

RESEARCH

Open Access



# A novel secured Euclidean space points algorithm for blind spatial image watermarking

Shaik Hedayath Basha<sup>1\*</sup>  and Jaison B<sup>2</sup>

\*Correspondence:  
shaikhedayathbasha@rmkcet.  
ac.in

<sup>1</sup> Department of Electronics  
and Communication  
Engineering, R.M.K. College  
of Engineering and Technology,  
Tamil Nadu, Chennai, India

<sup>2</sup> Department of Computer  
Science and Engineering, R.M.K.  
Engineering College, Tamil Nadu,  
Chennai, India

## Abstract

Digital raw images obtained from the data set of various organizations require authentication, copyright protection, and security with simple processing. New Euclidean space point's algorithm is proposed to authenticate the images by embedding binary logos in the digital images in the spatial domain. Diffie–Hellman key exchange protocol is implemented along with the Euclidean space axioms to maintain security for the proposed work. The proposed watermarking methodology is tested on the standard set of raw grayscale and RGB color images. The watermarked images are sent in the email, WhatsApp, and Facebook and analyzed. Standard watermarking attacks are also applied to the watermarked images and analyzed. The finding shows that there are no image distortions in the communication medium of email and WhatsApp. But in the Facebook platform, raw images experience compression and observed exponential noise on the digital images. The authentication and copyright protection are tested from the processed Facebook images. It is found that the embedded logo could be recovered and seen with added noise distortions. So the proposed method offers authentication and security with compression attacks. Similarly, it is found that the proposed methodology is robust to JPEG compression, image tampering attacks like collage attack, image cropping, rotation, salt-and-pepper noise, sharpening filter, semi-robust to Gaussian filtering, and image resizing, and fragile to other geometrical attacks. The receiver operating characteristics (ROC) curve is drawn and found that the area under the curve is approximately equal to unity and restoration accuracy of [67 to 100]% for various attacks.

**Keywords:** Authentication, Attacks, Image analysis, Euclidean space points (ESP), Tampering, Watermarking

## 1 Introduction

Authentication, tamper detection, broadcast monitoring, and copyright protection are the important applications of watermarking [2]. Image watermarking is significant to prove the authentication or ownership of the digital images. It provides copyright protection to the digital images and it is used to detect tampering of digital images [22]. In the proposed work, the watermarking system is designed significantly involving all the above applications. The watermarking systems are categories into two types, they are spatial and frequency domain watermarking, and the trade-off parameters are robustness, imperceptibility, payload, and security [8]. In the literature, it is a challenge to

propose a spatial domain watermarking system by maintaining the trade-off parameters. The authors have taken up the challenge to provide a better spatial domain watermarking system.

In digital image watermarking spatial domain watermarking is simple and embedding the logo in the least significant bit offers less robustness, the robustness is increased by embedding the logo in the intermediate significant bits [10]. Kutter and Petitcolas [17] suggest embedding 80 bits of watermark data in the host image for good quality of perception and the recovery of watermark it sufficient to obtain greater than 80% of the watermark. Yinyin et al. [33] thinks that embedding 2 bits in every pixel increases the payload and processing the two images for image integrity makes the work very complex. Chuan et al. [3] develop watermark from MSB and embedding them as reference bits and authentication bits, but according to the benchmarking techniques by Kutter and Petitcolas in [17], the watermark needs to be independent with the host image and it was violated. Shabir et al. [25] developed a watermarking scheme to embed the logo in the intermediate significant bits of the host image at specific spatial locations using a random vector address, the average peak signal-to-noise ratio (PSNR) of five standard images embedding logo in the 4th significant bit is 45.084 dB.

Works on the authentication and tampering are studied in which, few authentication oriented are presented here, Kostopoulos et al., [14] generate authentication codes and embed in the  $4 \times 4$  blocks of host image where the residual histogram is produced. The PSNR values range from 51.454 dB to 48.826 dB depending upon the images. Yinyin et al. [33] implemented reversible data hiding and image authenticated using two images and tampered images are detected. Hong and Chen in [9] made the comparison between pixel pair matching and optimal pixel adjustment process and diamond process. Nikolaidis and Pitas in [20] used watermark casting for protecting the copyright of the digital content and provides robustness against JPEG and low-pass filter attacks. When discussing tampering literature, Zhang and Wang in [31] propose fragile watermarking and use two different types of bits known as reference bits and check bits to obtain the tampered regions from the host image. Similarly, the same author with other co-authors Zhang et al. in [32] proposed recovery of the tampered area from the host image using two methods in which the first method recovers 5 MSB's digits, and the second method uses restoration methods to recover the data.

Abraham and Paul in [13] works on the spatial color image watermarking scheme, in which out-off the three color frames red, green, and blue, only the blue color frame is used for watermark embedding and the other two color frames red and green are not disturbed. The watermark is embedded in the least significant bit of the blue color frame using a spatial mask, another spatial mask is used for red and green frames to retain the color information.

Wang and Su in [29] the color image is QR decomposed and matrix R is used for copyright protection of the color image in spatial domain. R. Sinhal in [22] converted RGB to gray-scale image and embedded the  $2 \times 4$  watermark in the LSB domain in a structure. Chun-Chi Lo and Yu-Chen Hu in [4] worked on the tampered images and the preserving the

image integrity. George Voyatzis and Ionnis Pitas in [7] proposed the concepts of robust watermarking with various attacks and stated that geometrical attacks are still a problem to solve. Huynh-The et al. [11] work on the binary watermark bits; they are embedded in the DWT blocks HL4 and LH4 to provide imperceptibility and robustness in the color images. Liu in [16] work on YCbCr color model images, they were tamper-proofed. Using dual-option parity check and morphological operations it was recovered. Sajjad et al. [23] proposed image tampering and restoration using SVD. Lei-Doa and Bao-Long in [15] resist the geometric attacks in the spatial domain, the watermark is embedded in the circular regions of the even-odd quantization.

Qingtang Su et al. in [21] proposed color image watermarking in YCbCr color space and performed watermark embedding in the Y component using the DC component of each  $8 \times 8$  sub-block in the spatial domain similar to DCT transform, this work was robust against signal processing attacks and geometric attacks, it does not specify the pitfalls of the method for the future scope. It does not add the security parameter to the proposed algorithm.

Dipti Prasad Mukherjee et al. [5] work on a new algorithm in the spatial domain, which provides buyer authentication with the multimedia objects, it provides robust against the standard Stirmark attack.

Image authentication scheme is proposed by Zhaxoia et al. in [35] using random values authentication codes are generated and induced in the user-defined seed using Hilbert curve mapping. Authors thought authentication of digital images in the natural way using the concept of moles on the human body. Moles on the human body are considered as one of the basic identification marks (authentication) for a person. In the same analogy, authors thought of establishing moles like watermarks all over the image to provide authentication where these watermark points are invisible and the moles are visible. Mathematical investigation behind moles on the human body is still under research, so author's proposed the points of watermarks (as like moles) on the digital image mathematically using geometric and arithmetic series. The authors thought of generating geometric sequences instead of any predefined curves. So, in the proposed work the geometric sequences were derived to retain the image authentication with added security concept.

The knowledge behind the Euclidean Space points and their axioms are obtained from [28] the idea behind discrete mathematics in the form of Geometric and Arithmetic Sequence came into play in the author's mind using from [6]. In the same way, the implementation idea of the Diffie-Hellman key exchange protocol was initiated in [27] explains the similarities and differences between watermark security and cryptography security.

Using the above knowledge, Euclidean Space point's (ESP) algorithm is designed in the second section. In the third section, the digital watermark embedding scheme in the raw host image is described along with the Diffie-Hellman key exchange protocol algorithm. The blind watermark recovery is described in the fourth section. Testing the proposed work and comparing with the existing methods on the standard raw digital grayscale, and RGB color images are carried out in the fifth section. The results and discussion is carried out with different perspective in the spatial domain with the conclusion of the proposed work.

## 2 Methods: Euclidean space point's (ESP) algorithm and Diffie–Hellman key exchange protocol

### 2.1 Aim

The proposed work objective is:

- a) To design and develop a New Euclidean Space Points (ESP) Algorithm using discrete mathematics and algebra.
- b) To implement blind spatial domain image watermarking system for image authentication and copyright protection using the developed ESP algorithm and Diffie–Hellman key exchange protocol algorithm for security purpose.
- c) To test the authentication and copyright protection of the proposed watermarking system by sending the watermarked images in the Email, WhatsApp, and Facebook platform.
- d) To test the proposed watermarking system with various attacks.
- e) To restore the watermark logo after the attacks.
- f) To analyze and evaluate the proposed watermarking system using quality metrics and statistical methods.

### 2.2 Design

#### 2.2.1 Euclidean space point's (ESP) algorithm basics

The Euclidean space point's (ESP) algorithm is designed first by choosing the size of the host image in which the watermarking is desired. Using discrete mathematics, in (discrete mathematics), geometric sequence (GS), and arithmetic sequence (AS) are generated and arranged along the  $x$  and  $y$ -spatial Cartesian coordinate system using the axioms of the Euclidean plane (UChicago REU, 2013). The generation of GS and AS is described in the ESP algorithm with example values. The points of intercept (POI), of the GS (along with the  $x$ -axis), and AS (along the  $y$ -axis) in the host image define the ESP to embed the watermark in the spatial domain.

#### 2.2.2 Proposed Euclidean space point's (ESP) algorithm

Step 1 : Let the set  $\mathbf{x} = (x_{11}, x_{21}, x_{31}, \dots, x_{n1})$  and  $\mathbf{y} = (y_{11}, y_{21}, y_{31}, \dots, y_{n1})$  are the possible sets of all ordered  $n$ -tuples in  $x$ -coordinates and  $y$ -coordinates. Let  $X = \mathbf{R}_x^n \cup \mathbf{R}_y^n = \mathbf{R}^n$  and the elements of  $\mathbf{R}_x^n$  and  $\mathbf{R}_y^n$  are the points in the spatial coordinates. The axioms of the Euclidean spaces are defined in [28].

If  $x$ , and  $y \in \mathbf{R}^n$ ,  $a \in \mathbf{R}$

- a) Vectors additions  $(x_{11} + y_{11}, x_{21} + y_{21}, \dots, x_{n1} + y_{n1})$ .
- b) Multiplication by a real number 'a'.

$$\alpha x = (\alpha x_1, \alpha x_2, \dots, \alpha x_n) \text{ and } \alpha y = (\alpha y_1, \alpha y_2, \dots, \alpha y_n).$$

c) Vector product  $(x_1y_1 + x_2y_2 + \dots + x_ny_n)$ .

Step 2 : Geometric sequence is obtained using the recursive Eq. (1):

$$x_{11} = x * r^N, \tag{1}$$

where  $r$  is the common ratio and  $N \in \{0, 1, \dots, R\}$ . The first term is  $x_0 = x * r^0$ , the second term is  $x_1 = x_0 * r^1$ , the third term is  $x_2 = x_1 * r^2$  and so forth. For example, let  $r=2$ ,  $x_0 = x = 1$ , and  $R = \{0, 1, 2, 3, \dots, 9\}$ . Thus the sequence  $x_{11}$  (2) is obtained [10], with the cardinality of 10:

$$x_{11} = \{1, 2, 4, 8, 16, 32, 64, 128, 256, 512\}. \tag{2}$$

Step 3 : Arithmetic sequence is obtained using the recursive Eq. (3):

$$y_{11} = y_n = y_{n-1} + d, \tag{3}$$

where  $d$  is a common difference, the first term is  $y_0 = y$ , the second term is  $y_1 = y_0 + d$ , the third term is  $y_2 = y_1 + d$  and so on. For example, let  $d=2$  and  $y_0 = y = 1$ , thus sequence (4) is obtained [6] with the cardinality of 10:

$$y_{11} = \{1, 3, 5, 7, 9, 11, 13, 15, 17, 19\}. \tag{4}$$

Step 4 : To obtain more point locations on the host image, these set points  $(x_{11}, y_{11})$ , are Improved using the Euclidean space points axioms defined in  $i(a)$ ,  $i(b)$ , and  $i(c)$ .

Using the axiom  $i(b)$ ,

let 'a' = 19 (Secret Key) we obtained another  $x_{12}$  sequence (5) where:

$$x_{12} = a * x_{11} = 19 * x_{11}$$

$$x_{12} = \{19, 38, 76, 152, 304, 608, 1216, 2432, 4864, 9728\}. \tag{5}$$

Similarly  $y_{12}$  sequence (6) is obtained using the axiom  $i(b)$ ,

$$y_{12} = a * y_{11} = 19 * y_{11}$$

$$y_{12} = \{19, 57, 95, 133, 171, 209, 247, 285, 323, 361\}. \tag{6}$$

Using the above axiom  $i(a)$  we get  $x_{13}$  sequence (7),  $x_{13} = x_{11} + y_{11}$

$$x_{13} = \{2, 5, 9, 8, 15, 25, 43, 77, 143, 273, 531\}. \tag{7}$$

From axiom  $i(c)$  we get the sequence,  $y_{13}$  sequence (8),  $y_{13} = x_{11} * y_{11}$

$$y_{13} = \{1, 6, 20, 56, 144, 352, 832, 1920, 4352, 9728\}. \tag{8}$$

**Table 1** Full-reference quality metric and No-reference quality metrics—analysis on standard set of images

Parameter	Texture—64 tiff images	Misc—25 tiff images	Football—44 JPG images	Sequence—64.tif images	Std. 13—PNG images
AVG. PSNR	53.452	50.512	39.507	49.915	52.838
AVG. SSIM	0.999	0.995	0.982	0.991	0.997
AVG. MSE	0.357	0.787	7.337	1.805	0.368
AVG. BER	2070.344	2011.52	144,497.1	2085.928	2057.385
AVG. BRISQUE	40.436	24.992	24.054	33.69	26.247

Here  $\{x_{11}\}, \{x_{12}\}$  and  $\{x_{13}\}$  are the possible sets of points in the  $x$ -coordinate. Similarly,  $\{y_{11}\}, \{y_{12}\}$  and  $\{y_{13}\}$  are the possible sets of points in the  $y$ -coordinate.

Step 5 If these coordinate points exceed the size of the host image, the location point processing is described below:


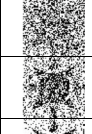
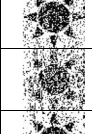
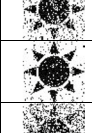

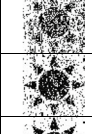
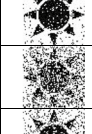
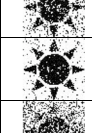

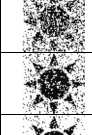
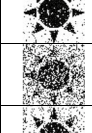
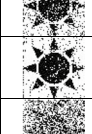

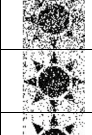
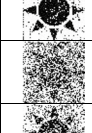


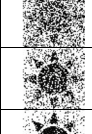
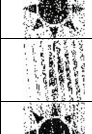
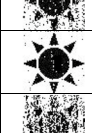
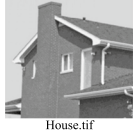
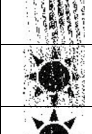

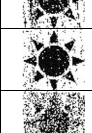

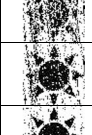
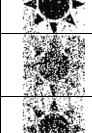
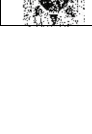

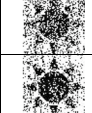

- a) If the size of the host image is  $M \times N$  then the location points are restricted to the maximum  $(M, N)$ , by applying modulus  $M$  on the  $x$ -coordinates points and modulus  $N$  on the  $y$ -coordinate points.
- b) The redundant location point values in the  $x$  and  $y$ -coordinates are removed.
- c) The set of processed  $x$ -coordinates and  $y$ -coordinates are taken as the location points to embed the watermark.

This set of sequences can further be expanded, but the designed algorithm takes only the axioms from the sequences (3) and (4) so that the processing time and the complexity can be reduced. An example of the ESP algorithm with (Tables 1, 2, and 3) is explained in the Supplementary material. In this algorithm, to initialize the security to the Euclidean Space points, the secret key is shared between the end-users using Diffie–Hellman key exchange protocol, which is explained in the next upcoming section.














### 3 Proposed watermark embedding scheme using ESP algorithm

In the proposed work, the host image is selected, and based on the size of the host image (different image sizes are chosen), the Euclidean Space points are designed using the ESP Algorithm. The main objective of the proposed work is to attain a blind and simple watermarking algorithm, imperceptibility of the watermark in the spatial domain, robust watermark for any attack, increased payload, and also to provide security to the watermark to preserve the owner copyrights or authentication. To achieve the mentioned parameters a block diagram is proposed which is shown in Fig. 1, the block diagram performs Euclidean space point’s based spatial domain watermarking and it is analyzed with both the grayscale image and RGB color model image. The proposed block diagram and algorithm are analyzed with the grayscale images and also with the RGB color model images.

**Table 2** Analysis of Facebook Images and Logo recovery in 4th, 5th, and 6th-bit planes

Input Image – Size – KB	Facebook Output Image – Size in KB - Compression Ratio in FB	Watermark Logo embedding at 4 <sup>th</sup> , 5 <sup>th</sup> , and 6 <sup>th</sup> Bit Position – PSNR(I, FB, I)	Logo's Obtained from FB	PSNR Logo_vs_FBLogo
 Crowd.tif 512 x 512 257 KB	56.3 KB 4.565:1	51.23		52.0796
		45.25		53.4445
		39.16		55.8471
 Women.tif 512 x 512 255 KB	41.9 KB 6.086:1	51.43		53.6815
		44.98		56.4874
		39.84		60.0548
 Pirate.tif 512 x 512 257 KB	74 KB 3.473:1	51.18		53.7856
		45.02		56.24
		39.05		60.14
 Woman_Blonde.tif 512 X 512 257 KB	74.5 KB 3.449:1	50.95		53.6892
		45.03		56.52
		38.57		59.58
 Mandril.tif 512 X 512 258 KB	70.5 KB 3.659:1	51.32		52.6139
		45.14		54.41
		39.26		57.21
 House.tif 512 x 512 186 KB	29.4 KB 6.326:1	52.40		53.3979
		44.14		56.75
		38.22		67.35
 Cameraman.tif 512 x 512 250 KB	47.2 KB 5.296:1	51.30		53.7700
		44.97		56.17
		39.44		59.87
 Woman.tif 512 x 512 250 KB	60.1 KB 4.293:1	51.15		53.7044
		45.11		55.51

**Table 2** (continued)

Lena.tif 512 x 512 258 KB		38.96		58.06
 Pepper.tif 512 x 512 237 KB	72 KB 3.292:1	51.14		53.5986
		45.05		56.02
		39.18		59.73
 Walkbridge.tif 512 x 512 257 KB	99.2 KB 2.590:1	51.17		53.6968
		45.18		56.42
		39.02		59.61
 Flower.png 768 x 512 215 KB	96.2 KB 2.235:1	52.82		53.79
		46.82		55.68
		40.93		59.51

#### 4 Proposed block diagram

In the proposed block diagram Fig. 1, the grayscale host image is first chosen in which the watermark is to be embedded. Next according to the size of the host image Euclidean space points are generated using the ESP algorithm. After obtaining the Euclidean space points, the grayscale intensity values of the host image at the POI are obtained and these grayscale intensity values of the host image are converted into its eight binary equivalent digits.

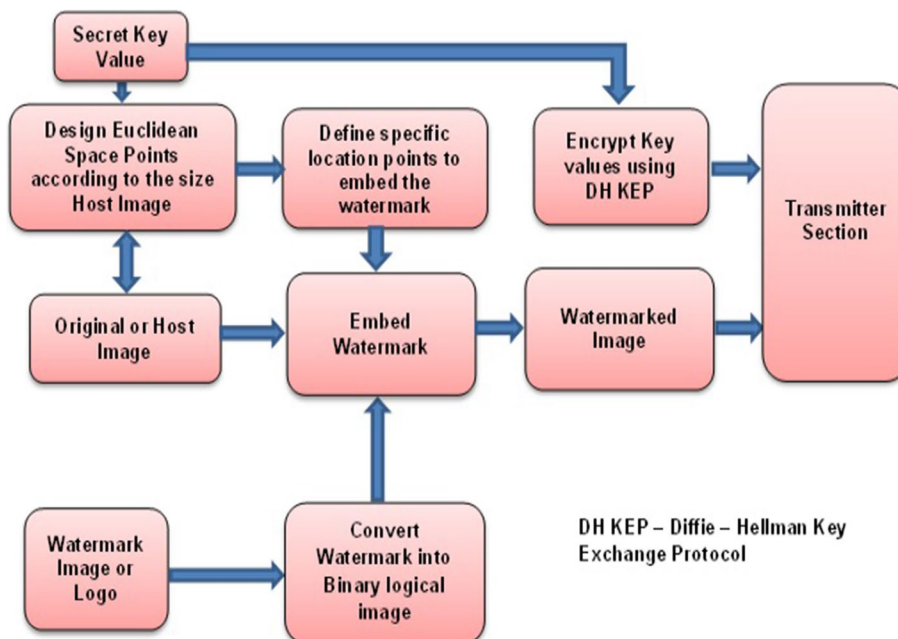
The watermark image or Logo is converted into a binary logical image using Otsu’s adaptive threshold method [26]. The binary digits of the logical logo are embedded in one of the bit planes or positions of POI obtained from the Euclidean space points and the watermarked image is obtained. The analysis was done on the host image by embedding the logo binary digits in every bit position of the POI. The watermarked image performance was obtained and it is described in the results and discussion.

In the second stage of the work, the RGB color image model is chosen as the host image. In this second proposed methodology, the RGB host image is processed by separating the red, green, and blue frames. The ESP algorithm is obtained according to the size of the Blue frame to obtain POI to embed the watermark logo. Intensity values of the blue frame at POI are obtained and converted to 8-bit binary digits. The binary digits of the logical logo are embedded in every bit position of POI and analyzed by merging the two frames. Similarly, the green color frame and red color frames are processed separately and analyzed. The results are described in the “Results and discussion” section. After individual frame processing, red, green, and blue frames are embedded with Logo2 at the same time and combined to get the RGB watermarked image.



**Table 3** Visual quality metrics of watermarked RGB color image vs. host RGB color image

Bit position	RED frame			Green frame			Blue frame		
	PSNR	SSIM	BRISQUE SCORE	PSNR	SSIM	BRISQUE SCORE	PSNR	SSIM	BRISQUE SCORE
1	73.91305	0.999999	3.652574	74.00604	0.999999	3.597931	73.93401	0.999999	3.662823
2	65.35526	0.999993	3.586746	65.48183	0.999995	3.544996	65.46446	0.999992	3.664936
3	58.45532	0.999966	3.594456	58.55183	0.999978	3.634625	58.52115	0.99996	3.599459
4	51.78935	0.999843	3.740193	52.06685	0.999902	4.336954	52.05295	0.999826	3.560328
5	45.51489	0.999335	4.745294	45.49001	0.999561	14.70399	45.76401	0.999265	3.685718
6	40.17327	0.9978	12.07964	39.2699	0.998131	28.00677	40.20428	0.997251	3.973584
7	34.64999	0.992523	26.86326	33.29469	0.993253	30.57064	34.81314	0.991155	7.408062
8	28.90179	0.97698	30.67823	27.81095	0.978214	30.27701	28.02154	0.968886	23.11204



**Fig. 1** Euclidean space points spatial domain watermarking

According to the concept of cryptography algorithm, public keys are shared in the public domain and private keys are shared securely. In the ESP algorithm, the initial  $x$ -coordinate value ( $x_0$ ), the initial  $y$ -coordinate value ( $y_0$ ), the common ratio value ( $r$ ), the common difference value ( $d$ ) and secret key value ( $a$ ) could be defined by the sender to obtain security of the Euclidean space points. This provides security to the Euclidean Space points where the watermark logo is going to reside. The concept of sharing private keys using Diffie–Hellman key exchange protocol is explained in the next section.

### 5 Diffie–Hellman key exchange protocol algorithm

The security of the secret key Diffie–Hellman key exchange protocol (DHKEP) [24] is one of the best algorithms to share the secret key securely in an unsecured channel [30].

The procedure of key exchange protocol is as follows:

- i. Let the two users be transmitter 'T' and receiver 'R' in a treaty to share the secret key.
- ii. In the treaty both 'T' and 'R' users agree on two prime numbers 'P' and 'G' and these are in the public domain. Choose P as a large number.
- iii. G is the primitive root modulo P.
- iv. Let 'T' and 'R' users choose privately 'a' and 'b'—a large random number or secret key or private key.
- v. 'T' computes  $A = G^a \text{mod} P$  and sends to 'R' and 'R' computes  $B = G^b \text{mod} P$  and sends to 'T'. Both 'T' and 'R' computes the shared key  $K = G^{ab} \text{mod} P$ ,

where 'T' computes  $K = B^a \text{mod} P = (G^b)^a \text{mod} P$ , and 'R' computes  $K = A^b \text{mod} P = (G^a)^b \text{mod} P$ . 'T' and 'R' share the shared key 'K' to exchange the secret key securely. This algorithm is the discrete logarithmic problem and it is equally as hard as RSA. In this proposed work  $P=7919$ ,  $G=3041$ ,  $a=19$  and  $b=17$ ,  $A=2753$ ,  $B=4886$ .

## 6 Proposed blind watermark extraction methodology

Figure 2 shows the proposed blind watermark extraction block diagram at the receiver end. In the transmission section, the host image could be either the grayscale image or the RGB color image. In the receiver section, after obtaining the watermarked image, the watermark logo can be removed and checked based on the required strategies. To prove the authentication of the sender at the transmission end the watermark logo could be recovered from the watermarked image without using the original logo or partial logo or original image, so the recovery of the watermark logo is very blind, so it is called blind watermarking. The logo is recovered by generating the secret key value 'a' from the shared keys between the two parties 'T' and 'R' using the Diffie–Hellman key exchange protocol.

Then the Euclidean space points are generated at the receiver end. The key value provides security to the location points of Euclidean space points where the logo was embedded. After obtaining the Euclidean space points from the secret key value, POI is obtained on the watermarked image, the intensity values of the POI from the watermarked image are obtained from all the specific locations of POI, and it is converted into its binary equivalent digits. As per the end–end user treaty, the bit where the digital bit of logo is embedded is obtained and all the digital bits are processed to form the logical digital binary logo, and hence the logical digital binary logo is recovered blindly without the use of any host image information or original watermark logo information and it proves the authentication or ownership of the user. Similarly, the logo is recovered from the RGB color image, and analysis was done and it is described in the “Result and discussion” section.

## 7 Results and discussion

The Euclidean space points (point of intercept of GS and AS) are obtained and shown in Fig. 3. The complete proposed work is implemented using custom MATLAB R2018a coding.

In the proposed work, the host image is selected and the Euclidean space points are generated using the ESP algorithm according to the size of the host image. Depending upon the initial values and secret key value the Euclidean space points are obtained, these points spread over the entire region of the host image, and it is an advantage that, when the watermark spreads over the entire region of the host image, authentication of the digital image could be obtained from every corner of the image.

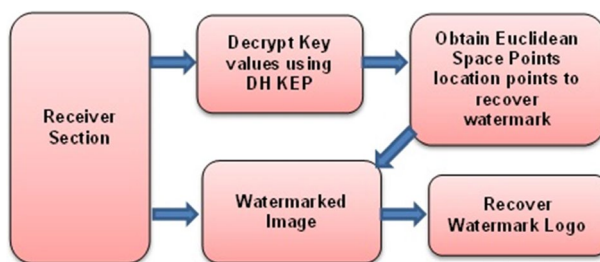
**7.1 Measure of imperceptibility**

The proposed watermarking scheme is applied on the data set (ImageProcessing-Place.com), in [12] which there are 166 raw images they are Gray Scale Data Set: Tiff\_Sequence\_Images: 64 images, Tiff\_Texture\_Image: 64 images, Tiff\_Misc\_Images: 25 images, and Standard\_PNG\_Images: 13 images, and JPG\_Football\_images: 44 images. ImageProcessingPlace.com data sets are the Image databases and it is selected because:

- a) These are the standard test images found frequently in literature.
- b) Almost all the images are uncompressed with higher resolution.
- c) Image databases are used for digital image processing using MATLAB, and they are in the DIP4E and DIPUM3E Faculty and Students Support Packages.
- d) In one place faculty and students can select different image data base according to their work.
- e) These databases are used in more than 50 countries worldwide.
- f) More than 1K research institution, industries, and educational institutes use DIP and DIPUM image databases.

**8 Most of the books, journals and publishers used these image databases**

In Fig. 4, ‘10’ standard grayscale images of size  $512 \times 512$  and ‘3’ standard color images of size  $512 \times 512$  are shown as few example images. Logo2 is  $64 \times 64$  which is the same proposed in [13]. In this proposed work, the grayscale Logo1.jpg or Logo2.jpg is used and is converted to a logical binary logo. The ESP algorithm is used to obtain the point of intersection of GS and AS according to the size of the host image. The length of the GS and AS is 90 without excluding zeros and redundant values. By removing the zeros and redundant values, the length of the GS and AS is 73, so 73 POI-ESP are obtained to embed the watermark of size  $32 \times 32$  logical binary logo, that is 1024 bits are required and for the  $64 \times 64$  logical binary logo 4096 bits are required to embed the binary logo in the host image. To obtain better imperceptibility of the watermark these 73 POI-ESP



**Fig. 2** Blind recovery of watermark

are not sufficient to embed the watermark. So, from GS and AS a maximum of  $73 \times 73$  array of POI is developed to hide the watermark in the host grayscale image. The  $73 \times 73$  POI of the host image is converted into 8-bit binary digits, and the logical binary digits of Logo1 are embedded in every bit and analyzed. The analysis is carried out with 166 raw grayscale images (\*.tiff and \*.png) and 44 \*.jpg images. The proposed methodology is analyzed with two types of quality metrics are Full-reference quality metrics and No-reference quality metrics.

### 8.1 Evaluation of image watermarking quality metrics

Image watermarking could degrade the quality of the host image to a certain degree, to test the watermarked image quality metric equal to the subjective perception of quality by a human observer [36] it can be done using two methods are Full-reference quality metrics and No-reference quality metrics. In the Full-reference quality metric, there are three algorithms used to check the quality of the image, they are image mean square error (MSE), image peak signal-to-noise ratio (PSNR), and image Structural Similarity Index (SSIM). MSE and PSNR are simple to calculate it is given in Eq. 9 from [19] peak Val is the maximum intensity value of the image, and Eq. 10, but they are very less compared to the quality of human perception:

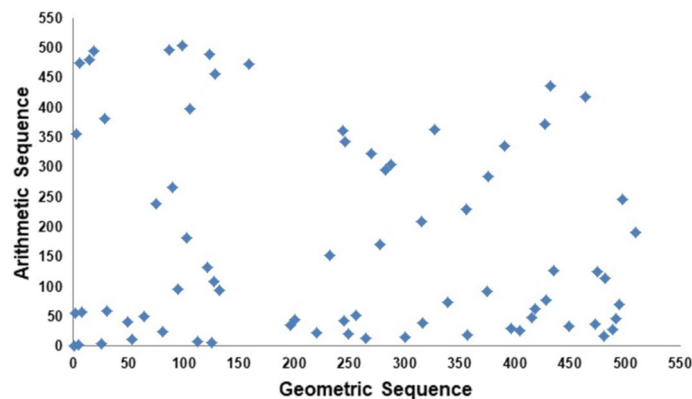
$$PSNR = 10 \log_{10} \frac{PeakVal^2}{MSE}, \tag{9}$$

$$MSE = \sum_{k=1}^3 \sum_{i=1}^M \sum_{j=1}^N \frac{WI(i,j) - I(i,j)}{3 * M * N}, \tag{10}$$

where  $WI(i, j)$  is the watermarked image and  $I(i, j)$  is the host image.

SSIM metric consists of luminance, contrast, and structural information of the digital image. The human visual system (HVS) perception is good at observing structures that are used in SSIM, so the metric SSIM is more related to the subjective quality score of human beings. Structural Similarity Index [26] is given in Eq. 11:

$$SSIM = [l(I, WI)]^\alpha * [c(I, WI)]^\beta * [s(I, WI)]^\gamma. \tag{11}$$



**Fig. 3** Euclidean space points—for  $512 \times 512$  host image with the initial values  $x_0 = y_0 = 1, r = 5, d = 2$ , secret key = 19

SSIM is based on the computation of three terms; they are luminance, contrast, and structural. They are computed using Eqs. (12), (13), and (14):

$$l(I, WI) = \frac{2\mu_I\mu_{WI} + C_1}{\mu_I^2 + \mu_{WI}^2 + C_1}, \tag{12}$$

$$c(I, WI) = \frac{2\sigma_I\sigma_{WI} + C_2}{\sigma_I^2 + \sigma_{WI}^2 + C_2}, \tag{13}$$

$$s(I, WI) = \frac{\sigma_{IWI} + C_3}{\sigma_I\sigma_{WI} + C_3}, \tag{14}$$

where  $\mu_I, \mu_{WI}, \sigma_I, \sigma_{WI}$ , and  $\sigma_{IWI}$  are the local means, standard derivations, and cross-covariance for images  $I$  (host image) and  $WI$  (Watermarked image).

If  $\alpha = \beta = \gamma = 1$  (default)

$$C_3 = C_2/2 \tag{15}$$

Substituting Eqs. 12, 13, 14, and 15 in 10, we obtain equation from [32]:

$$SSIM(I, WI) = \frac{(2\mu_I\mu_{WI} + C_1)(2\sigma_{IWI} + C_2)}{(\mu_I^2 + \mu_{WI}^2 + C_1)(\sigma_I^2 + \sigma_{WI}^2 + C_2)}. \tag{16}$$

The formula to calculate the correlation coefficient is given in Eq. (17):



**Fig. 4** Images: up to down. From left to right: first row: cameraman.tif, Lena.tif, Mandril\_gray.tif, Pepper.tif, Pirate.tif, second row: Walkbridge.tif, Woman\_blonde.tif, Woman\_blackhair.tif, White\_Page.tif, Black\_Page.tif, third row: Lena\_Color.tif, Mandril\_Color.tif, and Pepper\_Color.tif (grayscale and color host images of size 512 × 512), Logo1.jpg and Logo2.jpg (Grayscale images of size 64 × 64)

$$CC = \frac{\sum_M \sum_N (I_{M,N} - \bar{I})(WI_{M,N} - \bar{W})}{\sqrt{\left(\sum_M \sum_N (I_{M,N} - \bar{I})^2\right)\left(\sum_M \sum_N (WI_{M,N} - \bar{W})^2\right)}}, \quad (17)$$

where  $\bar{I}$  is the mean of the original image and  $\bar{W}$  is the mean of the watermarked image. The correlation coefficient value ranges from  $-1$  to  $1$ . ' $M$ ' and ' $N$ ' are the number of rows and columns of the host image  $I(M, N)$  and watermarked image  $WI(M, N)$ . The bit error rate is the ratio of no. of bits in error to that of total no. of bits.

The watermark Logo1 or Logo2 is embedded in all the bit planes of Fig. 4 images (Table 4 in Supplementary material) at the specific ESP of  $I(M, N)$ . Full Reference Quality Metric is measured, it is observed that using the proposed ESP algorithm and embedding methodology in the spatial domain gives the average PSNR of 46.21356 dB and 40.3028 dB between  $I$  and  $WI$  at the 5th-bit plane or position due to the logical binary logo of size  $32 \times 32$  and  $64 \times 64$ , respectively. At the 4th bit plane, the PSNR is 52.53392 and 46.4826, respectively. The PSNR is above 45 dB even if the watermark binary logo is embedded in the 4th-bit plane. In all the 166 raw grayscale images (\*.tiff and \*.png) the  $64 \times 64$  size binary watermark logo 'Logo2' is embedded in the 4th bit plane of the host image at the specific ESP, and whereas in the 44 \*.jpg images, the watermark is embedded in the 6th-bit plane instead of 4th plane because in compressed images \*.jpg, the embedded watermark in the 4th-bit plane could not be recovered properly.

## 8.2 No-reference quality metrics

In the No-reference quality metrics evaluation method, there are two algorithms, the first algorithm is Blind/Referenceless Image Spatial Quality Evaluator (BRISQUE), and the second algorithm is Natural Image Quality Evaluator (NIQE) from [1]. BRISQUE model is trained with the set of images with the known distortion, whereas NIQE can evaluate the quality of the images with arbitrary distortion. BRISQUE is opinion-aware that is the subjective quality score that correlates with HVS but NIQE is opinion-unaware. Figure 5 shows the relationship between the average SSIM and the average BRISQUE score of all the 10 standard grayscale images.

The BRISQUE value is low for good images and high for the distorted images. The proposed ESP algorithm and embedding methodology satisfy the relationship between BRISQUE and SSIM. Table 1 gives the values of the Full-reference quality metric and No-reference quality metrics of all the standard sets of images.

In all the raw images, that is \*.tiff, \*.tif, and \*.png the watermark Logo2 is embedded in the 4th bit plane of a specific ESP location. In the compressed images (\*.jpg), Logo2 is embedded in every 4th, 5th, and 6th-bit plane to check the blind recovery of Logo2 at the receiver end. The average Full-reference quality metrics and average No-reference quality metrics of all the images between the 'I' and 'WI' are measured. According to the measurement in Table 1, as the MSE (mean square error) more the PSNR (peak signal-to-noise ratio) is less. Similarly, the BER (bit error rate) is high for high MSE.

### 8.3 Watermarked image analysis via Email, WhatsApp, and Facebook

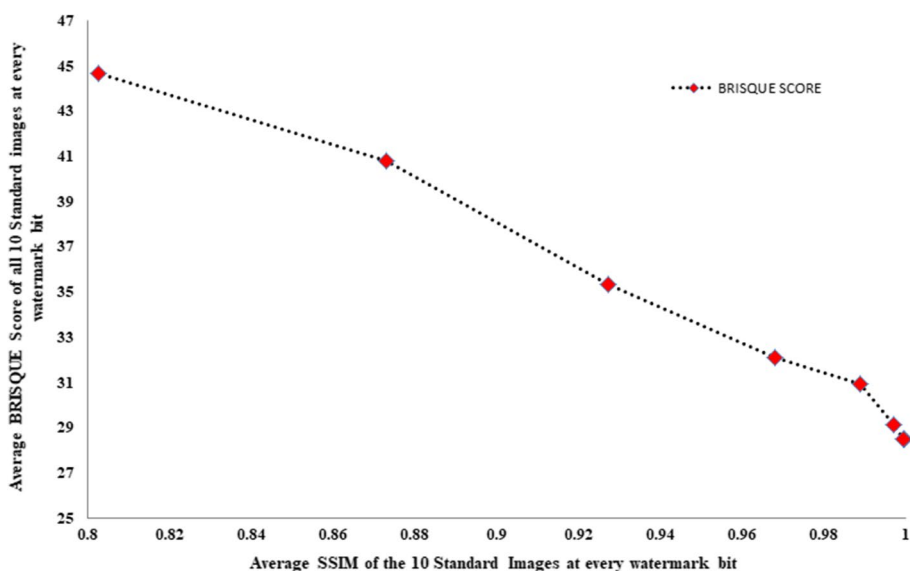
All the raw watermarked images (WIs) are zipped, attached in a folder, and sent to the personal email. The WIs from email (E\_WI) are downloaded and extracted through the compressed folder. Performance metric analysis on the images WI and E\_WI is done and it is found that the PSNR is infinite dB, SSIM is unity, BER is zero, and NC is unity. All the embedded logos are perfectly recovered from all the sets of images. Similarly, all the WIs are sent individually in WhatsApp and downloaded from WhatsApp the metric analysis between WI and W\_WI is done the result values are as same as email.

In the same way, the WIs are uploaded to the authors' Facebook (FB) book account and downloaded individually. It is shown in Fig. 6. The observations made in the analysis are the following:

- a) The input data set raw images are in the format \*.tiff, \*.tif, \*.png, the output image downloaded from FB is \*.jpg.
- b) If the size of the WI to the FB is  $M \times N$  (less than  $1024 \times 1024$  pixels), occupied space say  $XX$  KB (below 1 MB) of memory in the drive, the F\_WI size is as same as input image with fewer data storage (approximately  $XX/4$  KB). That is the memory compression is carried in FB. The embedded logo is blindly recovered.
- c) If the size of the WI to the FB is greater than say  $1024 \times 1024$  pixels and occupying more than 1 MB of storage, then the F\_WI size is different from that of the WI, and memory compression takes place it is approximately equal to  $XX/2$ .
- d) In this proposed work, if the size of the image is altered to a greater extent, the logo could not be perfectly recovered.
- e) Authentication is tested from the F\_WI images, it is observed that the binary watermark logo embedded 4th bit of host image could be partially recoverable with very low SSIM and PSNR. Then logo is embedded in the 5th and 6th-bits, found that the logo from F\_WI could be recovered blindly.

**Table 4** PSNR comparison of the proposed method with the other methods on Lena ( $512 \times 512$ ) image

S. no.	Method	PSNR in dB	PSNR after restoration from tampering in dB
1	Proposed method (Logo1– $64 \times 64$ )	[41.251, 63.244]dB	Inf
2	Proposed method (Logo1– $32 \times 32$ )	[47.105, 69.263]dB	Inf
3	Proposed method (Logo2– $64 \times 64$ )	[41.219, 63.191]dB	Inf
4	Chuan Qin et al., with different tampering rates [3]	[37.91, 51.15] dB	[40.72, 51.14] dB
5	R. Sinhal [22]	49.68 dB	Inf
6	Zhang and Wang, [31]	28.7 dB	Inf
7	Zhang et al. [32]	37.9 dB	[20, 40] dB



**Fig. 5** Average SSIM vs. average BRISQUE score

So for this proposed algorithm, 5th-bit logo embedding is advisable for the Facebook image authentication, because the 6th-bit offers very low PSNR (less than 40dB) between I and F\_WI from Table 2.

It is analyzed by comparing the histograms of WI and F\_WI. The histogram difference between the WI and F\_WI is similar to exponential noise. It is submitted in Annexure (Table 5) since the numbers of tables are more in this work:

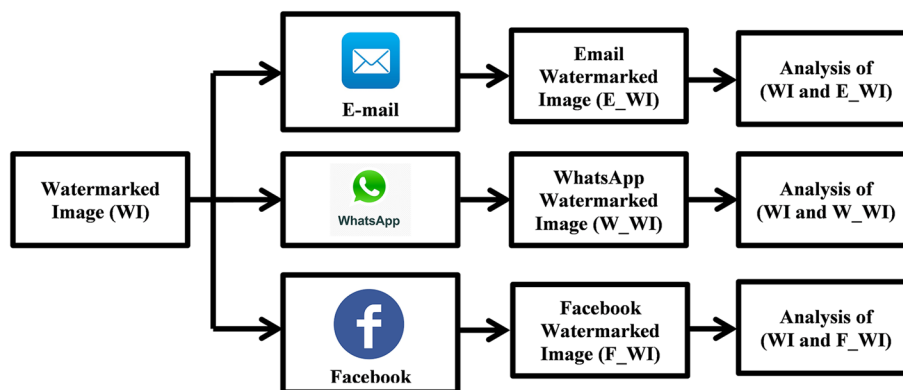
- f) All the Logos from WI are recovered blindly. So the proposed work falls in the category of blind image watermarking.

#### 8.4 Attacks and tests for image authentication

To test the proposed scheme for image authentication, the WI tampers with various attacks. The watermark logo is obtained from the tampered watermarked image without the reference of the host image (Blind Watermarking) and compared with the original logo as shown in Fig. 7. The tampered watermarked image obtained at the receiver section is processed with the ESP algorithm and the watermark logo is extracted. The tampered image can be recovered using the steps followed in Fig. 7.

The tampered image is recovered using the host image as a reference, at first the tampered image and the host image are subtracted to get the residual tampered region. Next, the residual tampered image region coordinates are collected and mapped with the coordinates of the host image. The intensity values of the coordinates from the host image are collected and the intensity values are replaced in the residual region to recover the tampered region. The PSNR between the recovered watermarked image and the watermarked image is infinity. In the proposed watermarking scheme even if the watermarked image tampers more than 90%, detection of the watermark is done as shown in Fig. 8h. Figure 8a–o shows the extraction of the watermark logo from the tampered





**Fig. 6** Analysis of watermarked image via E-mail, WhatsApp and Facebook

**Table 5** Confusion matrix to test the algorithm and watermarking scheme

Confusion matrix	Predicted NO: test bit, 'binary 0'	Predicted YES: test bit, 'binary 1'
Actual NO: reference bit 'binary 0'	TN—true negative	FP—false positive
Actual YES: reference bit 'binary 1'	FN—false negative	TP—true positive

watermarked images with different percentages of tampering. Tampering on the watermarked image was tested on the standard Lena image of size  $512 \times 512$  with the tampering rate from 0.59 to 95% the proposed work provides the PSNR of the watermark logo in the range of [81.2441 to 52.9996]. This shows that the proposed ESP algorithm, the watermarking embedding and recovering scheme offers very good image authentication.

**8.5 Imperceptibility in color images**

RGB color image model analysis: Lena.png image is processed by embedding Logo2.jpg in individual color frames and the PSNR of the watermarked image and RGB host image is calculated and shown in Table 3. The proposed work performance is very excellent compared with the other existing methods. Table 3 is evident for its performance. The BRISQUE score for the good quality image should be a low value, the ESP algorithm and the watermarking scheme provide the best watermarking, and the relationship between the PSNR, SSIM, and BRISQUE also satisfies the relation. Another observation is that the embedding can be carried out up to the 4th-bit position and 5th-bit position in the POI where the watermark would be still imperceptible.

**8.6 The restoration process of RGB color images**

In the practical view, when the digital images are transmitted in the channel, images may lead to different attacks by the intruders it may be an intentional or unintentional attack. The proposed work needs to offer good robustness and security to the intruders. So to

check the performance of the proposed algorithm 10 standard sets of raw images from (ImageProcessingPlace.com) are taken. Different types of attacks are performed on the watermarked image and the performance of the proposed ESP algorithm and the watermarking scheme was tested using the performance metrics SSIM, cross-correlation function (CC), mean square error (MSE), and bit error rate (BER). Figures 9, 10, 11, 12, 13 show the visual quality metrics on the recovered watermark before and after restoration. The Logo2 is embedded in all three color frames Red, Green, and Blue. The average SSIM of Logo2 before restoration that is after all attacks on the RGB color watermarked image is 0.979294 and after restoration is 0.995141. The restoration process enhances the correlation coefficient value to a greater extent. The restoration process was done as follows:

Input Host image: RGB Color Model image.

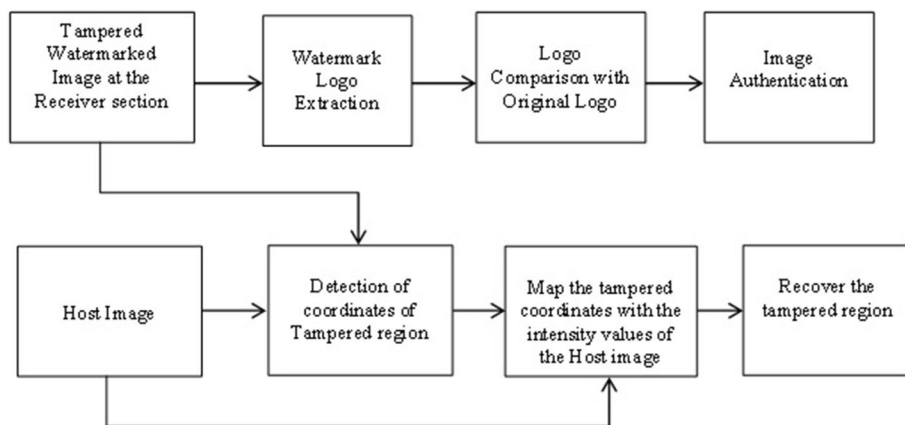
- Step 1: Store all the three color frames separately as 'R', 'G', and 'B' of the host image.
- Step 2: After watermarking and transmitting from the transmitter section in Fig. 1, store the watermarked image in the receiver section.
- Step 3: Let 'R\_A', 'G\_A', and 'B\_A' be the three color frames after an attack.
- Step 4: Restoration process: Let 'Res\_A', 'Res\_G', and 'Res\_B' be the restored frames. Calculate  $Res\_A = R - R\_A$ ;  $Res\_G = G - G\_A$ ; and  $Res\_B = Res\_B - B$ .
- Step 5: Using the restored frames Logo2 can be obtained with acceptable visual quality.

Using the above restoration process, the average correlation coefficient on all the attacks was increased by 0.450106 times.

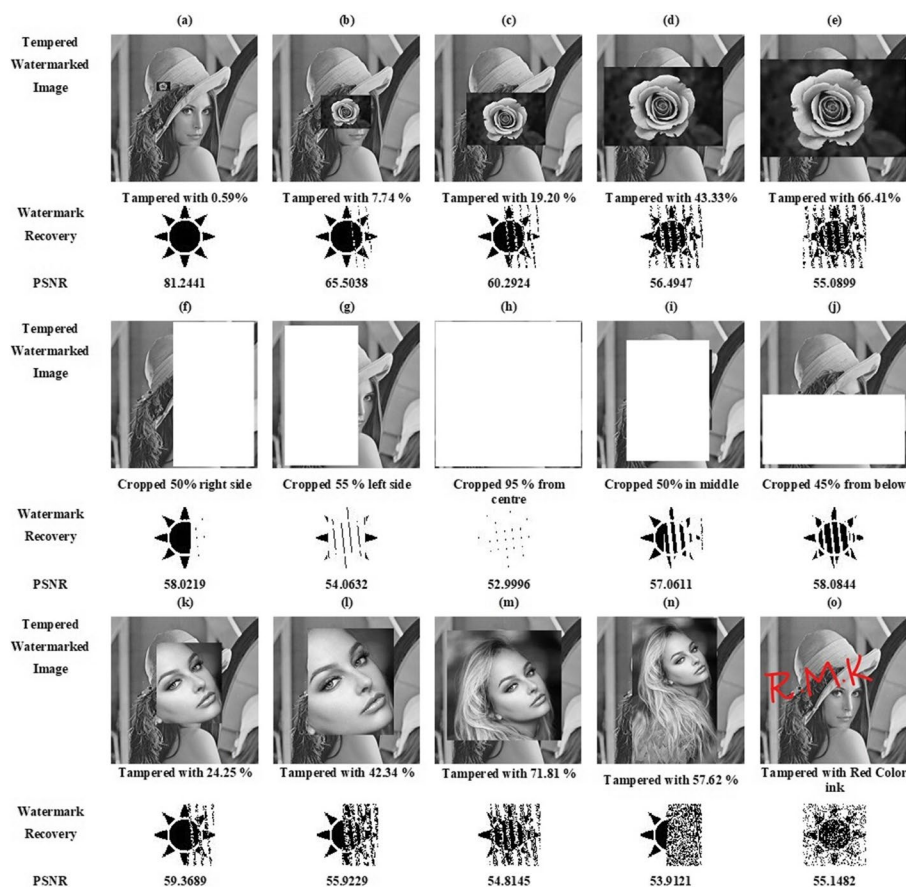
The average mean square error and average bit error rate on all the attacks were decreased by 0.232843 and 953.7059.

The accuracy is calculated by using the formula from [18] after the restoration process, it is given in Eq. (18):

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{18}$$



**Fig. 7** Image authentication and recovery from tampered watermarked image



**Fig. 8** Recovery of watermark from tampered watermarked images for image authentication

where TP: true positive, TN: true negative, FP: false positive, and FN: false negative.

Figure 12 shows that after the restoration process, the watermark Logo2 can be obtained with an accuracy of more than 67%. So the proposed ESP algorithm, watermarking scheme, and restoration scheme work more accurately.

### 8.7 Watermark restoration

The watermark Logo2 was better restored after the restoration process.

In Fig. 14, watermark Logo2 after the attack and restored watermark Logo2 from the watermarked image is shown with all different kinds of attacks. The proposed watermarking scheme and the algorithm are immune to salt-and-pepper noise and sharpening filter that is before restoration.

### 8.8 Comparison with the existing methods

Comparison of average PSNR values of 10 standard grayscale images with the other existing methods is presented in Table 4. The proposed ESP algorithm and watermarking methodology were analyzed by embedding a logical binary logo individually in every bit position of the host image. In Fig. 2 of Chuan Qin et al. in [3] at page 236, the watermark bits are used to recover MSB layers of the tampered image but

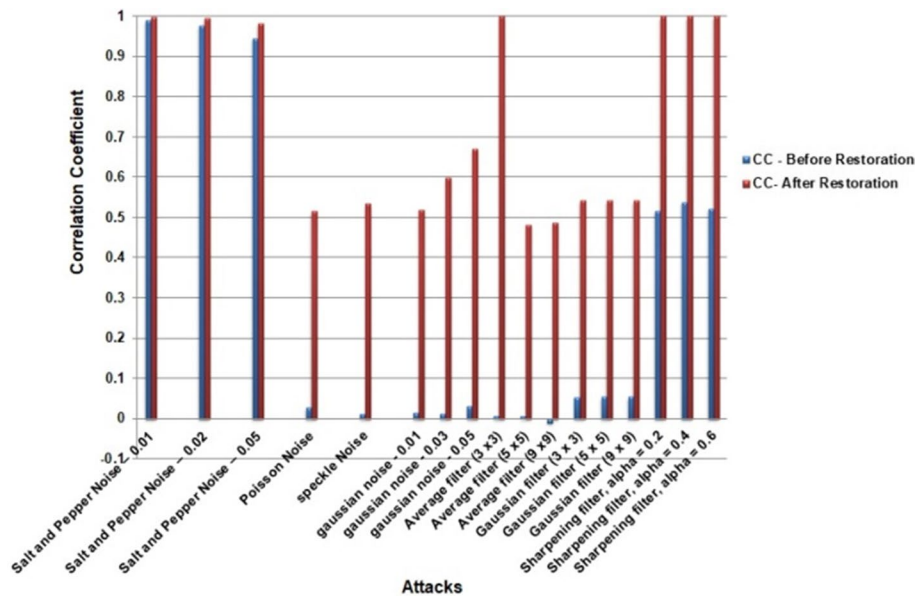


Fig. 9 Attacks vs. visual metrics—correlation coefficient

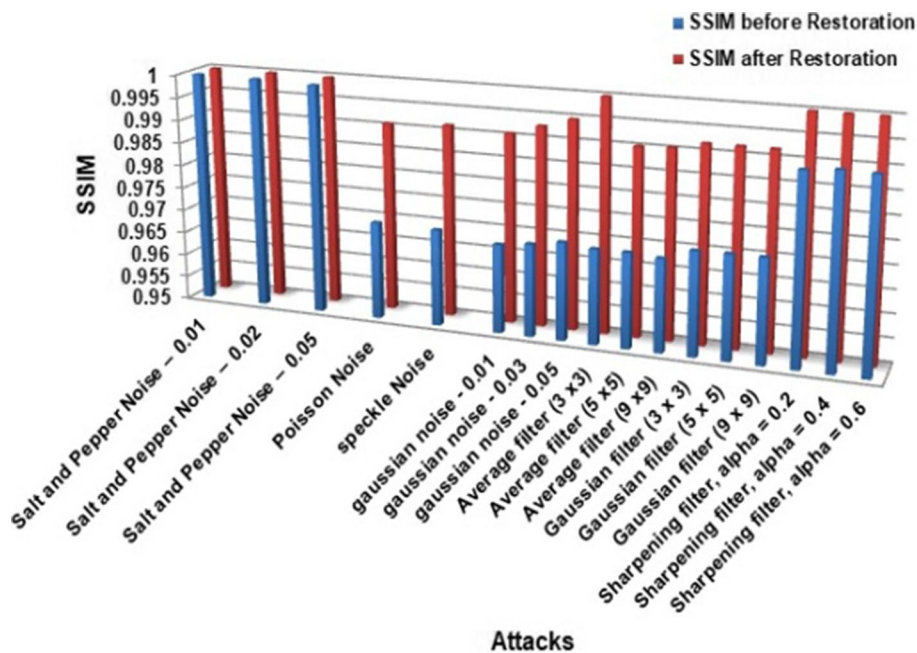


Fig. 10 Attacks vs. visual metrics—SSIM

watermark bits can authenticate the tampered images without recovering them since the purpose of watermarking is to provide image authentication.

In [3] tampering of Lena  $512 \times 512$ —the grayscale image at 6.84% leads to a PSNR of 44.16 dB and the recovered image has the PSNR of 46.37 dB which at the embedding mode (6, 2). In Table 4 the proposed method is compared with the particular references [3, 22, 31], and [32] because all these existing methods are purely based

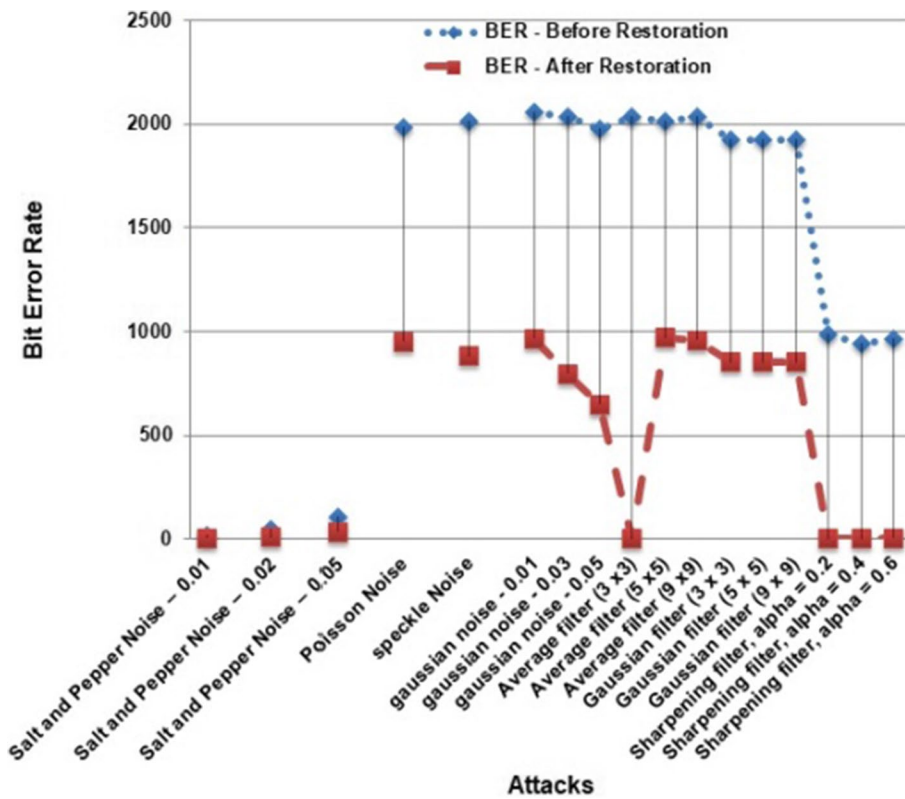


Fig. 11 Attacks vs. bit error rate

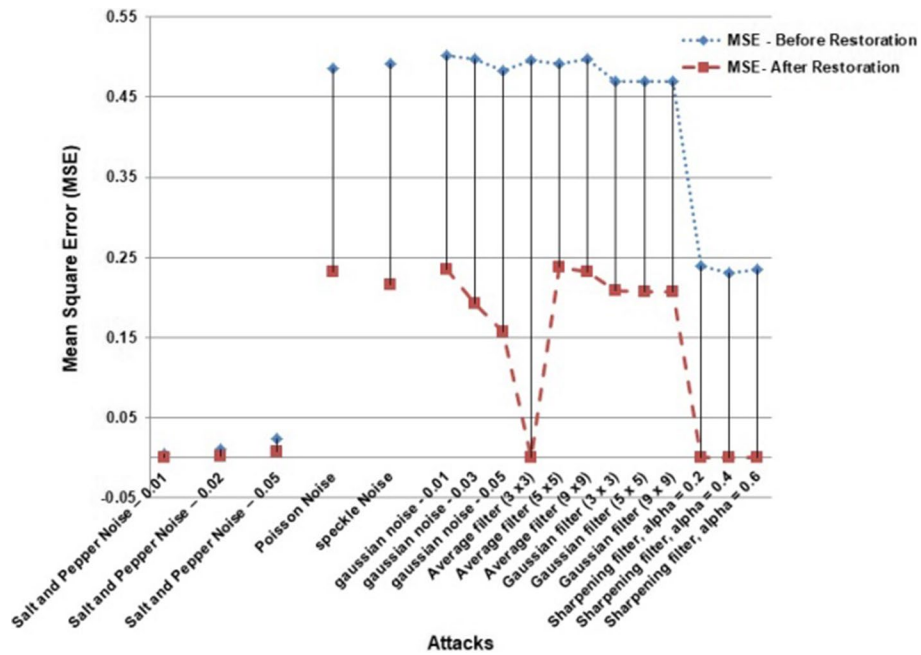
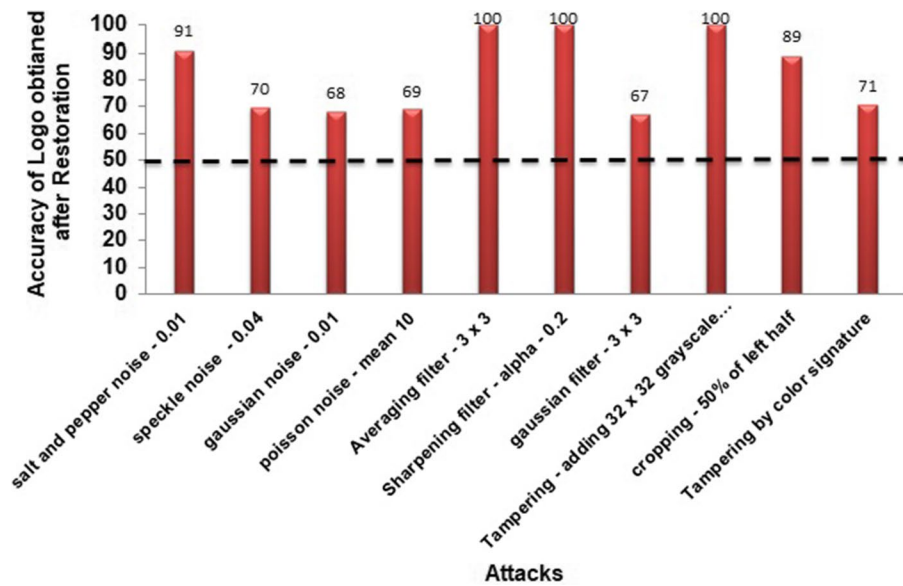


Fig. 12 Attacks vs. mean square error



**Fig. 13** Attacks vs. accuracy of logo obtained after restoration

on spatial domain image watermarking technique as the proposed work, in which the PSNR metric is calculated depending upon the different significant bits i.e. from ISB to LSB. In a similar manner, the existing techniques calculated PSNR metric after restoration technique from tampering attack.

**8.9 Comparison of statistical performance with the existing methods**

In [33], the confusion matrix and its analysis were carried out to find the TPR (true positive rate) and FPR (false positive rate) to check the quality of the proposed work. Similarly, for the proposed work statistical performance was carried out. The confusion matrix was constructed and is shown in Table 5.

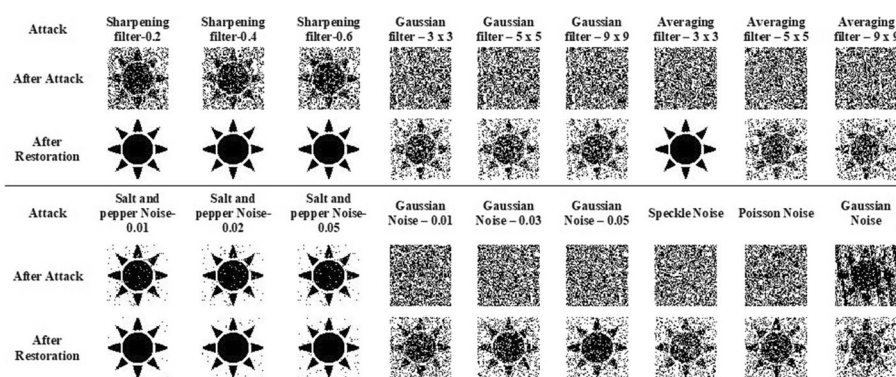
The formula for TPR and FPR is calculated from [18] and it is given in Eqs. (19) and (20):

$$\text{Truepositiverate(TPR)} = \frac{TP}{TP + FN}, \tag{19}$$

$$\text{Falsepositiverate(FPR)} = \frac{FP}{FP + TN}. \tag{20}$$

Using the above confusion matrix, Eqs. (19) and (20), Table 6 values are calculated for the proposed work and compared with the existing works.

In Table 6 the statistical parameters TP, TN, FP FN, TPR and FPR are calculated for the proposed work to check the performance of the proposed watermark embedding and blind recovery using ESP algorithm with the other existing methods in [4], [33], [34] and [35]. In the existing methodologies similar statistical parameters were used to analyze the watermarking system, so these reference were chosen for comparison. From Table 6 it is evident that TPR is higher and FPR is lower for the proposed methodology



**Fig. 14** Attacks and recovery of Logo2 before and after restoration

than all other existing methods in [4], [33], [34] and [35]. So the proposed methodology is better than the other existing methodologies.

The proposed system is compared with Chun-Chi Lo et al. [4], and Zhaoxia Yin et al. [35]. It is found that the TPR value is high and the FPR value is very less compared with all the other existing methodologies, which confirms that the proposed ESP algorithm and the watermarking scheme is better than the other existing schemes. The receiver operating characteristics (ROC) curve is drawn in Fig. 15 for the 10 standard grayscale images and it is shown that the area under the ROC is nearly equal to unity. Similarly, raw RGB color images (17.png images and 10 raw.tif) were also analyzed with the ESP algorithm and the proposed watermarking methodology. The comparison of the proposed work is carried out with the standard Lena.tif (512 × 512 × 3) image and is shown in Table 7.

In Table 7, the proposed method is compared with [11, 13, 16, 22] and [34] existing methods because in these existing methods spatial domain watermarking on color images are focused. The proposed work has excellent image subjective quality than the other mentioned existing methods.

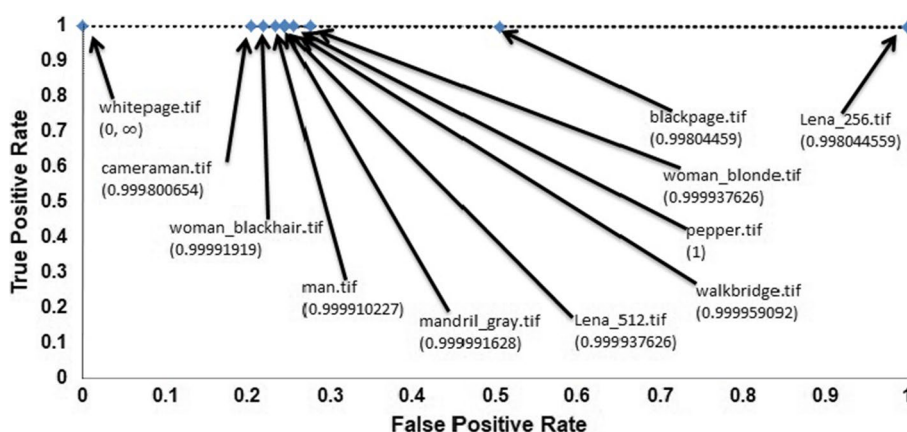
Jobin Abraham and Varghese Paul in [13] used masks to adjust the color variation after watermark embedding and the same Logo2 was used in embedding but the PSNR was very low compared with the proposed work and in this work, there is no need for such mask. The work is done in [11] and [16] also does not require such a mask, the proposed ESP algorithm and watermark embedding scheme provides very high PSNR at the LSB level. The PSNR 69.1941 dB is achieved when the Logo2 is embedded in the 4<sup>th</sup> bit plane of Lena image of size (512 × 512).

### 9 Conclusion

Blind and semi-fragile spatial domain watermarking is proposed for image authentication. The ESP algorithm is developed with fixed initial values and a secret key. The points of intercept, of GS and AS make the algorithm to be more secured where the confusion probability will be more. It is difficult for the intruder to identify the watermark presence in the host image since the logo is embedded appending the Diffie–Hellman key exchange protocol with the ESP algorithm. According to the proposed methodology embedding the logo is better in the 4th bit plane for the raw images and the 5th-bit plane

**Table 6** Comparison of statistical parameters with the existing methodologies

Methods	TP	TN	FP	FN	TPR	FPR
Proposed method—4th bit plane embedding (Logo1)— $32 \times 32$	1,032,497	1,064,187	178	290	0.99971921	0.000167218
Proposed method—4th bit plane embedding (Logo1)— $64 \times 64$	1,031,516	1,063,587	778	1271	0.99876935	0.000730614
Proposed method—4th bit plane embedding (Logo2)— $64 \times 64$	1,032,089	1,063,021	1344	698	0.99932416	0.001263492
Yinyin Peng et al. Watermarking1, [33]	3561	258,425	59	99	0.9730	0.00023
Yinyin Peng et al. Watermarking2, [33]	3568	258,432	52	92	0.9749	0.00021
Chun-Chi Lo et al. [4]	3171	258,391	93	489	0.8664	0.00036
Zhaoxia Yin et al. [34]	3323	258,319	165	337	0.9079	0.00064



**Fig. 15** ROC curve using proposed system

for compressed images, where the authentication could be done perfectly. The proposed ESP spreads over the entire region of the host image, so the image authentication could be done from any corner of the image. The image authentication is tested by sending the WI in the E-mail, WhatsApp, and Facebook. It is observed that using this proposed method, image authentication in E-mail and WhatsApp can be done perfectly with 100% accuracy the SSIM of the original Logo and recovered Logo is unity. In FB, to obtain better image authentication, the embedding is done in the 5th-bit plane of the host image, because after downloading the WI from the FB the WI is in the compressed format. So the image authentication is done with more accuracy. Image tampering attacks are done on the WI with the tampering attack ranging from 0.59 to 95%, the proposed work provides the PSNR of the watermark logo in the range [81.2441 to 52.9996] dB. The proposed work is robust to JPEG compression from it can withstand up to 7:1 compression ratio as given in Table 2. Similarly, the work is robust to tampering, image cropping, salt-and-pepper noise, sharpening filter, semi-robust to Gaussian filtering, rotation ( $1^\circ$ ), and image resizing, and fragile to other geometrical attacks. Logo detection is 100% after averaging filter attack, tampering WI with  $32 \times 32$  grayscale image attack, and sharpening filter attack. The average accuracy of logo detection is more than 65% for all the attacks. The proposed ESP algorithm and the watermark embedding scheme provide



**Table 7** Comparison of color images with the existing methods

Parameters	Huynh-The et al. [11]	Jobin Abraham and Varghese Paul [13]	Liu [16]	Sinhal [22]	Yaun [34]	Proposed method
Size of host image/type	512 × 512	512 × 512	512 × 512	512 × 512	512 × 512	512 × 512
Size of watermark	64 × 64	64 × 64	Image features	2 × 4 blocks	32 × 32 × 3	3 × 64 × 64 (Three Logos)
Domain of operation	Transform domain	Spatial domain	Spatial domain	Spatial domain	Spatial and Frequency domain	Spatial domain
Embedding color frame	Red, green, and blue	Blue	Red, green, and blue	RGB to gray conversion	Red, green, and blue	Red, green, and blue
PSNR (dB)	43.51	47.6	39	49.62	44.4928	69.1941
Image subjective quality	Good	Superior	Good	Good	Good	Excellent
Adjustment of color variations	No	Yes	No	No	No	No

higher imperceptibility, security, and robustness to the raw and compressed grayscale images. Similar to the RGB images, it offers higher imperceptibility with a higher payload and the logo recovery rate is very high. Overall, the proposed methods provide the best image authentication compared with the other existing methods.

## 10 Future scope

The proposed work is handcrafted over different image data set of various sizes and it is working well for the grayscale images and also with the color images, but the downloaded colored watermarked images from the FB give poor authentication. After embedding the watermark logo in all three color frames separately, the PSNR between the host image and FB\_WI is 45 dB which is acceptable. But the authentication is not satisfactory for the author, where the SSIM is very low. The downloaded watermarked image from FB is checked with the original WI image, it is observed that about 48.19% of pixels are affected in FB color image. So another spatial watermarking method is to be developed for color images to maintain authentication in FB. Deep Neural Networks (DNN)-based spatial domain watermarking with the handcrafted ESP algorithm is the future scope of this proposed work.

### Abbreviations

*.jpeg	Joint Photo Experts Group—Image Format
*.jpg	Joint Photo Graph—Image Format
*.png	Portable Network Graphics—Image Format
*.tif	Tagged Image File
*.tiff	Tagged Image File Format
AS	Arithmetic sequence
BER	Bit error rate
BRISQUE	Blind/referenceless image spatial quality evaluator
CC	Cross correlation
dB	Decibels
DHKEP	Diffie–Hellman key exchange protocol
ESP	Euclidean space points—algorithm developed for the proposed work

FB	Facebook
FN	False negative
FP	False positive
FPR	False positive rate
GS	Geometric sequence
I(M, N)	Input image, of size M—rows and N—columns
ISB	Intermediate significant bit
JPEG	Joint Photograph Experts Group
KB	Kilo byte
LSB	Least significant bit
MSB	Most significant bit
MSE	Mean square error
NIQE	Natural image quality evaluator
POI	Point of intercept
PSNR	Peak signal-to-noise ratio
RGB	Red green and blue frames—from a color image
ROC	Receiver operating characteristics
SSIM	Structural similarity
TN	True negative
TP	True positive
TPR	True positive rate
WI(M, N)	Watermarked image of size M, N

### Acknowledgements

I extend my sincere thanks and gratitude to Dr. P. Suhail Parvaze, Ph. D, IIT Madras, and Research Consultant for Philips India, for his valuable suggestions and to improve the quality of the paper.

### Author contributions

Contribution of the first author: designed, developed and MATLAB implementation of the three modules they are (i) new ESP algorithm (ii) DHKEP, and the watermarking system. (iii) Testing and analysis. Contribution of the second author: (i) discussed the literature survey and its outcomes (ii) suggested the test to send in Email, WhatsApp and Facebook. (iii) Watermark restoration process. Both authors read and approved the final manuscript.

### Funding

The proposed work was not applied to any of the organization, so there is no funding applicable for this work.

### Availability of data and materials

MALTA Coding – Individually for Every Image Set.

Image Data Set (\*.tiff, \*.tif, \*.png, \*.jpg).

Example of the Proposed ESP Algorithm and Complete Quality Metric Analysis of images.

### Declarations

#### Competing interests

Image authentication scheme [35] is proposed using Hilbert curve mapping which is complex instead of that the authors proposed simple ESP algorithm using geometric and arithmetic sequences with added security.

Compared with [35] our system is simple, semi-robust and secure.

In RGB watermarking, Jobin Abraham and Varghese Paul [13] used spatial mask to recover the distorted Red and Green Frames, In this work No such Spatial Masks are required.

The False Positive Rate of the proposed system is less compared with [3, 33] and [35] works.

Received: 31 July 2021 Accepted: 15 August 2022

Published online: 23 September 2022

### References

1. Anish M, Anush KM, Alan CB (2011) Blind/Referenceless Image Spatial quality Evaluator”, a Conference Record of the Forty Fifth Asilomar Conference on Signals, Systems, and Computers (ASILOMAR – 2011) – IEEE Xplore–2012, P 723–727. <https://doi.org/10.1109/ACSSC.2011.6190099>.
2. I.P. Christine, J.D. Edward, Digital Watermarking: Algorithm and Application. IEEE Signal Process. Magaz. (2001). <https://doi.org/10.1109/79.939835>
3. C. Qin, H. Wang, X. Zhang, X. Sun, Self-embedding fragile watermarking based on reference-data interleaving and adaptive selection of embedding mode. Inf. Sci. **373**(2016), 233–250 (2016). <https://doi.org/10.1016/j.ins.2016.09.001>
4. C.-C. Lo, Hu. Yu-Chen, A novel reversible image authentication scheme for digital images. Signal Process. **98**, 174–185 (2014). <https://doi.org/10.1016/j.sigpro.2013.11.028>
5. P.M. Dipti, M. Subhamoy, T.A. Scott, Spatial domain Watermarking of Multimedia object for Buyer Authentication. IEEE Trans. Multimed. **6**(1), 1590–9210 (2004). <https://doi.org/10.1109/TMM.2003.819759>
6. Discrete Mathematics: An Open Introduction: [http://discrete.openmathbooks.org/dmoi2/sec\\_seq-arithgeom.html](http://discrete.openmathbooks.org/dmoi2/sec_seq-arithgeom.html)

7. G. Voyatzis, I. Pitas, Protecting Digital-Image Copyrights: A Framework. January/February **19**, 18–24 (1999). <https://doi.org/10.1109/38.736465>
8. C.L. Gerhurd, S. Iwan, L.L. Reginaid, Watermarking digital image, and video data – a state of the art overview. *IEEE Signal Process. Magaz.* (2000). <https://doi.org/10.1109/79.879337>
9. W. Hong, T.S. Chen, A novel data embedding method using adaptive pixel pair matching. *IEEE Trans. Inform. Foren. Secur.* **7**(1), 176–184 (2012). <https://doi.org/10.1109/TIFS.2011.2155062>
10. H.-C. Chen, Y.-W. Chang, R.-C. Hwang, A watermarking algorithm. *J. Inf. Optim. Sci.* **32**(3), 697–707 (2011). <https://doi.org/10.1080/02522667.2011.10700081>
11. T. Huynh-The, O. Banos, S. Lee, Y. Yoon, T. Le-Tien, Improving digital image watermarking by means of optimal channel selection. *Expert Syst. Appl.* **62**(2016), 177–189 (2016). <https://doi.org/10.1016/J.ESWA.2016.06.015>
12. ImageProcessingPlace.com. [http://www.imageprocessingplace.com/root\\_files\\_V3/image\\_databases.htm](http://www.imageprocessingplace.com/root_files_V3/image_databases.htm).
13. A. Jobin, P. Varghese (2019) An imperceptible spatial domain color image watermarking scheme. *J. King Saud Univ. Comput. Inf. Sci.* **31**(1), 125–133. DOI <https://doi.org/10.1016/j.jksuci.2016.12.004>.
14. S. Kostopoulos, A.M. Gilani, A.N. Skodras. Color image authentication based on a self-embedding technique. In: 14th International Conference on Digital Signal Processing Proceedings. (2002) DOI: <https://doi.org/10.1109/ICDSP.2002.1028195>.
15. L. Lei-Doa, G. Bao-Long, Localized image watermarking in spatial domain resistant to geometric attacks. *Int. J. Electron. Commun.* **63**(2), 123–131 (2009). <https://doi.org/10.1016/J.AEUE.2007.11.007>
16. Liu, K.C., (2012). Color image watermarking for tamper-proofing and pattern-based recovery. *IET Image Proc.* **6** (5), 2012, pp. 445–454. DOI: <https://doi.org/10.1049/IET-IPR.2011.0574>
17. M. Kutter, F.A.P. Petitcolas, A fair benchmark for image watermarking system, *Electronic Imaging '99, Security and Watermarking of Multimedia Contents*, vol. 3657, Sans Jose, CA, USA, 25–27. *Int. Soc. Opt. Eng.* **1999**, 1–14 (1999)
18. Machine Learning Crash Course. <https://developers.google.com/machine-learning/crash-course/classification/accuracy>
19. MathWorks. [https://in.mathworks.com/help/images/ref/psnr.html#bt5uhgi-2\\_1](https://in.mathworks.com/help/images/ref/psnr.html#bt5uhgi-2_1)
20. N. Nikolaidis, I. Pitas, Robust image watermarking in the spatial domain. *Signal Process.* **66**(1998), 385–403 (1998)
21. Su. Qingtang, Y. Niu, A blind color image watermarking based on DC component in the spatial domain. *Optik Int. J. Light Elect. Optics* **124**(23), 6255–6260 (2013). <https://doi.org/10.1016/J.IJLEO.2013.05.013>
22. R. Sinhal, I.A. Ansari, C.W. Ahn, Blind Image Watermarking for Localization and Restoration of Color Images. *IEEE Access* **8**, 200157–200169 (2020). <https://doi.org/10.1109/ACCESS.2020.3035428>
23. S. Dadkhah, A.A. Manaf, Y. Hori, A.E. Hassanien, S. Sadeghi, An effective SVD – based image tampering detection and self-recovery using active watermarking. *Signal Process.* **1197–1210**, 0923–5965 (2014). <https://doi.org/10.1016/j.image.2014.09.001>
24. B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd edn. (Wiley, New York, 2016), pp.513–516
25. S.A. Parah, J.A. Sheikh, U.I. Assad, G.M. Bhat, Realisation and robustness evaluation of a blind spatial domain watermarking technique. *Int. J. Electron.* **104**(4), 659–672 (2017). <https://doi.org/10.1080/00207217.2016.1242162>
26. The Lab Book Pa. <http://www.labbookpages.co.uk/software/imgProc/otsuThreshold.html>
27. T. Kalker, Considerations on Watermarking security, *IEEE Fourth Workshop on Multimedia Signal Processing*, IEEE Xplore: 07th August 2002. *IEEE* **2001**, 201–206 (2002). <https://doi.org/10.1109/MMSP.2001.962734>
28. UChicago REU 2013 Apprentice Program: Prof. Babai, Lecture 16, July 23<sup>rd</sup>, 2013, Axioms of Euclidean Space. <https://home.ttic.edu/~madhurt/courses/reu2013/class723.pdf>
29. H. Wang, Q. Su, A color image watermarking method combined QR decomposition and spatial domain. *Multimed. Tools Appl.* (2022). <https://doi.org/10.1007/s11042-022-13064-y>
30. Wolfram Math World. <https://mathworld.wolfram.com/Diffie-HellmanProtocol.html>
31. X. Zhang, S. Wang, Fragile watermarking with error-free restoration capability. *IEEE Trans. Multimedia* **10**(8), 1490–1499 (2008). <https://doi.org/10.1109/TMM.2008.2007334>
32. X. Zhang, S. Wang, Z. Qjan, G. Feng, Reference Sharing Mechanism for watermark self-embedding. *IEEE Trans. Image Process.* **20**(2), 485–495 (2011). <https://doi.org/10.1109/tip.2010.2066981>
33. Y. Peng, X. Niu, Fu. Lei, Z. Yin, Image authentication scheme based on reversible fragile watermarking with two images. *J. Inf. Secur. Appl.* **40**, 236–246 (2018). <https://doi.org/10.1016/J.JISA.2018.04.007>
34. Z. Yuan, Q. Su, D. Liu et al., A blind image watermarking scheme combining spatial domain and frequency domain. *Vis. Comput.* **37**, 1867–1881 (2021). <https://doi.org/10.1007/s00371-020-01945-y>
35. Y. Zhaxoia, N. Xuejing, Z. Zhili, T. Jin, L. Bin, Improved reversible image authentication scheme. *Cogn. Comput.* **8**, 890–899 (2016). <https://doi.org/10.1007/S12559-016-9408-6>
36. W. Zhou, C.B. Alan, R.S. Hamid, P.S. Eero, Image quality assessment: from error visibility to structural similarity. *IEEE Trans. Image Process.* **13**(4), 600–612 (2004). <https://doi.org/10.1109/TIP>

## Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

**Shaik Hedayath Basha** Working as Asst. Professor in RMK College of Engineering and Technology, department of Electronics and Communication Engineering, Chennai, India. Having 15 years of teaching Experience. Completed Bachelor Degree under Madras University, Chennai. Bagged two Master degrees, one in Applied Electronics from Satyabama University, Chennai and the other in Digital Electronics and Communication Systems from JNTU, Anantapuramu, Anantapur, Andhra Pradesh. Pursing Ph.D from Anna University, Chennai. Published 10 International Journal papers, 3 International, and 3 Indian Conference. Area of interest is Image and Video Watermarking, Image Encryption, Image Analysis, Image Processing, and IoT.

**Jaion B** Working as Professor in RMK Engineering College, department of Computer Science and Engineering, Chennai, India. Having 22 years 7 Months of teaching Experience in that 5 years of Research experience is combined. Completed Ph.D, Bachelor and Masters in the years 2015, 2007, and 1996. Published 40 International Journal papers and attended many International, and Indian Conference. Area of interest is Data mining, Bioinformatics and Knowledge discovery, Image Analysis, Image Processing, IoT, and Cloud Computing.

**Submit your manuscript to a SpringerOpen<sup>®</sup> journal and benefit from:**

- ▶ Convenient online submission
- ▶ Rigorous peer review
- ▶ Open access: articles freely available online
- ▶ High visibility within the field
- ▶ Retaining the copyright to your article

---

Submit your next manuscript at ▶ [springeropen.com](https://www.springeropen.com)

---