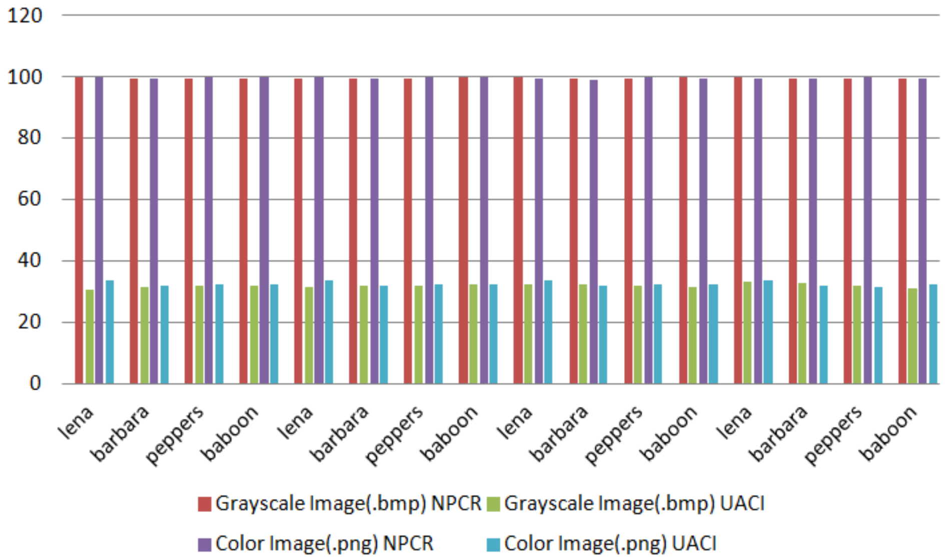

Fig. 6: NPCR and UACI Values for Grayscale and Color Images

Table 1: NPCR and UACI values for Grayscale and Color Images

Message Image	Cover Image	Grayscale Image(.bmp)		Color Image(.png)	
[64 x 64]	[512 x 512]	NPCR	UACI	NPCR	UACI
lena	peppers	99.6826	30.6075	99.6719	33.3943
barbara		99.4873	31.1939	99.5524	31.6786
peppers		99.5422	31.9608	99.5771	32.2321
baboon		99.5605	31.807	99.3421	32.4321
lena	barbara	99.6154	31.2776	99.6114	32.4744
barbara		99.5422	31.9608	99.4524	33.2568
peppers		99.5422	31.9608	99.4582	32.4621
baboon		99.6398	32.1701	99.6582	32.2341
lena	lena	99.6414	32.1689	99.6093	33.3016
barbara		99.6032	32.235	99.1419	31.6786
peppers		99.5422	31.9608	99.5534	32.4021
baboon		99.649	31.573	99.3324	33.0121
lena	baboon	99.6208	33.015	99.4582	33.0816
barbara		99.5861	32.8376	99.6093	31.6786
peppers		99.5422	31.9608	99.4656	31.4321
baboon		99.612	30.9768	99.5221	32.4341

Table 2: Comparison of the NPCR and the UACI values with state-of-the-arts

Image	Lena Image		Peppers Image	
	NPCR	UACI	NPCR	UACI
Tong et al.[39]	99.6296	33.7284	99.6201	32.9631
Nayak et al.[40]	99.6337	33.4564	99.6188	33.4711
Dong et al.[41]	99.6123	33.4293	99.6314	33.4284
Xian et al.[42]	99.6123	33.4293	99.6314	33.4284
Munoz et al.[43]	-	-	99.6094	33.393
Proposed Method	99.6298	33.7214	99.6217	32.9214

Table 3: Encryption and Decryption time in Second for Grayscale and Color Images [64 × 64].

Message Image	Cover Image	Grayscale(time in sec)		Color(time in sec)	
		ENCRYPTION	DECRYPTION	ENCRYPTION	DECRYPTION
lena64	Peppers512	0.3906	0.2656	2.1438	0.7013
barbara64		0.4062	0.2531	2.1314	0.7531
peppers64		0.4243	0.2812	2.2111	0.7613
baboon64		0.3437	0.1718	2.1406	0.7031
lena64	Barbara512	0.25	0.1875	2.0321	0.6875
barbara64		0.4175	0.2187	2.0532	0.7123
peppers64		0.3906	0.2812	2.2078	0.6821
baboon64		0.4175	0.1875	2.1123	0.6875
lena64	Lena512	0.2968	0.1718	2.2031	0.6949
barbara64		0.2968	0.1937	2.2165	0.6978
peppers64		0.2656	0.1718	2.0219	0.625
baboon64		0.2968	0.1562	2.1688	0.6923
lena64	Boat512	0.3281	0.1562	2.1125	0.6404
barbara64		0.4231	0.1718	2.2213	0.6921
peppers64		0.4312	0.2656	2.2344	0.7178
baboon64		0.4331	0.2187	2.1643	0.625

Table 4: Encryption and Decryption time in Second for Grayscale and Color Images [128 × 128].

Message Image	Cover Image	Grayscale(time in sec)		Color(time in sec)	
		ENCRYPTION	DECRYPTION	ENCRYPTION	DECRYPTION
lena128	Peppers512	0.625	0.1562	6.0469	1.1094
barbara128		0.5468	0.25	6.0425	1.0156
pepper128		0.6475	0.1718	6.1254	1.0213
baboon128		0.6406	0.1875	6.1406	1.1022
lena128	Peppers512	0.6093	0.1975	6.0156	1.0313
barbara128		0.7123	0.2031	6.1213	1.0124
pepper128		0.6743	0.2556	5.9721	1.0781
baboon128		0.7122	0.2136	6.1405	1.0225
lena128	Peppers512	0.675	0.1875	5.9375	1.0938
barbara128		0.7211	0.1562	6.1875	1.0645
pepper128		0.6076	0.2187	5.9844	1.0625
baboon128		0.6406	0.2343	6.0121	1.0469
lena128	Peppers512	0.625	0.2277	6.1094	1.0781
barbara128		0.7231	0.1718	6.125	0.9879
pepper128		0.6132	0.2187	6.1134	1.0469
baboon128		0.7134	0.2156	5.9856	1.0625

The encryption and decryption times for our unique techniques using grayscale and color images are shown in Table 3 for message image size [64 × 64] with cover image having size [512 × 512]. Similarly Table 4 represents the same for message image

size [128 × 128] with cover image having size [512 × 512]. Same the above information are represented by using Fig. 7 and Fig. 8 respectively.

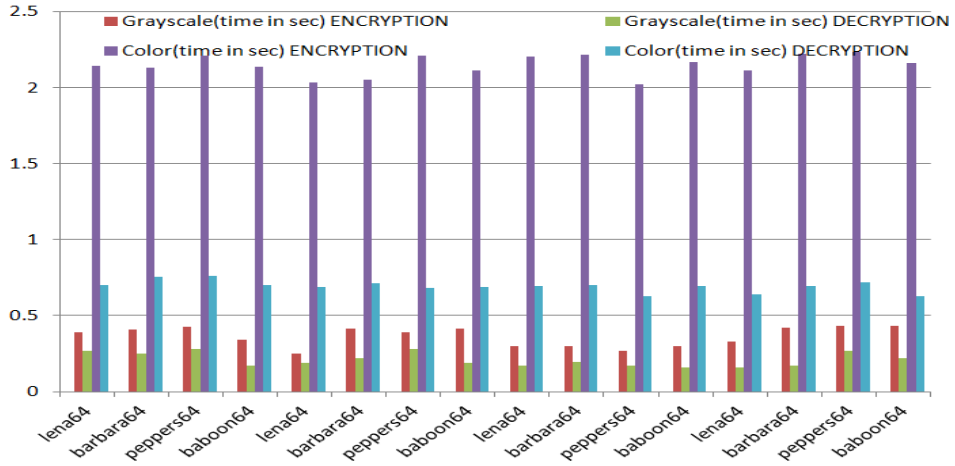

Fig. 7: Encryption Decryption time(in second for Grayscale and Color Images[64 × 64]).

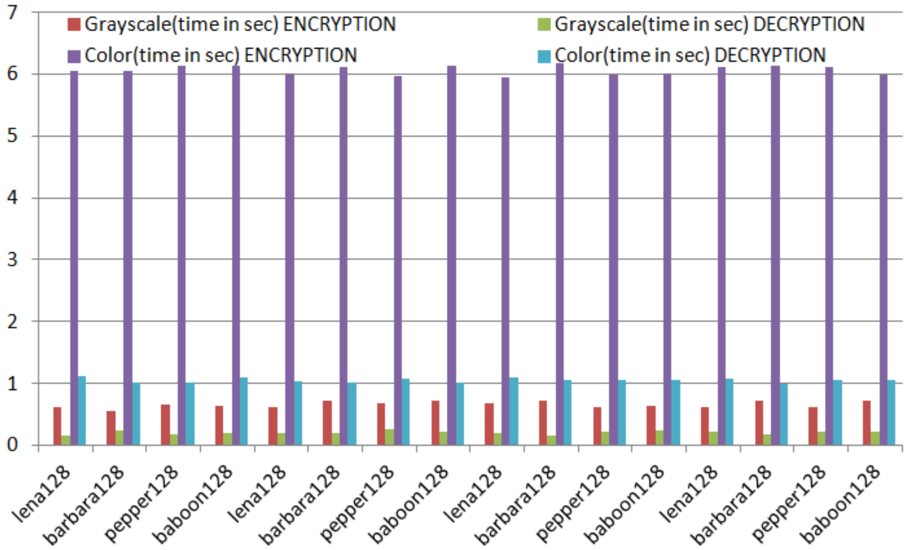

Fig. 8: Encryption Decryption time(in second for Grayscale and Color Images [128 × 128]).

5.2 Entropy

The amount of randomness in a digital image can be determined in large part through entropy information analysis. The optimal entropy value in this situation is 8 [46], which indicate a perfectly random image. Digital photographs typically feature 8-bit intensity levels. Consequently, the entropy value of the encrypted image should be close to 8 for the best photo encryption approach. The entropy of an image is computed using equation (6).

$$H(M) = \sum_{i=0}^{N-1} P(M_x) log_2 \frac{1}{P(M_x)} \qquad (6)$$

Table 5: Entropy calculation for Grayscale and Color Images for Original Vs Encrypted Image.

Image Size	Original(Gray)	Encrypted(Gray)	Original(Color)	Encrypted(Color)
lena64	7.267	7.2994	7.4546	7.6193
barbara64	7.3523	7.4696	7.6274	7.7193
peppers64	7.4134	7.4269	7.4369	7.5506
baboon64	7.5945	7.6161	7.5992	7.6227
lena128	7.3914	7.4178	7.4801	7.5067
barbara128	7.4582	7.4771	7.4557	7.5848
peppers128	7.549	7.6337	7.5689	7.6641
baboon128	7.5091	7.618	7.6101	7.627

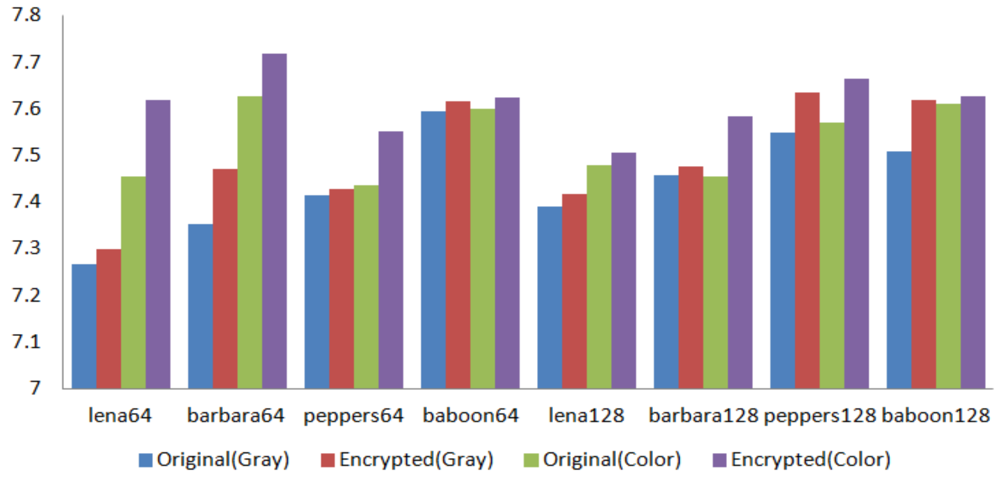

Fig. 9: Graphical representation of Entropy for Gray scale and Color Images

Where M_x stands for the pixel values (between 0 and 256), $P(M_x)$ for the probability of the symbol M_x, and N for the total number of symbols (256 in the case of a gray scale image). Table 5's entropy data shows values that are close to ideal values, demonstrating how similar the suggested method is to a random source. Same information is graphically represented by using Fig. 9.

5.3 Correlation Coefficient

One technique for encrypting digital images entails the encryption of the original image, which is then contrasted with the encrypted version using the correlation coefficient method. A statistic known as the correlation coefficient can be used to assess the effectiveness of a cryptographic method that depends on the correlation of two variables [46]. The correlation coefficient (r) has a range of values from -1 to 0 to 1, with a value of 0 denoting full dissociation between the two images (the best situation), a value of -1 denoting anti-correlation, and a value of 1 denoting identity. In Table 6, the r value is nearly zero, indicating a reliable cryptographic method. To determine the correlation coefficient using equation 7, apply the equation shown below:

Size	Image Name	Grayscale	Color
[64 x 64]	lena.png	-0.03315	0.0088
	barbara.png	0.0111	0.0019
	peppers.png	0.0036	-0.02256
	baboon.png	-0.0013	-0.00076
[128 x 128]	lena.png	0.0067	0.0014
	barbara.png	0.001	0.0041
	peppers.png	-0.0101	-0.00051
	baboon.png	-0.0012	-0.00135

Table 6: Calculated values for r between input message image Vs Encrypted message images(Grayscale and Color).

$$r_{pq} = \frac{cov(p,q)}{\sigma_p \sigma_q} = \frac{\frac{1}{N_s}\sum_{i=1}^{N_s}(p_i - E(p))\,(q_i - E(q))}{\sqrt{\frac{1}{N_s}(p_i - E(p))^2}\,\sqrt{\frac{1}{N_s}(q_i - E(q))^2}} \quad (7)$$

5.4 Histogram Analysis

A histogram is a two-dimensional, visual depiction of the pixels in a digital image. This shows each type of pixel in the digital image along with how frequently it appears. For the red, green, and blue channels of the Image, the histogram of the pixel values for the plain image and that of the encrypted image are displayed in Fig. 10. The images demonstrate how the histograms of the encrypted image are uniformly distributed and considerably dissimilar from those of the plain image.

5.5 Mean Squared Error (MSE) Analysis

A measurement of the difference between the plain and unencrypted image is the mean square error. The plain image and the encrypted image differ noticeably when the mean square error is significant. As a result, it advises using a strong encryption method. On the other hand, a high mean square error score shows that the encrypted image may be more vulnerable to attack because the original and encrypted images may be quite similar. Calculating the MSE involves using Equation 8. Table 7 shows the MSE values for colour and grayscale images.

$$MSE = \frac{1}{M * N}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(X(p,q) - Y(p,q))^2 \quad (8)$$

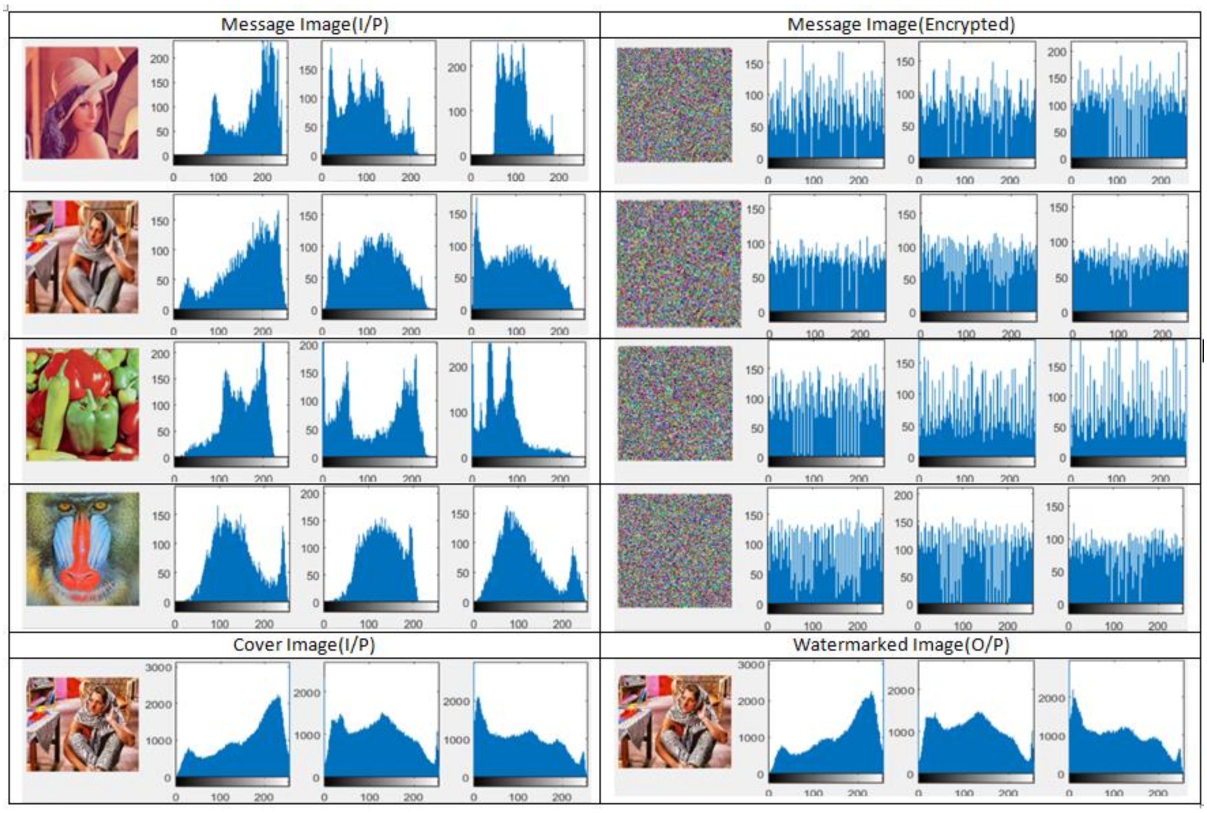

Fig. 10: Histogram for three components of Color Images for Message Image(I/P) with Message Image(Encrypted) of various type with one sample of Cover Image(I/P) and Watermarked Image(O/P)

Table 7: Calculated MSE and PSNR values for Grayscale and Color Images.

Image Name	MSE(Gray)	PSNR(Gray)	MSE(Color)	PSNR(Color)
lena64	7.6346	9.3029	10.135	8.0722
barbara64	9.4266	8.3872	9.1266	8.5277
peppers64	8.0092	9.0948	9.9076	8.171
baboon64	9.1266	8.5277	7.9046	9.1519
lena128	7.5353	9.3482	7.8105	9.204
barbara128	9.9076	8.1711	10.5517	7.8974
peppers128	8.3424	8.9178	8.4442	8.8651
baboon128	7.8105	9.204	8.3424	8.91788

The pixel values in this example are X (p, q) for the plain picture and Y (p, q) for the cypher image.

4.6 Peak Signal-to-Noise Ratio (PSNR) Test

PSNR test is used to evaluate the effectiveness of the encryption algorithm. It is reasonable to claim that efficient encryption is indicated by a low PSNR number. The PSNR values for the channels are determined using equation (9).

$$PSNR = 10log_{10}(255^2/MSE) \quad (9) PSNR = 10log_{10}(255^2/MSE) \quad (9)$$

The PSNR values for gray scale and color images are shown in Table 7, where as Table 8 indicating that our the suggested technique is performing comparatively better then previously existing techniques.

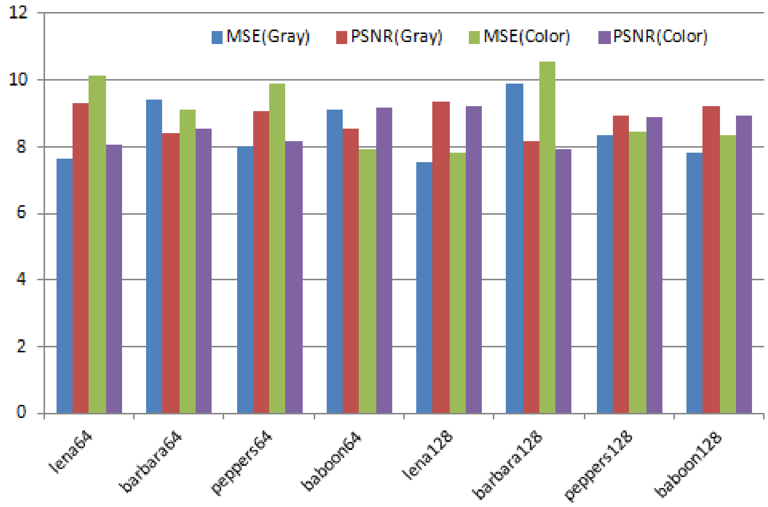

Fig. 11: Graphical representation of MSE and PSNR value for Grayscale and Color Images

Table 8: Comparison of MSE and PSNR values for Existing Methodologies with our Approach comparatively better then previously existing techniques.

Image	Matrics	Lena	Peppers	Barbara	Baboon

Som et al. [47]	MSE	7.244×10^3	8.431×10^3	-	-
	PSNR	9.56	8.91	-	-
Zhu[48]	MSE	7.229×10^3	8.205×10^3	-	-
	PSNR	9.54	8.99	-	-
Proposed Scheme	MSE	10.2724×10^3	10.0522×10^3	10.1956×10^3	7.9046×10^3
	PSNR	8.0141	7.9372	8.5277	9.1519

5. Conclusion

This innovative digital image encryption technique relies on the Bogdanov and Duffing maps as its foundational components. It comprises a two-phase process, augmented by the Discrete Wavelet Transform (DWT) watermarking method, to create a doubly encrypted message image. Subsequently, this image is converted into a watermarked representation, yielding the final encrypted image from the original. The reversal of this process retrieves the original image from the doubly encrypted, watermarked final image. Notably, this approach offers robust security, featuring an extensive key space that thwarts predictability and bolsters resistance against various attacks, thereby advocating a two-tier encryption strategy. Empirical results confirm the method's effectiveness, displaying a substantial key space, close-to-optimal NPCR and UACI values, favorable correlation, and entropy levels, thereby enhancing encryption standards. Additionally, the technique holds potential for integration into future 3D systems and applications in video and speech steganography.

Refrences

[1] Guo, J., Zheng, P., Huang, J.: Secure watermarking scheme against watermark attacks in the encrypted domain. Journal of Visual Communication and Image Representation 30, 125–135 (2015)

[2] Wang, B., Xie, Y., Zhou, C., Zhou, S., Zheng, X.: Evaluating the permutation and diffusion operations used in image encryption based on chaotic maps. Optik 127(7), 3541–3545 (2016)

[3] Abbas, N.A.: Image encryption based on independent component analysis and arnold's cat map. Egyptian informatics journal 17(1), 139–146 (2016)

[4] El Bireki, M.F.M., Abdullah, M., Ukasha, A.A.M., Elrowayati, A.A.: Digital image watermarking based on joint (dct-dwt) and arnold transform. International Journal of Security and Its Applications 10(5), 107–118 (2016)

[5] Ur-Rehman, O., ˇZivi´c, N.: Fuzzy image authentication with error localization and correction. In: Robust Image Authentication in the Presence of Noise, pp. 129–154. Springer, ??? (2015)

[6] Qureshi, M.A., Tao, R.: A comprehensive analysis of digital watermarking. Information Technology Journal 5(3), 471–475 (2006)

[7] Zhu, Q., Du, B., Turkbey, B., Choyke, P.L., Yan, P.: Deeply-supervised cnn for prostate segmentation. In: 2017 International Joint Conference on Neural Networks (IJCNN), pp. 178–184 (2017). IEEE

[8] Nguyen, T.-S., Chang, C.-C., Yang, X.-Q.: A reversible image authentication scheme based on fragile watermarking in discrete wavelet transform domain. AEU-International Journal of Electronics and Communications 70(8), 1055–1061 (2016)

[9] Wang, B., et al.: Reversible integer wavelet transform for the joint of image encryption and watermarking. Mathematical Problems in Engineering 2015 (2015)

[10] Zeki, A.M., Manaf, A.A., Ibrahim, A.A., Zamani, M.: A robust watermark embedding in smooth areas. Research Journal of Information Technology 3(2), 123–131 (2011)

[11] C, etınel, G., C, erkezi, L.L.: Chaotic digital image watermarking scheme based on dwt and svd. In: 2015 9th International Conference on Electrical and Electronics Engineering (ELECO), pp. 251–255 (2015). IEEE

[12] Liu, Y., Wang, Y., Zhu, X.: Novel robust multiple watermarking against regional attacks of digital images. Multimedia Tools and Applications 74, 4765–4787 (2015)

[13] Ravichandran, D., Praveenkumar, P., Rayappan, J.B.B., Amirtharajan, R.: Dna chaos blend to secure medical privacy. IEEE transactions on nanobioscience 16(8), 850–858 (2017)

[14] Praveenkumar, P., Amirtharajan, R., Thenmozhi, K., Rayappan, J.B.B.: Medical data sheet in safe havens–a tri-layer cryptic solution. Computers in biology and medicine 62, 264–276 (2015)

[15] Hu, J., Han, F.: A pixel-based scrambling scheme for digital medical images protection. Journal of Network and Computer Applications 32(4), 788–794 (2009)

[16] Kanso, A., Ghebleh, M.: An efficient and robust image encryption scheme for medical applications. Communications in Nonlinear Science and Numerical Simulation 24(1-3), 98–116 (2015)

[17] Fu, C., Meng, W.-h., Zhan, Y.-f., Zhu, Z.-l., Lau, F.C., Chi, K.T., Ma, H.-f.: An efficient and secure medical image protection scheme based on chaotic maps. Computers in biology and medicine 43(8), 1000–1010 (2013)

[18] Subashini, V., Poornachandra, S.: Chaos based image encryption using bogdanov map. Journal of Computational and Theoretical Nanoscience 14(9), 4508–4514 (2017)

[19] Stoyanov, B., Kordov, K.: Novel zaslavsky map based pseudorandom bit generation scheme. Applied Mathematical Sciences 8(178), 8883–8887 (2014)

[20] Mahdi, A., Jawad, A.K., Hreshee, S.S.: Digital chaotic scrambling of voice based on duffing map. International Journal of Information and Communication Sciences 1(2), 16–21 (2016)

[21] Sinha, B., Kumar, S., Pradhan, C.: Comparative analysis of color image encryption using 3d chaotic maps. In: 2016 International Conference on Communication and Signal Processing (ICCSP), pp. 0332–0335 (2016). IEEE

[22] Terzija, N., Geisselhardt, W.: Digital image watermarking using complex wavelet transform. In: Proceedings of the 2004 Workshop on Multimedia and Security, pp. 193–198 (2004)

[23] Asatryan, D., Asatryan, N.: Combined spatial and frequency domain watermarking. In: Proceedings of the 7th International Conference on Computer Science and Information Technologies, pp. 323–326 (2009)

[24] Kansal, M., Singh, G., Kranthi, B.: Dwt, dct and svd based digital image watermarking. In: 2012 International Conference on Computing Sciences, pp. 77–81 (2012). IEEE

[25] Qianli, Y., Yanhong, C.: A digital image watermarking algorithm based on discrete wavelet transform and discrete cosine transform. In: 2012 International Symposium on Information Technologies in Medicine and Education, vol. 2, pp. 1102–1105 (2012). IEEE

[26] Zhang, Y., Li, Y., Sun, Y.: Digital watermarking based on joint dwt–dct and omp reconstruction. Circuits, Systems, and Signal Processing 38, 5135–5148 (2019)

[27] Shih, F.Y.: Digital Watermarking and Steganography: Fundamentals and Techniques. CRC press, ??? (2017)

[28] Gunjan, R., Laxmi, V., Gaur, M.S.: Detection attack analysis using partial watermark in dct domain. In: Proceedings of the Fifth International Conference on Security of Information and Networks, pp. 188–192 (2012)

[29] Shekhawat, R.S., Rao, V.S., Srivastava, V.: A biorthogonal wavelet transform based robust watermarking scheme. In: 2012 IEEE Students' Conference on Electrical, Electronics and Computer Science, pp. 1–4 (2012). IEEE

[30] Pradhan, C., Saxena, V., Bisoi, A.K.: Non blind digital watermarking technique using dct and cross chaos map. In: 2012 International Conference on Communications, Devices and Intelligent Systems (CODIS), pp. 274–277 (2012). IEEE

[31] Huang, C.-K., Liao, C.-W., Hsu, S., Jeng, Y.: Implementation of gray image encryption with pixel shuffling and gray-level encryption by single chaotic system. Telecommunication Systems 52(2), 563–571 (2013)

[32] Wang, H., Xiao, D., Chen, X., Huang, H.: Cryptanalysis and enhancements of image encryption using combination of the 1d chaotic map. Signal processing 144, 444–452 (2018)

[33] Balaska, N., Ahmida, Z., Belmeguenai, A., Boumerdassi, S.: Image encryption using a combination of grain-128a algorithm and zaslavsky chaotic map. IET Image Processing 14(6), 1120–1131 (2019)

[34] Luo, Y., Yu, J., Lai, W., Liu, L.: A novel chaotic image encryption algorithm based on improved baker map and logistic map. Multimedia Tools and Applications 78(15), 22023–22043 (2019)

[35] Muhammad, K., Ahmad, J., Rehman, N.U., Jan, Z., Sajjad, M.: Cisskalsb: color image steganography using stego key-directed adaptive lsb substitution method. Multimedia Tools and Applications 76(6), 8597–8626 (2017)

[36] Singh, S., Parida, R., Pradhan, C.: Comparative analysis of image encryption using 2d and 3d variations of duffing map. In: 2018 International Conference on Communication and Signal Processing (ICCSP), pp. 0751–0754 (2018). IEEE

[37] Parida, R.R., Singh, S., Pradhan, C.: Analysis of color image encryption using multidimensional bogdanov map. In: istopathological Image Analysis in Medical Decision Making, pp. 202–225. IGI Global, ??? (2019)

[38] Wu, Y., Noonan, J.P., Agaian, S., et al.: Npcr and uaci randomness tests for image encryption. Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT) 1(2), 31–38 (2011)

[39] Tong, X.-J., Wang, Z., Zhang, M., Liu, Y.: A new algorithm of the combination of image compression and encryption technology based on cross chaotic map. Nonlinear Dynamics 72, 229–241 (2013)

[40] Nayak, P., Nayak, S.K., Das, S.: A secure and efficient color image encryption scheme based on two chaotic systems and advanced encryption standard. In: 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 412–418 (2018). IEEE

[41] Dong, C.: Color image encryption using one-time keys and coupled chaotic systems. Signal Processing Image Communications 29(5), 628–640 (2014)

[42] Xian, Y., Wang, X.: Fractal sorting matrix and its application on chaotic image encryption. Information Sciences 547, 1154–1169 (2021)

[43] Munoz-Guillermo, M.: Image encryption using q-deformed logistic map. Information Sciences 552, 352–364 (2021)

[44] Xu, L., Li, Z., Li, J., Hua, W.: A novel bit-level image encryption algorithm based on chaotic maps. Optics and Lasers in Engineering 78, 17–25 (2016)

[45] Shafique, A., Shahid, J.: Novel image encryption cryptosystem based on binary bit planes extraction and multiple chaotic maps. The European Physical Journal Plus 133(8), 331 (2018)

[46] Ahmad, J., Ahmed, F.: Efficiency analysis and security evaluation of image encryption schemes. computing 23, 25 (2010)

[47] Som, S., Kotal, A., Mitra, A., Palit, S., Chaudhuri, B.: A chaos based partial image encryption scheme. In: 2014 2Nd International Conference on Business and Information Management (ICBIM), pp. 58–63 (2014). IEEE

[48] Zhu, C.: A novel image encryption scheme based on improved hyperchaotic sequences. Optics communications 285(1), 29–37 (2012)