Reversible Image Watermarking Using Modified Quadratic Difference Expansion and Hybrid Optimization Technique

H. R. Lakshmi[1]*, Surekha Borra[2]

[1] Department of ECE, K.S. Institute of Technology, Visvesvaraya Technological University, Belagavi, Karnataka (India)
[2] Department of ECE, K. S. Institute of Technology, Bangalore, Karnataka-560109, (India)

Received 13 October 2022 | Accepted 21 January 2022 | Early Access 4 August 2023

Abstract

With increasing copyright violation cases, watermarking of digital images is a very popular solution for securing online media content. Since some sensitive applications require image recovery after watermark extraction, reversible watermarking is widely preferred. This article introduces a Modified Quadratic Difference Expansion (MQDE) and fractal encryption-based reversible watermarking for securing the copyrights of images. First, fractal encryption is applied to watermarks using Tromino's L-shaped theorem to improve security. In addition, Cuckoo Search-Grey Wolf Optimization (CSGWO) is enforced on the cover image to optimize block allocation for inserting an encrypted watermark such that it greatly increases its invisibility. While the developed MQDE technique helps to improve coverage and visual quality, the novel data-driven distortion control unit ensures optimal performance. The suggested approach provides the highest level of protection when retrieving the secret image and original cover image without losing the essential information, apart from improving transparency and capacity without much tradeoff. The simulation results of this approach are superior to existing methods in terms of embedding capacity. With an average PSNR of 67 dB, the method shows good imperceptibility in comparison to other schemes.

Keywords

Cuckoo Search, Difference Expansion, Fractal Encryption, Grey Wolf Optimization, Information Security, Reversible Watermarking.

DOI: 10.9781/ijimai.2023.08.002

I. Introduction

Due to the rapid usage of mobile devices and the Internet, digital images are often captured, stored, and shared on social media [1] – [3], ultimately leading to several intellectual property rights issues [4]. To address these issues, digital watermarks are frequently employed for evidence of ownership, copyright protection, and integrity verification. The key components of the digital watermarking system are embedding and extraction [5] – [7]. In the case of invisible watermarking, the watermark (owner's identification data) is invisibly embedded into all the images belonging to an owner, so that the registered watermark can be extracted from the published watermarked images solely by the owner (using his secret key and extraction algorithm) to prove the ownership in case of ownership-related disputes [8] – [9]. In invisible watermarking, it is important to embed watermarks in images without affecting the quality of the images (ex: sensitive medical images, high-quality photographs, satellite images, military maps, product designs, etc.). The distortion brought on by watermarking is often restricted to ensuring that the watermark cannot be detected, making the host (original data) and the watermarked image visually identical. Hence, the imperceptibility requirement with respect to an invisible watermark implies that the perceptual quality of the watermarked images be kept high even after watermark embedding. In watermarking, the watermark can be of different types, ranging from simple text (Owner ID, time and date stamp, company name, etc.) to binary, grayscale, or color images (depending on the quality of the company logo). Further, there may be multiple owners for the image in some applications. For example, a certain medical image can be owned by the diagnostics center, the hospital, the radiologist, and the patient. In such a scenario, the application demands a large embedding capacity. While most of the existing watermarking techniques deal with robustness in the extraction process and imperceptibility after insertion, the general requirements for digital watermarks are simplicity, high embedding capacity, and security.

The transform domain approaches, which are typically complex, performed satisfactorily in terms of robustness and imperceptibility [10] – [12]. Spatial domain techniques, on the other hand, are relatively simpler, but the robustness of such schemes has fallen short. Irrespective of the embedding domain, which has been heavily used in the field of watermarking, some alterations are always applied to the cover picture when a hidden image is combined with it to generate a watermarked image. Even if they are little, these changes are undesirable in delicate applications like defense, forensics, medical imaging, etc. [13] – [14]. In reversible watermarking, the original host can be reversed from a published watermarked image after watermark

* Corresponding author.
E-mail address: hrl.lakshmi@gmail.com

Please cite this article in press as:
H. R. Lakshmi, S. Borra. Reversible Image Watermarking Using Modified Quadratic Difference Expansion and Hybrid Optimization Technique, International Journal of Interactive Multimedia and Artificial Intelligence, (2023), http://dx.doi.org/10.9781/ijimai.2023.08.002

extraction if required. There are many research opportunities in the field of reversible watermarks (RW), as they are suitable for applications containing sensitive images.

Least-significant-bit-based techniques are the earliest methods for reversible watermarking [15]. Contrarily, after extracting the watermark, the picture may also be reversed by modifying the coefficients of various transforms [16] – [18]. Several algorithms, including the Integer Wavelet Transform (IWT), the Riesz transform, the discrete wavelet transform (DWT), the discrete cosine transform (DCT), and the discrete Fourier transform (DFT), are used to convert the image into the frequency domain prior to embedding and extracting the watermark.

A few publications [19],[20] use singular value decomposition (SVD) to provide a strong framework against noise. The transform-domain reversible watermarking schemes discussed in the literature are proven to be more robust, but they are more complex and time-consuming [21]. While few reversible approaches require location maps [22], much research has been done to construct location maps from the host image, embed them with the watermark for later watermark extraction, and/or cover image recovery. The methodologies that use location maps are prediction error expansion (PEE) [23], histogram shifting [24], difference expansion (DE) [25],[26], integer transform [27], and hybrid techniques (combination of two or more techniques) [28],[29]. The primary goal of such strategies is to improve embedding capacity.

This article introduces a hybrid reversible image watermarking method that improves embedding capacity along with transparency and security. This study makes the following improvements to the existing reversible watermarking methods, in addition to leveraging fractal encryption to increase security:

- Hybrid soft computing using Cuckoo search and grey wolf optimization (CSGWO) is employed to determine where in the image a watermark should be embedded to ensure a higher convergence rate and visual quality.
- A novel distortion control unit is proposed to ensure imperceptibility and optimal embedding. The fitness function incorporates 3-SSIM, PSNR, cross entropy (CE) for optimal location finding in the embedding process.
- Modified quadratic difference expansion (MQDE) method to embed and extract high-capacity watermarks.

The study is organized as follows: The earlier research in the fields of difference expansion-based reversible watermarking and reversible watermarking employing optimization approaches is covered in Section II. In Section III, the preliminaries are explained. In Section IV, the suggested model is explained in detail. The experimental assessment of the suggested model is covered in Section V; Section VI provides a discussion on the performance; and Section VII provides the conclusion.

II. Literature Review

The necessity of striking a compromise between picture quality and embedding capacity in watermark methods is well demonstrated by researchers. Soft computing approaches and optimization techniques are often used to reduce the trade-off problem and to select pixel positions, blocks, or thresholds for the overall performance improvement of RW.

This study is based on difference expansion (DE)-based techniques, which Tian et al. [30] initially presented to have visual quality and satisfactory embedding capacity. A pair of pixels is chosen for one bit of secret information, based on some criteria related to the difference in their pixel values. A location map may be embedded as auxiliary data along with the secret information. Tian et al. [26] later proposed a non-compression method for masking watermark data, taking advantage of the similarity in successive pixels and increasing the value of the difference. Tzu et al. [31] proposed a lossless scheme wherein each host image pixel is split into 4-bit parts, where the nibble pairs between adjacent pixels are used for embedding the secret information. This method claims high payload capacity and full reversibility. The difference expansion method based on triplets [32] provides much more information hiding capacity, as each of the selected triplets can hide two bits of watermark. The results showed that the computational cost is comparatively less than most of the transforms, as it uses a total of only 10 additions and 6 shift operations for embedding and extraction with minimal alteration of embedding coefficients. To obtain a large payload capacity with little picture distortion, Alattar [33] explored pixel vector-based difference expansion, where a feedback system modulated the payload to be added based on the required quality. The method supports hiding data in color images and recursive embedding to increase capacity. Blocks (3×3) of the host image are classified into various categories based on their structure [34]. The variance between each block is computed, and data is embedded in each block accordingly. Secret bits and auxiliary data are embedded in separate parts of the image. Secret data is embedded by utilizing the method proposed by Alattar [33], and the auxiliary information is inserted using the substitution of LSB. Hu et al. [35] used Haar-based transforms to embed bits in both horizontal and vertical directions to increase payload capacity. A dynamic approach for pixel selection ensures balance between both embedding directions such that only the small difference values are used for embedding, thus reducing distortion.

Difference expansion (DE) schemes mostly use regions where the pixel values are similar, thus limiting the capacity. A DE-based scheme put forth by Maniriho et al. [36] has an additional mod-based function to allow for embedding pairs with both positive and negative differences. If the difference is less than 2 and greater than -2, then those pixels are chosen for embedding, thereby increasing the embedding capacity. A reduced difference expansion [37] entails selecting difference values for embedding and further reducing them before inserting payload to increase embedding capacity. Another reduced-difference expansion [38]-based scheme is put forth to increase the capacity further by embedding payload into non-changeable pixels, which in other methods were not used for embedding. Variable block size was also used in the method for capacity-based processing. Only the index of the first pixel of the variable pair is contained in the decreased size of the location map [39]. Two rounds of differential expansion are employed to increase embedding capacity.

An adaptive difference expansion (ADE) method, which typically uses a few well-known parameters for watermarking and extraction, was proposed by H.S. El-sayed et al. [40]. This technique greatly expands the embedding capacity and demonstrates the superiority of watermarked photos over many other techniques. S. Weng, et al. [41] presented an optional embedding scheme (OES) to lower the distortion based on the requirements. DE is utilized for embedding by default, and adaptive embedding fulfils the requirement of a large embedding rate with low local variance. In addition to achieving respectable performance at all embedding rates, using a local smoothness estimator and four prediction frameworks increases the number of pixels that can be embedded. Z. Zhang et al. [42] developed a quadratic difference expansion-based method for enhancing the visual quality and embedding rate. Following the first omission of the pixel points with 0 and 255 greyscale values, linear difference expansion (LDE) is used to add half of the jumbled data to the cover picture. The Quadratic Difference Expansion (QDE) is used to incorporate the remaining secret data into the previously created picture. The final watermarked

picture is generated after appending the greyscale pixel values of 0 and 255. The results and simulation section showed that the technique resulted in high visual quality and embedding rates.

A computationally less expensive scheme was proposed [43] by combining downscaling and data hiding. The scheme proposed an adaptive adjustment of the capacity-quality trade-off for improved performance. It was suggested that the capacity be increased via a reversible DE technique [44]. The host image and the secret data were both encoded, and the secret was inserted in relation to a parameter representing the acceptable range of difference values. Wang [45] proposed a DE-based scheme that works bidirectionally. The pixel arrangement for data insertion is unlike other schemes, following a unique pattern. A cluster-based DE scheme [46] aimed at improving the payload capacity Upper and lower bounds are assigned, and clusters are accordingly formed. The difference expansion parameters are calculated based on the bounds and the cluster in question. Prediction error-based reversible data hiding (RDH) [47] was proposed, where data is embedded in forward and backward directions to improve capacity, and a block size 1×3 was chosen for embedding to improve the visual quality.

A few hybrid schemes used nature-inspired algorithms to optimize and improve performance parameters such as capacity and visual quality [48],[49]. The optimal brightness fitness function value was determined iteratively by the Firefly Technique (FA) [50] before secret information was embedded in the database using a DE-based algorithm. Over the earlier designs, it was observed that with this method, there was less distortion and a higher capacity. Particle Swarm Optimization (PSO) is employed for the selection of the appropriate threshold value and subsequently for the reduction of distortion in reversible watermarking based on 2D difference expansion and wavelet transform [51]. Results showed better PSNR in comparison to previous schemes. The interpolation-based expansion scheme [52] used the genetic algorithm (GA) and PSO to estimate the neighboring pixels and concluded that GA gave better results than PSO. Improvement in visual quality with respect to mean square error (MSE) and PSNR was observed [53] when embedding regions were selected using the Firefly algorithm in the DWT domain. Arnold transformation was used for watermark encryption [54] to increase the security of the reversible watermarking (RW) scheme. Both the secret image and the cover image were color images. To increase PSNR and MSE values, the strength factor is adjusted using Grey Wolf Optimization (GWO), while the secret information is incorporated using the SVD lifting procedure. The method's resilience has been successfully demonstrated for salt and pepper noise, Poisson noise, and set partitioning in hierarchical trees (SPIHT) compression.

A blind, reversible methodology that Zarrabi et al. [55] presented involves iteratively embedding the data into non-regions of interest (NROI). During embedding and extraction, ROI is identified and excluded using deep neural networks: one for segmentation and the other for classification. The resulting DCT domain scheme is lossless but not robust. A fragile reversible watermarking system based on SVD and PSO presented by Frank et al. [56] allows for dynamic capacity modification based on the desired embedding rate. Keeping the ROIs unchanged after automatic detection resulted in better quality than traditional transform domain schemes. Arsalan et al. [57] proposed using genetic programming (GP) and the integer wavelet transform (IWT) to solve the overflow and underflow problems and find the best wavelet coefficients to embed. The balance between capacity and quality is significantly reduced as companding is used for watermark insertion.

Balasamy et al. [58] developed a DWT and PSO-based method to protect medical images to find the optimal wavelet coefficients for data insertion. The approach does not produce any further data to aid in enhancing embedding capability; however, the visual quality produced is inadequate when compared to other schemes. Using Tian's DE [26], Vargas [59] created an intelligent RW scheme using a genetic algorithm (GA) to enhance the visual quality and choose the best threshold value for embedding. While simple DE is applied to 4×4, 8×8, 16×16 blocks of cover image for evaluation, the fitness function is based on MSE. Since the RW scheme is completely reversible, ROI calculations are not needed. However, embedding multiple times may lead to a smoothing effect, which is undesirable. A DWT-based RW scheme was proposed using hybrid optimization, combining two algorithms—the Tunicate Swarm Algorithm (TSA) and Simulated Annealing (SA)—for optimizing the scale factor and a deep recurrent neural network with long short-term memory (RNN-LSTM) for extraction. The authors claimed better robustness in comparison with using individual optimization schemes [60]. Ayad et al. [61] proposed a medical image watermarking approach using DWT and SVD with a text watermark encoded using QAM-16. The results showed better robustness and quality in comparison with non-hybrid schemes and were resilient against salt and pepper, and Gaussian noise. However, geometric attacks may hamper watermark detection and decoding. Kaur et al. [62] proposed a compression technique for color images using Fast Fourier Transform (FFT) compression and for optimizing 3 thresholds using the Intelligent Water Drop (IWD) algorithm: 1 for each color, by using 10 nodes for each value. The evaluation showed better SSIM values in contrast to manually chosen threshold values.

To summarize, the general measures that were taken by the researchers to improve embedding capabilities are: 1. Reduction and shrinking of the location map dimension. 2. Repeated use of DE to improve payload. 3. Make every effort to do away with the necessity for location maps. To enhance the image quality, the actions taken are: 1. Use of thresholds whose values define quality 2. Selection of the smallest (smoothest) difference-valued area of the image for embedding. However, there is an inherent trade-off between capacity and quality in the existing schemes.

This paper presents a RW technique to simultaneously meet many requirements: large embedding capacity, high security, high reversibility, high imperceptibility, and an improvement in robustness when compared to the recently published related works. The entropy value, payload, structural similarity index, and peak signal-to-noise ratio are the evaluation metrics used to track the performance of the suggested technique. While underflow and overflow are the major concerns faced by the researchers in RW schemes that degrade the system's performance, these issues are also addressed by the proposed scheme through the optimal selection of pixels using the distortion control unit.

III. Preliminaries

A. Linear Difference Expansion (LDE)

The LDE performs an integer transform on any picture pixel pair P=(s,t) to produce the difference d and mean m as stated in (1) and (2). Later, watermark bits (b) are inserted into the chosen pixel pairs of the host image.

$$d = s - t \tag{1}$$

$$m = \left\lfloor \frac{s+t}{2} \right\rfloor \tag{2}$$

The inverse transform is given in the Eqs. (5), (6).

$$s' = m + \left\lfloor \frac{d'+1}{2} \right\rfloor \tag{3}$$

$$t' = m + \left\lfloor \frac{d'}{2} \right\rfloor \tag{4}$$

The new value of difference is $d' = 2d + b$, where d is shifted to the left by one-bit b, which is the least significant bit, and is referred to as the Linear Difference Expansion (LDE). Pixel overflow results from using basic difference expansion to include hidden information or a watermark. This problem needs to be solved as the inverse transform of original pixel pairs s' and t' should fall in the range of [0, 255] for proper visibility. In addition, it is essential to limit d' as given in (5).

$$|d'| \leq (2(255 - m), 2m + 1) \tag{5}$$

B. Cuckoo Search–Grey Wolf Optimization (CSGWO)

This subsection describes how the proposed watermarking system uses the hybrid Cuckoo Search–Grey Wolf Optimization (CSGWO) algorithm to effectively select cover image pixels for watermarking while meeting the fitness function. The model combines the Grey Wolf Optimization (GWO), developed from grey wolf hunting activities [63], with a population-based algorithm called cuckoo search (CS), which uses the Levy Flight mechanism to update the new solutions (nests) in a pseudo-random manner. Thus, in the proposed method, the GWO metaheuristic incorporates CS to reinforce and increase its ability to avoid entrapment inside local optima and converge to the global minimum. The CS exploration skills are used to direct the wolves (or searching agents) to locations aided by the CS metaheuristic. In the CSGWO [64] algorithm, the GWO location update is modified to account for the CS update equation to get a faster convergence rate. The generalized equation of GWO is modified to update the position in the CSGWO algorithm, and therefore, an additional term is included in the numerator, as shown in (6) [65]:

$$\vec{G}(t+1) = \frac{\vec{G}_1 + \vec{G}_2 + \vec{G}_3 + \vec{G}_4}{4} \tag{6}$$

Where, $\vec{G}_4$ is the position vector projected using the CS update rule and $\vec{G}_1$, $\vec{G}_2$, $\vec{G}_3$ are the hunt agents according to the best hunt agent G_α, second and third best hunt agents G_β and G_δ [66]. Cuckoo search is a metaheuristic algorithm based on the reproductive performance of cuckoos. While each egg in the nest represents a problem that is solved more effectively, this activity is utilized to update positions in the proposed CSGWO algorithm using the $\vec{G}_4$ term, defined in (7) :

$$\vec{G}_4 = \vec{G}_t + \gamma \oplus Levy\ (\lambda) \tag{7}$$

Where $\vec{G}_t$ is the agent's position in the presenter petition, γ is the step size, which attains a value from 0 to 1. *Levy* (λ) is the Levy flight equation, which gives an arbitrary walk and is defined as $Levy \sim v = (t\text{–}\lambda)$, where λ is a constraint, whose values are in the interval [1, 3]. The addition of fourth term ($\vec{G}_4$) in proposed algorithm makes it more effective with the exploration of the search space of Levy flight.

C. Fitness Function Parameters

A gradient magnitude computation method [67] suggested that any image is composed of three regions, namely, edge, smooth, and texture, and that the segmentation is based on the threshold of the pixel gradient. Let g_{ij} represent the gradient of the original picture in (i, j) coordinates. The following guidelines form the basis for pixel categorization:

- If $g_{ij} > TH_1$, the pixel is deliberated as edge pixel.
- If $g_{ij} < TH_2$, pixels are processed as part of the smooth area.
- Otherwise, these pixels fall into the textured area.

Structural Similarity Index (SSIM): Since the luminous intensity of an object's surface is the result of reflection and illumination, it is preferable to eliminate the exposure effect to examine the images' structural information. The SSIM between two signals x and y is given by (8),

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_Y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \tag{8}$$

where μ_x and μ_y are the images x and y average intensities. σ_x and σ_y are variances, and σ_{xy} is the covariance of the two images. C_1 and C_2 are stabilizer variables that depend on the dynamic rank of the values of pixels [68].

3-SSIM: The value of 3-SSIM is calculated by comparing watermarked and original images using (9).

$$3\text{-}SSIM = A \times SSIM_{edge} + B \times SSIM_{smooth} + C \times SSIM_{texture} \tag{9}$$

where the weight factors of various regions are expressed by variables A, B and C. The notations $SSIM_{texture}$, $SSIM_{smooth}$ and $SSIM_{edge}$, indicate the SSIM values for the texture regions, smooth regions, and edge regions, respectively.

Normalized Capacity C_n: The normalized capacity of the inclusions (C_n) is calculated using (10) :

$$C_n = \frac{C_{wdc}}{C_{\frac{w}{odc}}} \tag{10}$$

where C_{wdc} and $C_{\frac{w}{odc}}$ indicate whether data can be masked with DC (distortion control) or without DC. It should be noted that the C_n falls between 0 and 1.

Cross Entropy (*CE*): Using the entropy definition, KL divergence [68], and log rules, cross entropy is defined in (11):

$$CE(p, q) = -\sum_{i=0}^{n} p(x_i) log\ (q(x_i)) \tag{11}$$

where p(x) is the watermarked image and q(x) is the original image.

Peak Signal to Noise Ratio (*PSNR*) (12):

$$PSNR = 10\ log_{10}\left(\frac{255^2}{MSE}\right) \tag{12}$$

$$MSE = 1/mn \sum_{x=0}^{m-1} \sum_{y=0}^{n-1} [I(s,t) - d(s,t)]^2 \tag{13}$$

where, the original input image is denoted as $I(s, t)$, the recovered image is denoted as $d(s, t)$, the rows and columns of the image are denoted as m and n, and MSE denotes mean square error.

D. Fractal Algorithm

Fractal encryption is a one-to-one encryption approach that depends on modulo operations. At the first stage of the proposed watermarking approach, fractal encryption of the watermark is performed to determine the recursive contract transformation of pixels. Fractal encryption has a strong key to encrypt pictures in the context of other encryption models because of the random and disordered nature of fractals. Attributes such as zoom level, iterations, and coordinates are utilized for generating the fractal image. In this technique, two keys are generated as in (14) and (15) for encryption and decryption processes using a random number that ranges between zero and one.

$$Key\ 1 = Random \times 25 + 4 \tag{14}$$

$$Key\ 2 = Key\ 1\ \times 2 \tag{15}$$

Fig. 1 (a) and (d) show the histograms of the cover image before and after embedding the encrypted watermark image. Results indicate that the histogram of the image is consistent after watermarking. Hence, no useful statistics about the watermark can be drawn by the attacker from the published watermarked image.

Fractal encryption, when combined with the L-shaped tromino theorem, enhances the security of image transmission [69]. L shaped tromino works based on two attribute symbols, "–" or "+", and degree $\theta = 90$. The L-shaped tromino is divided into smaller trominos based on the number of iterations, determined by the size of the watermark.

In Fig. 2, the first and second iterations of the L-shaped tromino are graphically depicted.

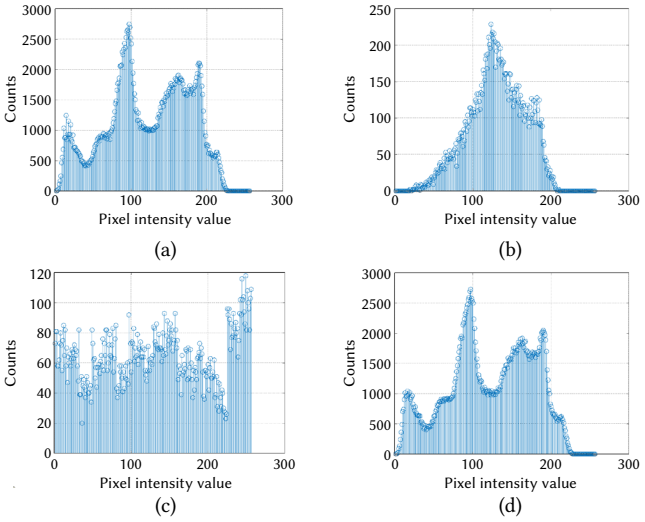


Fig. 1. Histogram graphs for (a) cover image, (b) watermark image, (c) fractal encrypted watermark and (d) watermarked cover image.

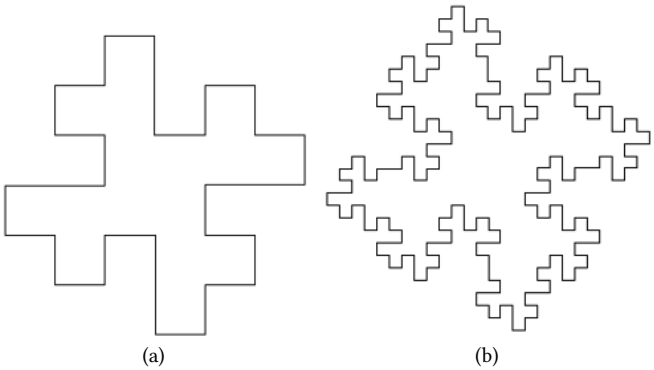


Fig. 2. (a) 1st iteration (b) 2nd iteration.

IV. Methodology

This section proposes a reversible hybrid image watermarking concept to support high-capacity (payload) secure watermarking while maintaining the visual quality of the watermarked image. This method also allows the original image to be recovered post watermark extraction. Fig. 3 shows the watermark embedding flow. The watermark image is first encrypted with the fractal encryption method to provide an extra layer of security. To safeguard data transfer with minimal system complexity, L-shaped fractal tromino-encryption is preferred. Furthermore, the best 8×8 blocks for watermark integration are selected by processing the host image using the Cuckoo search and grey wolf optimization (CSGWO) algorithm.

After exploration of the optimum location map in the host image by the CSGWO distortion control unit, modified quadratic difference expansion (MQDE) is applied for embedding the encrypted watermark to ensure better capacity and transparency. The result is a watermarked image, which can be safely published on the Internet. The embedded watermark can be extracted from the published watermarked images solely by the owner to prove ownership in cases of ownership-related disputes using his secret key and extraction algorithm.

Fig. 4 graphically shows the process of watermark extraction, where the watermarked image is initially subjected to inverse modified QDE according to the location map decided by the CSGWO distortion control unit to extract the encrypted watermark, which is later fed to a fractal decryption algorithm to finally extract the watermark and in parallel to recover the cover image from the lossy watermarked image. In the subsections that follow, each of the algorithms used in the embedding and extraction processes is discussed in detail, followed by a summary of the steps involved in applying these algorithms for the proposed reversible hybrid watermarking.

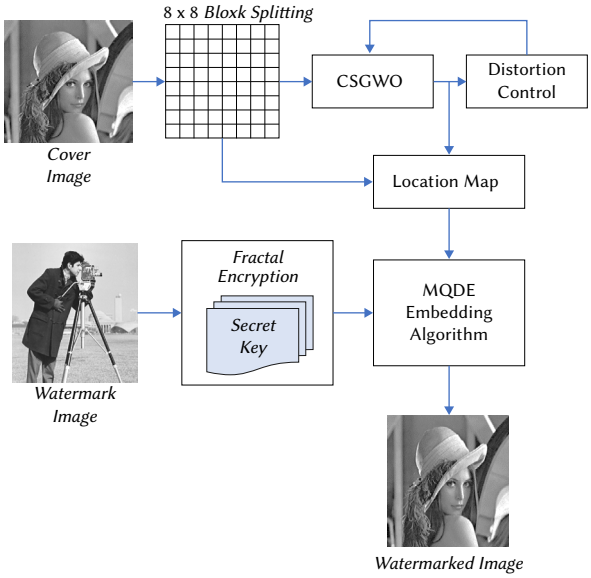


Fig.3. Watermark Embedding.

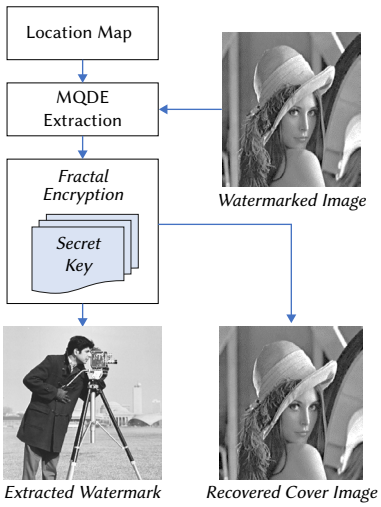


Fig.4. Watermark Extraction.

A. Modified Fitness Function

In the proposed method, the weighted sum of 3-SSIM, CE, PSNR and C_n defines the fitness function and is represented in (16)

$$F=(W_1 \times 3\text{-}SSIM)+(W_2 \times C_n)+\{W_3 \times (1-CE)\}+W_4 \times (PSNR) \quad (16)$$

The weights W_1, W_2, W_3 and W_4 must sum to 1 and are independently defined in (17) – (20)

$$W_1 = \frac{C_n \times (1-CE) \times PSNR}{3-SSIM\{C_n+(1-CE)\}+\{C_n \times (1-CE)\}+PSNR} \quad (17)$$

$$W_2 = \frac{3-SSIM \times (1-CE) \times PSNR}{3-SSIM\{C_n+(1-CE)\}+\{C_n \times (1-CE)\}+PSNR} \quad (18)$$

$$W_3 = \frac{(3-SSIM) \times C_n \times PSNR}{3-SSIM\{C_n+(1-CE)\}+\{C_n \times (1-CE)\}+PSNR} \quad (19)$$

$$W_4 = \frac{(3-SSIM)\times C_n\times(1-CE)}{3-SSIM\{C_n+(1-CE)\}+\{C_n\times(1-CE)\}+PSNR} \quad (20)$$

Replacing the values W_1, W_2, W_3 and W_4 in (16), the expression of the modified fitness function is represented as in (21).

$$F = \frac{4\{3-SSIM\times C_n\times(1-CE)\times PSNR\}}{3-SSIM\{C_n+(1-CE)\}+\{C_n\times(1-CE)\}+PSNR} \quad (21)$$

Starting with (14), the process continues until acceptable standard values are reached for the preferred iterations, or for 3-SSIM, PSNR, CE, and C_n.

Fig. 5 describes the steps involved in finding optimal location map using the modified fitness function obtained in the distortion control unit, to compensate for balancing hiding capacity, security, and imperceptibility in the proposed reversible watermarking.

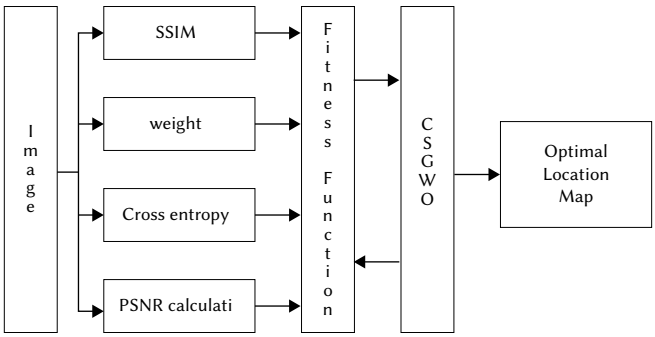


Fig.5. Distortion control unit.

B. Modified Quadratic Difference Expansion (MQDE)

The image pixel pairs s' and t' generated by difference transform in the preliminaries section using (3),(4) are utilized once again for performing quadratic watermark embedding that helps in improving the embedding capacity. The following process is mathematically stated in (1), (2), (5). d'' is the expanded difference.

$$d'' = \left[\frac{d''}{2}\right] + b \quad (22)$$

After embedding watermark using LDE, the generated watermarked image may overflow, and it returns to original image after performing modified QDE. Detailed process of modified QDE is given. Assuming the initial image pixel pair as $P = (s, t)$, the LDE process embed with the secret bit value b and the QDE process embeds the secret bit value b' using (23)-(29).

$$s' = \left[\frac{s+t}{2}\right] + \left[(s-t) + \frac{b+1}{2}\right] \quad (23)$$

$$t' = \left[\frac{s+t}{2}\right] - \left[(s-t) + \frac{b}{2}\right] \quad (24)$$

$$m = \left[\frac{s'+t'}{2}\right] = \left[\frac{\left[\frac{s+t}{2}\right]+\left[\frac{2(s-t)+1+b}{2}\right]+\left[\frac{s+t}{2}\right]-\left[\frac{2(s-t)+b}{2}\right]}{2}\right] \quad (25)$$

$$d = s' - t' = \left[\frac{2(s-t)+1+b}{2}\right] + \left[\frac{2(s-t)+b}{2}\right] \quad (26)$$

$$d'' = \left[\frac{\left[\frac{2(s-t)+1+b}{2}\right]+\left[\frac{2(s-t)+b}{2}\right]}{2}\right] + b' \quad (27)$$

$$s'' = \left[\frac{\left[\frac{s+t}{2}\right]+\left[\frac{2(s-t)+1+b}{2}\right]+\left[\frac{s+t}{2}\right]-\left[\frac{2(s-t)+b}{2}\right]}{2}\right] + \left[\frac{\left[\left(\frac{\left[\frac{2(s-t)+1+b}{2}\right]+\left[\frac{2(s-t)+b}{2}\right]}{2}\right)\right]+b'+1}{2}\right] \quad (28)$$

$$t'' = \left[\frac{\left[\frac{s+t}{2}\right]+\left[\frac{2(s-t)+1+b}{2}\right]+\left[\frac{s+t}{2}\right]-\left[\frac{2(s-t)+b}{2}\right]}{2}\right] - \left[\frac{\left[\left(\frac{\left[\frac{2(s-t)+1+b}{2}\right]+\left[\frac{2(s-t)+b}{2}\right]}{2}\right)\right]+b'}{2}\right] \quad (29)$$

Hence, the original pixel pair (s, t) and the new pixel pair values (s'', t'') are different based on the watermark embedding value.

Consider any pixel pair (s', t') in a watermarked image (obtained through LDE) for embedding the secret information using QDE, where the to-be embedded watermark bit is represented as b'. The newly generated image pixel pairs (s'', t'') are given by (30), (31).

$$s'' = \left[\frac{s'+t'}{2}\right] + \left[\frac{\left[\frac{s'-t'}{2}\right]+b'+1}{2}\right] \quad (30)$$

$$t'' = \left[\frac{s'+t'}{2}\right] + \left[\frac{\left[\frac{s'-t'}{2}\right]+b'}{2}\right] \quad (31)$$

C. Inverse MQDE

Whenever there is a need to prove ownership, the owner first applies inverse MQDE to extract the embedded watermark from the location map [pixel pairs (s'', t'')] that is with him. Later, the original image recovery is done by applying inverse LDE.

A location map is first used to select a set of pixel pairs (s'', t'') from the watermarked image where the watermark was hidden. The average and difference values of the pixel pairs are then calculated using Equations (3), (4). Later (32) is used to normalizes the pixel values to binary 0 or 1, on applying the modulus function, which checks the pixel (s'', t'') and difference (d') values for even or odd conditions

$$A = mod(s'', 2),\ B = mod(t'', 2),\ C = mod(d', 2) \quad (32)$$

For instance, if the pixel value of s'' is 235, then the value is odd. The modulus operation in (32) returns A = 1. Similarly, even pixel value returns a value of 0. Based on the values of watermarked pixels and their difference, the following condition is used to extract the corresponding watermark bits.

$$Extracted\ bit = b = XNOR\ (A, B, C) \quad (33)$$

Here, XNOR performs a logical operation to check if the pixel values and difference are all even or odd. If (A, B, C) are all odd or even, the watermark bit is set to 1, otherwise it is set to 0.

The original image recovery starts with finding the LDE embedded pixel pair as given in (34) – (35)

$$s' = m' + \frac{(2(s''-t'')+1)}{2} \quad (34)$$

$$t' = m' - \frac{(2(s''-t''))}{2} \quad (35)$$

The original image pixels (s, t) are then recovered using the following equations:

$$s = \frac{6s'+2t'-2b-3}{8} \quad (36)$$

$$t = \frac{2s'+6t'+2b-1}{8} \quad (37)$$

If the secret bit that was retrieved is1, $s = s - 1$ and t is unmodified

If the secret bit that was taken is 0, s is unaltered, and t is $t - 1$.

D. Watermark Embedding Algorithm

Inputs: Secret Key, Secret Information, Cover Image

Output: Watermarked Image

1. Read the watermark and cover image.
2. Fractal encrypt the watermark using (14), (15). Convert the encrypted image into a 1-D vector.
3. Carry out CSGWO optimization on the cover picture to choose the optimal pixel pairings for embedding using the fitness function in (21) to get a higher visual quality. *I_loc* is a map that contains the locations of these pixel pairs.
4. Choose pixel pairs starting with $P = (s, t)$ based on *I_loc* (s, t).
5. Using (1,2), determine the difference and average of pixel pairs.
6. Using s (23, 24), transform the pixel pairings after LDE has expanded the difference. This results in the modified pair (s', t').
7. Find the difference and average for the pair (s', t') using (25, 26).
8. Expand the difference using (27) and use (30,31), to determine the final MQDE converted pair (s'', t'').
9. For each pair of pixels from *I_loc*, repeat steps 4 through 8 to create a watermarked picture.

E. Watermark and Cover Image Recovery Algorithm

Inputs: Location Map and Watermarked Image

Outputs: Expected Watermark, Recovered Cover Image

1. The selection of pixel pairs in the watermarked image P= (s'', t'') with the help of *I_loc*,
2. Utilizing (1,2), discover the average value and difference of pixels.
3. Utilizing (32), check for odd and even circumstances of difference and pixel pair.
4. Utilizing (33), discover the extracted watermark bit.
5. In two steps, recover the cover picture. Using (34), first separate the LDE changed pixels (s', t') from (s', t'') (35). Then, using (36), reconstruct the cover image pixel pair (s, t) (37).
6. Modify the anticipated pixel values for the cover image according to the recovered watermark bit in step 4.
7. For each pair of *I_loc* pixel pairs, repeat steps 1-6 to recover the cover image.

V. Experimental Results

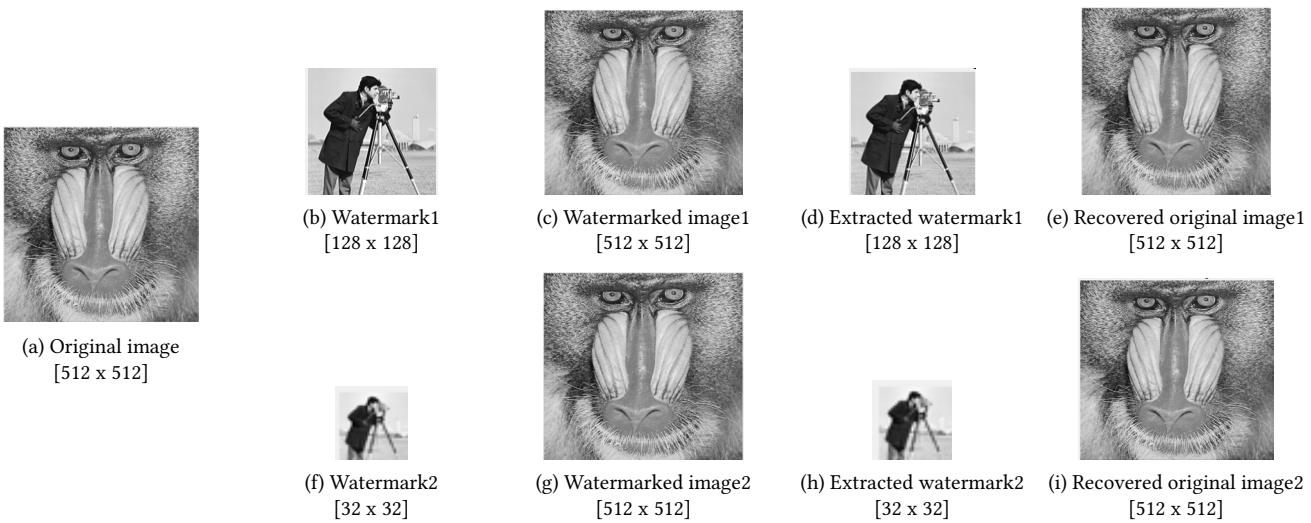
A. Performance of Watermarking in the Absence of Attacks

This section presents the quantitative and qualitative findings of the suggested model in the absence of attacks on published watermarked images. In Fig. 6, the subjective results of the embedding and extraction processes are shown, considering the greyscale Baboon image (512 x 512) as the original image (to be watermarked) and the cameraman images of two sizes (128 x 128 and 32 x 32) as the watermarks. These results after embedding the individual watermarks exhibits high imperceptibility of the watermark in watermarked images along with high-quality reversed images after watermark extraction, regardless of the size of the watermark (either 128 × 128 or 32 × 32). In the absence of an attack on the watermarked picture, Table I tabulates the objective findings after comparing the similarity between the original image and recovered original image, original image, and watermarked image, and original and extracted watermarks.

When a 128× 128 greyscale pixels (131072 bits) watermark is embedded in a 512×512 greyscale cover image, the suggested technique derived an average of 46 dB PSNR when evaluated on original and watermarked images, indicating high imperceptibility. An average of 67 dB PSNR was noticed, when calculated between the original and recovered cover images, indicating high reversibility. When the watermark size is reduced to 32×32 pixels, the imperceptibility and reversibility are even better. It is to be noted that the watermark is extracted without any loss in the absence of attacks, as PSNR (OW, EW) is infinity, where EW is the extracted watermark and OW is the original watermark.

B. Time Complexity Analysis

Fig. 7 depicts a comparison of seven optimization strategies in terms of the calculation time necessary to get the ideal value using different reference functions with varying numbers of design variables. The calculation time of seven optimization approaches is accounted for by the NFE (number of function evaluations) in the collection of reference functions [70]. It was observed that the GWO and CSA take the least amount of computing time. Thus, the hybrid CSGWO approach offers the least computation time among other hybrid methods. The authors of [71] also concluded that GWO performs better than other metaheuristic algorithms in terms of complexity.



(a) Original image [512 x 512]
(b) Watermark1 [128 x 128]
(c) Watermarked image1 [512 x 512]
(d) Extracted watermark1 [128 x 128]
(e) Recovered original image1 [512 x 512]
(f) Watermark2 [32 x 32]
(g) Watermarked image2 [512 x 512]
(h) Extracted watermark2 [32 x 32]
(i) Recovered original image2 [512 x 512]

Fig.6. Subjective results of proposed reversible watermarking.

TABLE I. Objective Results in the Absence of Attacks

Cover Image	PSNR (OI, WI)	SSIM (OI, WI)	PSNR (OI, ROI)	SSIM (OI, ROI)	PSNR (OW, EW)	SSIM (OW, EW)
	For watermark of size 128×128					
Baboon	46.384	0.99442	65.56	0.99987	Inf	1
Lena	46.357	0.97918	68.10	0.99988	Inf	1
Peppers	46.359	0.98308	67.94	0.99988	Inf	1
Barbara	46.359	0.98567	67.93	0.99992	Inf	1
	For watermark of size 32×32					
Baboon	51.601	0.99894	71.95	1	Inf	1
Lena	51.597	0.99494	72.37	0.99988	Inf	1
Peppers	51.589	0.99509	73.36	0.99997	Inf	1
Barbara	51.597	0.99498	72.38	0.99998	Inf	1
OI – Original Image, WI – Watermarked Image, ROI – Recovered Original Image, OW- Original Watermark, EW- Extracted Watermark						

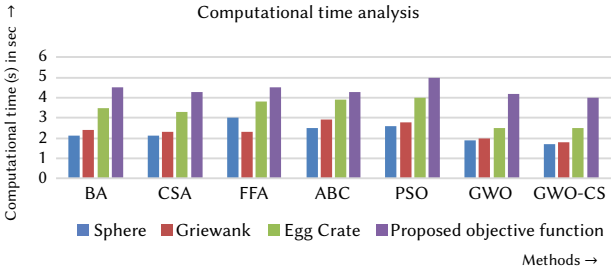


Fig.7. Computational time analysis for various optimization methods.

C. Embedding Capacity Analysis

Fig. 8–12 illustrates the impact of changes in embedding capacity on various watermarking evaluation parameters. Embedding capacity has been changed with respect to 10, 30, 70, 90, and 100 percentages. Fig. 8 represents the outcome between entropy and embedding capacity, where entropy is calculated among different images. It is to be noted that there is not much deviation in entropy as embedding capacity changes. Fig. 9 shows the SSIM vs. embedding capacity, and it can be clearly observed that lower embedding rates lead to less distortion in the watermarked image. Similarly, Fig. 10 represents PSNR vs. embedding capacity, where PSNR values go down as embedding capacity increases. It is interesting to note that even with 100% embedding capacity, the PSNR values remain above 50 dB. Furthermore, Fig. 11 shows that NCC values decrease as embedding capacity increases but remain significantly good even at 100% capacity. Fig. 12 indicates that MSE values go up with capacity.

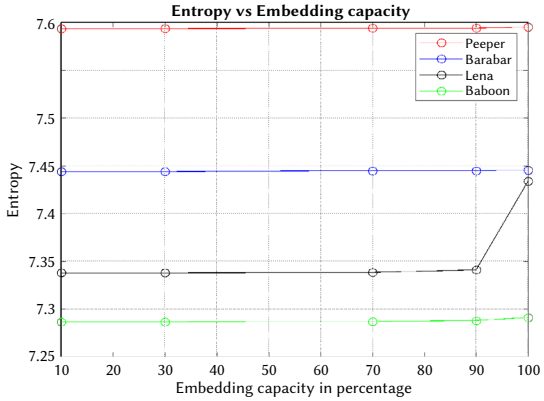


Fig. 8. Embedding capacity vs. Entropy.

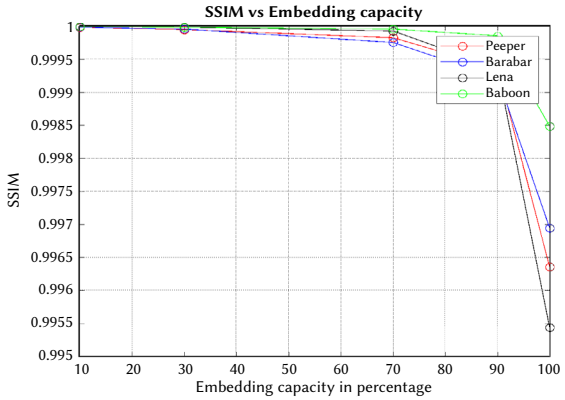


Fig. 9. Embedding capacity vs. SSIM.

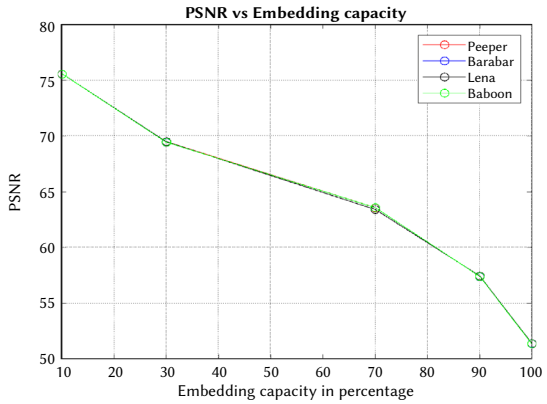


Fig. 10. Embedding capacity vs. PSNR.

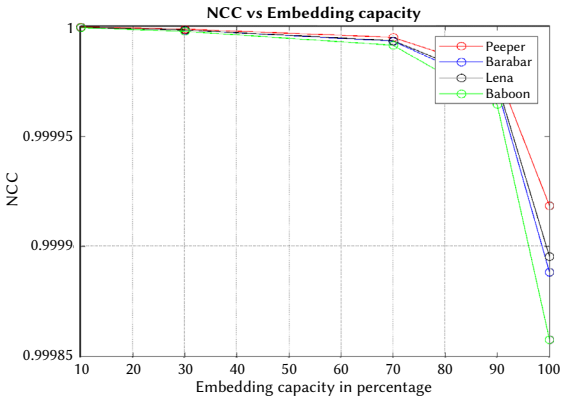


Fig.11. Embedding capacity vs. NCC.

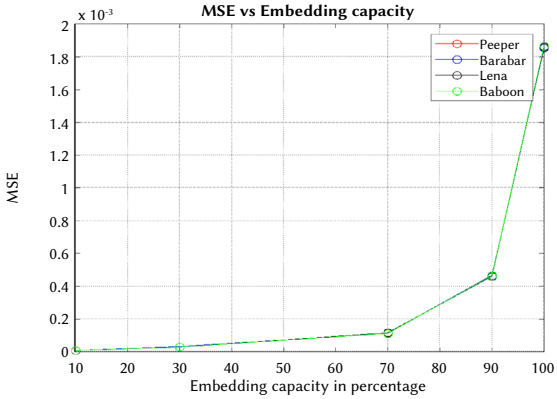


Fig.12. Embedding capacity vs. MSE.

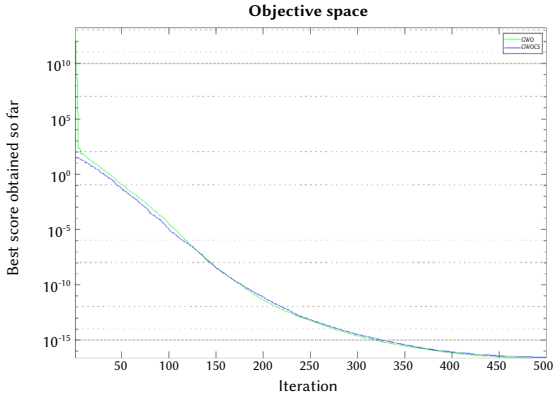


Fig.13. Convergence graph of GWO and hybrid CSGWO.

D. Comparison of Hybrid CSGWO With GWO

With Table II listing the simulation parameters for the proposed CSGWO, it can be concluded from Fig.13, that the convergence rate is high in the proposed CSGWO as compared to simple GWO. At the time of initial iteration, best-score achieved by hybrid approach is better than GWO. As iteration increases the obtained best score in GWO and hybrid CSGWO become similar.

TABLE II. Simulation Parameters for the Proposed CSGWO

Number of search agents	40
Maximum Iteration	100
Search Dimension	2
Domain of Search for alpha	[-1000 1000]
Domain of search for beta	[-1 1]
Domain of search for delta	[0 1000]

Table III depicts the comparative performance analysis of Grey Wolf (GWO), Cuckoo Search (CS) algorithm and Hybrid (CSGWO) approaches. The PSNR and SSIM when calculated for various benchmark images after embedding a payload of 16384 bytes (128×128) indicates that the CSGWO gives better results. Approximately 2 dB improvement is achieved with the proposed hybrid CSGWO as compared to traditional GWO and CS respectively.

E. Attack Resilience of Watermarking

Attacks [72], [73] that are both purposeful and unintended are considered while evaluating the suggested watermarking strategy. Considering Cameraman (128×128) as a watermark, Baboon (256×256) as an original image, the PSNR calculated between the original and extracted watermarks in the presence of a few attacks is tabulated in Table 4. Results show that the method is resistant to histogram equalization, cropping, and salt and pepper noise.

TABLE IV. Performance in the Presence of Attacks

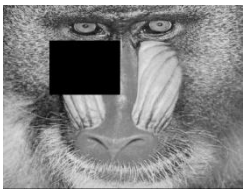
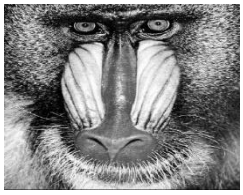
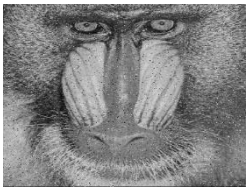
Attacks	Watermarked image	Extracted watermark
10% Crop		
PSNR (OI, ROI)	26.971	
PSNR (OW, EW)	26.786	
Histogram equalization		
PSNR (OI, RI)	17.619	
PSNR (OW, EW)	Inf	
Salt and Pepper noise (0.05 density)		
PSNR (OI, RI)	18.58	
PSNR (OW, EW)	16.61	

TABLE III. Performance Evaluation of Reversible Watermarking With Respect to Various Optimization Techniques

Cover Image	PSNR (CSGWO)	SSIM (CSGWO)	PSNR (GWO)	SSIM (GWO)	PSNR (CS)	SSIM (CS)
	For watermark of size 128×128					
Baboon	46.384	0.99442	44.845	0.9895	44.163	0.9820
Lena	46.357	0.97918	44.894	0.9613	44.920	0.9728
Peppers	46.359	0.98308	43.269	0.9598	44.249	0.9609
Barbara	46.359	0.98567	44.738	0.9730	44.209	0.9789

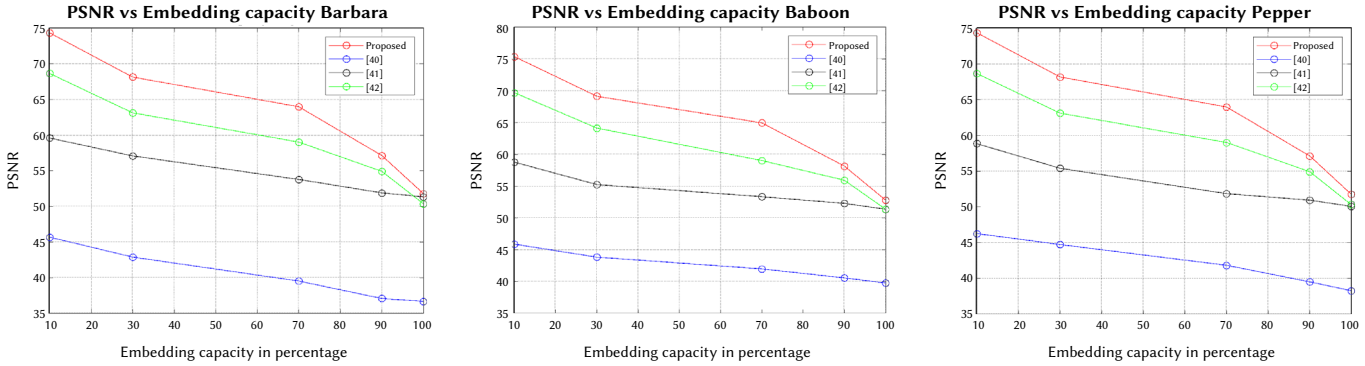


Fig.14. Proposed method vs research works [40], [41] and [42].

TABLE V. Comparative Analysis With State-of-the Art Techniques

	[43]		[44]		[45]		[46]		[47]		Proposed	
	Capacity	**PSNR**	**Capacity**	**PSNR**	**Capacity**	**PSNR**	**Capacity**	**PSNR**	**Capacity**	**PSNR**	**Capacity**	**PSNR**
Airplane	228863	25.97	164962	32.98	-	-	71,680	53.6	51376	52.60	259422	55.2
Baboon	459737	20.53	128256	30.25	26000	32	71,680	53.5	16011	51.47	258676	55.38
Barbara	290234	23.43	-	-	31000	32	-	-	30559	51.80	261226	56.36
Boat	301995	25.26	142506	30.89	-	-	71,680	53.87	29686	51.73	257662	55.61
Couple	299203	24.02	-	-	-	-	-	-	-	-	258894	55.42
Lena	224528	28.35	172627	32.28	182000	32	-	-	36607	52.02	261298	55.35
Peppers	223295	26.79	181258	33.3	104000	32	-	-	34797	51.88	258458	55.36

VI. Comparative Investigation and Discussion

The embedding capacity (watermark size with respect to the original image) is varied in terms of percentages (10%, 30%, 70%, 90%, and 100%) and the corresponding PSNR calculated between the original and watermarked images is compared in Fig. 14 for three different reversible watermarking schemes proposed in the literature. The results indicate that the proposed method outperforms [40]–[42] and exhibits high imperceptibility (high PSNR) under different embedding capacities for four benchmark images. Table 5 extends the comparative analysis of other state-of-the art techniques. The proposed method supports large-sized watermarks while still maintaining high invisibility. Hence, it is concluded that the proposed hybrid algorithm mainly reduces the capacity-invisibility tradeoff compared to the related invisible reversible watermarking schemes.

An analytical comparison of the suggested method with the current hybrid and non-hybrid models is shown in Table 6. Adaptive Difference Expansion (ADE)-based techniques claim to improve embedding capacity at the expense of imperceptibility. Further, the method is complex as it requires many parameters, such as the stego-image, average, difference, maximum, and minimum pixel values of surrounding pixels, apart from the watermarked image and location maps for watermark extraction and the watermark recovery process. On the same Baboon grayscale image of size 512×512, the optional embedding scheme (OES) claims high imperceptibility (53 dB PSNR) but can only embed a 15000-bit watermark. The hybrid models, which combined LDE and QDE, claimed high imperceptibility after reporting a PSNR of 76.87 dB. An additional layer of protection, encryption, is applied to the watermark and has the benefit of not requiring a map of its position. However, it has an additional process of first removing 0 and 255 valued pixels and then again attaching them for both embedding and extraction. The performance of these three methods was not evaluated and reported for complexity, robustness, and reversibility. Furthermore, there is no optimization of pixel selection to improve visual quality. The hybrid models that combined difference expansion with a genetic algorithm for embedding watermark bits supported a maximum capacity of 0.7 bpp for Lena and Boats images at 32.43 dB and 31.3 dB PSNR, respectively. The imperceptibility of this hybrid model is low, and the smoothing effect [26] remains. It has been shown that when capacity rises, visual quality falls, creating a trade-off. To control quality deterioration, a high-capacity RW system must be designed. A favorable capacity-quality ratio is largely maintained by our proposed approach, which could embed 128×128 greyscale image (131072 bits) and could achieve a high PSNR and high visual quality based on the results presented in Table VI. Hence, compared to relevant algorithms, the approach proposed in this paper exhibits high embedding capacity, supports grayscale images as watermarks, and retains the quality of both watermarked and reversed images (an average PSNR of 67 dB). The suggested technique is resistant to many common attacks.

The technique is further strengthened by using fractal encryption of the watermark before its embedding. The secret key used in the fractal encryption method is neither being transferred over the network nor embedded into the image. It is only held by the owner and is used by him for encryption (before watermark embedding) and decryption (after watermark extraction). For the sake of secret key recovery, an attacker could attempt to distinguish any notable information between the normal image and its encryption version. An image with considerable visual information is distinguished by strong correlation and redundancy between surrounding pixels, whether in vertical, diagonal, or horizontal orientations. A well-designed encryption algorithm [74] – [76] should be capable of concealing such links between neighboring pixels while demonstrating zero correlation. The number of pixel change rate (NPCR) parameter is calculated and compared with various encryption algorithms employed in earlier state-of-the-art reversible watermarking techniques to estimate the correlation performance of fractal encryption for its applicability in the proposed watermarking. Because the achieved NPCR (99.65) was close to the theoretical value of 100, fractal encryption was chosen.

TABLE VI. Existing Models Comparison

	Non-Hybrid Techniques		Hybrid Techniques		
	[40]	[41]	[42]	[59]	**Proposed**
Methodology	Adaptive Difference Expansion (ADE)	Optional Embedding Scheme (OES)	Quadratic Difference Expansion (QDE)	Difference Expansion with Genetic Algorithm	Hybrid Modified Difference with Fractal encryption and GWO
Watermark Type	Bit stream	Bit stream	Binary image	Bit stream	Greyscale image
Secret keys	No	No	Required	No	Required
Optimization for selection of pixels	No	No	No	Genetic Algorithm	Grey Wolf Optimization
Location map	No	Required	No	Required	Required
Inputs of Watermark embedding phase	Cover Image, Embedding parameters ep1, ep2, ep3, Watermark bit stream; Average, Maximum and minimum of pixel values of surrounding pixels	Cover Image, Location map, Overhead information (EC), Watermark bitstream	Cover Image with 0 and 255 pixels removed, Scrambled Watermark	Cover Image, Location map, Watermark bitstream	Cover image, Encrypted watermark, Location map
Watermark Size	88448 bits	15000 bits	1024 bits	183500 bits	131072 bits
PSNR (OI, WI)	39.76 dB	53 dB	76.87 dB	32.43 dB	66.38 dB

The proposed hybrid model combined meta heuristics to choose optimal locations for embedding watermark bits, thereby improving performance by reducing tradeoffs between embedding capacity and imperceptibility. The disadvantage of a particular optimization algorithm can be overcome by utilizing a complementary feature of another algorithm, thus gaining from both algorithms, and resulting in better performance. GWO was selected in the proposed method over other meta-heuristics because of its relatively simple structure and lower storage requirements. Only two parameters needed to be tuned, and the decision variables were also limited. GWO aims to find the individual with the best fitness value, thus limiting the global search and increasing the chance of encountering a local optimum. However, the update mechanism has two major drawbacks in optimizing real-world functions: first, due to the use of the best global solutions found so far, the algorithm converges very quickly to a local optimal solution and loses its optimization power significantly; second, it causes the loss of a variety of new populations in each iteration of the algorithm. To fix these two shortcomings and strengthen the GWO algorithm, CS is incorporated into GWO for better performance regarding good exploration. It is much easier to jump from the current region to another, as CS updates the nest's positions with a certain probability independent of the search path, and with random directions. In CSGWO, the GWO location update is modified to account for the CS update equation to get a faster convergence rate in comparison to GWO.

The hybrid approach of combining meta-heuristic algorithms may also lead to an additional computational cost. To make a data hiding algorithm reversible or lossless, it is desirable to keep the complexity low, which directly impacts the robustness. Since the proposed scheme uses a spatial domain technique, its robustness is limited to a few attacks. It is still difficult to create a spatial domain RW scheme that is resistant to all types of attacks. Hiding multiple secret images or watermarks using the same scheme to hide more information without a tradeoff in imperceptibility is another challenge to work toward. Further, the performance of a hybrid meta-heuristic approach depends on the defined fitness function. Therefore, one cannot generalize that a hybrid approach always outperforms individual meta-heuristic algorithms. Thus, choosing a hybrid approach suitable for the given fitness function remains another challenge, which may be taken up as future work.

VII. Conclusion

This study introduced a reversible watermarking technique based on MQDE with hybrid optimization and fractal encryption, to meet the three important properties: imperceptibility, embedding capacity, and security. Correlated to former embedding techniques, CSGWO with the MQDE method considerably expands the optimal visual quality and embedding capacity. A novel data-driven distortion control unit is used for defining the optimization parameters with each iteration. The proposed model achieved satisfactory imperceptibility and was observed to be superior to the existing models (ADE, OES, and QDE) considering robustness against salt and pepper noise, cropping attacks, and histogram equalization. An average PSNR of 67 dB was achieved. The L-shaped tromino method combined with fractal encryption produces a protected image watermark. The suggested algorithms exceed the current methodologies with all these benefits, especially in terms of embedding capacity and reversibility, without sacrificing invisibility, and with the ability to withstand minimal attacks. Future research focuses on improving the reversibility performance of the proposed system in the presence of geometric attacks. While the method can easily be extended to be compatible with color images, the development of methods for the elimination of location maps can be explored. More meta-heuristics and combinations of them can be explored to determine the best approach for the given application.

Conflict of Interest

Author 1 (Lakshmi H R) declares that she has no conflict of interest.

Author 2 (Surekha Borra) declares that she has no conflict of interest.

On behalf of all authors, the corresponding author states that there is no conflict of interest.

Funding

Nil.

Ethical Approval

This article does not contain any studies with human participants or animals performed by any of the authors.

References

[1] H. R. Lakshmi and S. Borra, "Difference expansion based reversible watermarking algorithms for copyright protection of images: state-of-the-art and challenges," *International Journal of Speech Technology*, vol. 24, no. 24, pp. 823-852, 2021, doi: https://doi.org/10.1007/s10772-021-09818-y.

[2] K. Curran and R. Lautman, "The Problems of Jurisdiction on the Internet," *International Journal of Ambient Computing and Intelligence (IJACI)*, vol. 3, no. 3, pp. 36-42, 2011, doi: https://doi.org/10.4018/jaci.2011070105.

[3] D. Quinn, L. Chen, and M. Mulvenna, "Social network analysis: A survey," *International Journal of Ambient Computing and Intelligence (IJACI)*, vol. 4, no. 3, pp. 46-58, 2012, doi: https://doi.org/10.4018/jaci.2012070104.

[4] S. Borra and H. R. Lakshmi, "Visual Cryptography Based Lossless Watermarking for Sensitive Images," in *International Conference on Swarm, Evolutionary, and Memetic Computing*, vol. 9873, B. Panigrahi, P. Suganthan, S. Das and S. Satapathy, Eds. Cham: Springer International Publishing, 2015, pp. 29-39.

[5] D. Ariatmanto and F. Ernawan, "Adaptive scaling factors based on the impact of selected DCT coefficients for image watermarking," *Journal of King Saud University-Computer and Information Sciences,* vol. 34, no. 3, pp. 605-614, 2020, doi: https://doi.org/10.1016/j.jksuci.2020.02.005.

[6] S. Borra Surekha, H. R. Lakshmi, N. Dey, A. S. Ashour, and F. Shi, "Digital Image Watermarking Tools: State-of-the-Art," in *2nd International Conference on Information Technology and Intelligent Transportation Systems,* vol. 296, V. E. Balas, C. J. Lakhmi, X. Zhao, F. Shi, Frontiers in Artificial Intelligence and Applications: IOS Press, 2017, pp. 450-459.

[7] S. Borra, R. Thanki, and N. Dey, *Digital image watermarking: theoretical and computational advances*, New York, USA: CRC Press, 2018.

[8] Y. Zhang and Y. Sun, "An image watermarking method based on visual saliency and contourlet transform," *Optik*, vol. 186, pp. 379-389, 2019, doi: https://doi.org/10.1016/j.ijleo.2019.04.091

[9] H. R. Lakshmi, B. Surekha. and S. Viswanadha Raju, "Real-time Implementation of Reversible Watermarking," *In: Intelligent Techniques in Signal Processing for Multimedia Security*, vol. 660, N. Dey, V. Santhi, Eds. Cham: Springer International Publishing, 2017, pp. 113-132.

[10] H.J. Ko, C.T. Huang, G. Horng and W.A.N.G. Shiuh-Jeng, "Robust and blind image watermarking in DCT domain using inter-block coefficient correlation," *Information Sciences*, vol. 517, pp. 128-147, 2020, doi: https://doi.org/10.1016/j.ins.2019.11.005 517.

[11] B. Surekha, G. Swamy and K. S. Rao, "A multiple watermarking technique for images based on visual cryptography," *International Journal of Computer Applications,* vol. 1, no. 11, pp. 77-81, 2010, doi: 10.5120/236-390

[12] A. K. Pal, P. Das and N. Dey, "Odd-even embedding scheme based modified reversible watermarking technique using Blueprint", arXiv preprint, arXiv:1303.5972, 2013. Accessed: Oct. 12, 2022. [Online]. Available: https://arxiv.org/ftp/arxiv/papers/1303/1303.5972.pdf

[13] B. Surekha and G. Swamy, "A semi-blind image watermarking based on Discrete Wavelet Transform and Secret Sharing," in *2012 IEEE International Conference on Communication, Information & Computing Technology (ICCICT)*, Mumbai, India, 2012, pp. 1-5.

[14] M. Cinque, A. Coronato and A. Testa, "Dependable Services for Mobile Health Monitoring Systems," *International Journal of Ambient Computing and Intelligence*, vol. 4, no.1, pp. 1-15, 2012, doi: https://doi.org/10.4018/jaci.2012010101

[15] S. L. Li, K. C. Leung, L. M. Cheng and C. K. Chan, "Data Hiding in Images by Adaptive LSB Substitution Based on the Pixel-Value Differencing," in *First IEEE International Conference on Innovative Computing, Information and Control - Volume I (ICICIC'06)*, Beijing, China, 2006, pp. 58-61.

[16] S. H. Wang and Y. P. Lin, "Wavelet tree quantization for copyright protection watermarking," in *IEEE Transactions on Image Processing*, vol. 13, no. 2, pp. 154-165, 2004, doi: 10.1109/TIP.2004.823822.

[17] W. H. Lin, Y. R. Wang, S. J. Horng, T. W. Kao and Y. Pan, "A blind watermarking method using maximum wavelet coefficient quantization," *Expert Systems with Applications*, vol. 36, no. 9, pp. 11509-11516, 2009, doi: https://doi.org/10.1016/j.eswa.2009.03.060

[18] A. A. Reddy and B. N. Chatterji, "A new wavelet-based logo-watermarking scheme," *Pattern Recognition Letters*, vol. 26, no. 7, pp. 1019-1027, 2005, https://doi.org/10.1016/j.patrec.2004.09.047

[19] M. Yamni, A. Daoui, H. Karmouni, M. Sayyouri, H. Qjidaa and J. Flusser, "Fractional Charlier moments for image reconstruction and image watermarking," *Signal Processing*, vol. 171, pp. 107509, 2020, doi: https://doi.org/10.1016/j.sigpro.2020.107509

[20] S. Chakraborty, S. Chatterjee, N. Dey, A.S. Ashour and A.E. Hassanien, "Comparative Approach Between Singular Value Decomposition and Randomized Singular Value Decomposition-based Watermarking," *In Intelligent Techniques in Signal Processing for Multimedia Security,* vol. 660, N. Dey, V. Santhi, Eds. Chams: Springer International Publishing, 2017, pp. 133-149. vol 660.

[21] H. R. Lakshmi and B. Surekha, "Asynchronous Implementation of Reversible Image Watermarking Using Mousetrap Pipelining," in *2016 IEEE 6th International Conference on Advanced Computing (IACC)*, Bhimavaram, India, 2016, pp. 529-533.

[22] S. Gujjunoori and B. B. Amberker, "DCT based reversible data embedding for MPEG-4 video using HVS characteristics," *Journal of information security and applications*, vol. 18, no. 4, pp. 157-166, 2013, https://doi.org/10.1016/j.istr.2013.01.002.

[23] M. Liu, H. S. Seah, C. Zhu, W. Lin and F. Tian, "Reducing location map in prediction-based difference expansion for reversible image data embedding," *Signal Processing*, vol. 92, no. 3, pp. 819-828, 2012, doi: https://doi.org/10.1016/j.sigpro.2011.09.028.

[24] Z. Ni, Y. Q. Shi, N. Ansari and W. Su, "Reversible data hiding," in *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 16, no. 3, pp. 354-362, 2006, doi: 10.1109/TCSVT.2006.869964.

[25] C. C. Chang and T. C. Lu, "A difference expansion-oriented data hiding scheme for restoring the original host images," *Journal of Systems and Software*, vol. 79, no. 12, pp. 1754-1766, 2006, https://doi.org/10.1016/j.jss.2006.03.035.

[26] J. Tian, "Reversible data embedding using a difference expansion," in *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13, no. 8, pp. 890-896, 2003, doi: 10.1109/TCSVT.2003.815962.

[27] X. Wang, X. Li, B. Yang and Z. Guo, "Efficient Generalized Integer Transform for Reversible Watermarking," *in IEEE Signal Processing Letters*, vol. 17, no. 6, pp. 567-570, 2010, doi: 10.1109/LSP.2010.2046930.

[28] H. C. Huang, F. C. Chang and W. C. Fang, "Reversible data hiding with histogram-based difference expansion for QR code applications," in *IEEE Transactions on Consumer Electronics*, vol. 57, no. 2, pp. 779-787, 2011, doi: 10.1109/TCE.2011.5955222.

[29] W. L. Tai, C. M. Yeh and C. C. Chang, "Reversible Data Hiding Based on Histogram Modification of Pixel Differences," in *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 19, no. 6, pp. pp. 906-910, 2009, doi: 10.1109/TCSVT.2009.2017409.

[30] J. Tian. "Reversible watermarking by difference expansion," in *Proceedings of workshop on multimedia and security*, vol. 19, J. Dittmann, J. Fridrich, P. Wohlmacher, Eds. ACM, 2002, Juan-les-Pins: ACM, 2002. Multimedia and Security Workshop at ACM Multimedia '02, December 6, 2002, pp. 19–22.

[31] T. C. Lu, and C. C. Chang, "Lossless nibbled data embedding scheme based on difference expansion," *Image and Vision Computing*, vol. 26, no. 5, pp. 632-638, 2008, doi: https://doi.org/10.1016/j.imavis.2007.07.011.

[32] E. Chrysochos, V. Fotopoulos and A. N. Skodras, "A new difference expansion transform in triplets for reversible data hiding," *International Journal of Computer Mathematics*, vol. 88, no. 10, pp. 2016-2025, 2011, doi: https://doi.org/10.1080/00207160.2010.539210

[33] A. M. Alattar, "Reversible watermark using the difference expansion of a generalized integer transform," in *IEEE Transactions on Image Processing*, vol. 13, no. 8, pp. 1147-1156, 2004, doi: 10.1109/TIP.2004.828418.

[34] J. Y. Hsiao, K. F. Chan and J. M. Chang, "Block-based reversible data embedding," *Signal Processing*, vol. 89, no. 4, pp. 556-569, 2009, doi: https://doi.org/10.1016/j.sigpro.2008.10.018

[35] Y. Hu, H. K. Lee, K. Chen and J. Li, "Difference Expansion Based Reversible Data Hiding Using Two Embedding Directions," in *IEEE Transactions on Multimedia*, vol. 10, no. 8, pp. 1500-1512, 2008, doi:10.1109/TMM.2008.2007341.

[36] P. Maniriho and T. Ahmad, "Information hiding scheme for digital images using difference expansion and modulus function," *Journal of king saud university-computer and information sciences,* vol. 31, no. 3, pp. 335-347, 2019, doi: https://doi.org/10.1016/j.jksuci.2018.01.011

[37] P. Maniriho and T. Ahmad, "Enhancing the Capability of Data Hiding Method Based on Reduced Difference Expansion," *Engineering Letters*, vol. 26, no. 1, pp. 45-55, 2018.

[38] M. H. A. Al-Hooti, T. Ahmad and S. Djanali, "Improving the Capability of Reduced Difference Expansion based Digital Image Data Hiding," *IAENG International Journal of Computer Science*, vol. 46, no. 4, 2019.

[39] S. Gujjunoori and M. Oruganti, "Difference expansion based reversible data embedding and edge detection," *Multimedia Tools and Applications*, vol. 78, pp. 25889–25917, 2019, doi: https://doi.org/10.1007/s11042-019-07767-y.

[40] H. S. El-sayed, S. F. El-Zoghdy and O. S. Faragallah, "Adaptive difference expansion-based reversible data hiding scheme for digital images," *Arabian Journal for Science and Engineering*, vol. 41, no. 3, pp. 1091-1107, 2016, doi: https://doi.org/10.1007/s13369-015-1956-7

[41] S. Weng, J. S. Pan and L. Zhou, "Reversible data hiding based on the local smoothness estimator and optional embedding strategy in four prediction modes," *Multimedia Tools and Applications*, vol. 76, no. 11, pp. 13173-13195, 2017, doi: https://doi.org/10.1007/s11042-016-3693-7.

[42] Z. Zhang, M. Zhang, L. Wang, "Reversible Image Watermarking Algorithm Based on Quadratic Difference Expansion," *Mathematical Problems in Engineering*, vol. 2020, 2020. https://doi.org/10.1155/2020/1806024.

[43] A. A. Mohammad, A. Al-Haj and M. Farfoura, "An improved capacity data hiding technique based on image interpolation," *Multimedia Tools and Applications*, vol. 78, no. 6, pp. 7181-7205, 2019, doi: https://doi.org/10.1007/s11042-018-6465-8

[44] R. Anushiadevi, P. Praveenkumar, J. B. B. Rayappan and R. Amirtharajan, "Reversible data hiding method based on pixel expansion and homomorphic encryption," *Journal of Intelligent & Fuzzy Systems*, vol. 39, no. 3, pp. 2977-2990, 2020, doi: 10.3233/JIFS-191478.

[45] W. Wang, "A reversible data hiding algorithm based on bidirectional difference expansion," *Multimedia Tools and Applications*, vol. 79, no. 9, pp. 5965-5988, 2020, doi: https://doi.org/10.1007/s11042-019-08255-z

[46] A. J. Ilham, and T. Ahmad, "Reversible Data Hiding Scheme based on General Difference Expansion Cluster," *International. Journal of Advance Soft Computing and Applications*, vol. 12, no. 3, pp. 11-24, 2020.

[47] M. Abdul Wahed and H. Nyeem, "Reversible data hiding with dual pixel-value-ordering and minimum prediction error expansion," *Plos one*, vol. 17, no. 8, 2022, doi: https://doi.org/10.1371/journal.pone.0271507

[48] N. Dey, J. Chaki, L. Moraru, S. Fong and X. S. Yang, "Firefly Algorithm and Its Variants in Digital Image Processing: A Comprehensive Review," in *Applications of Firefly Algorithm and its Variants*, Dey, N. Ed. Singapore, Springer, 2020, ch. 1, pp. 1-28, doi: https://doi.org/10.1007/978-981-15-0306-1_1.

[49] N. Dey, A. S. Ashour and S. Bhattacharyya, *Applied nature-inspired computing: algorithms and case studies*, Singapore: Springer International Publishing, 2020.

[50] M. B. Imamoglu, M. Ulutas and G. Ulutas, "A new reversible database watermarking approach with firefly optimization algorithm," *Mathematical Problems in Engineering*, vol. 2017, 2017, doi: https://doi.org/10.1155/2017/1387375.

[51] A. Ghardallou, A. Kricha, A. Sakly and A. Mtibaa, "Adaptive block sized reversible watermarking scheme based on integer transform," in *2016 17*th *IEEE International Conference on Sciences and Techniques of Automatic Control and Computer --Engineering (STA)*, Sousse, Tunisia, 2016, pp. 347-351.

[52] T. Naheed, I. Usman, T. M. Khan, A. H. Dar and M. F. Shafique, "Intelligent reversible watermarking technique in medical images using GA and PSO," *Optik*, vol. 125, no. 11, pp. 2515-2525, 2014, doi: https://doi.org/10.1016/j.ijleo.2013.10.124.

[53] S. Sharma and H. Patil, "Secure data hiding scheme using firefly algorithm with hidden compression," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 23, no. 2, pp. 525-534, 2020, doi: https://doi.org/10.1080/09720529.2020.1729502

[54] M. K. Pandey, G. Parmar, R. Gupta and A. Sikander, "Lossless robust color image watermarking using lifting scheme and GWO," *International Journal of System Assurance Engineering and Management*, vol. 11, no. 2, pp. 320-331, 2020, doi: https://doi.org/10.1007/s13198-019-00859-w.

[55] H. Zarrabi, A. Emami, P. Khadivi, N. Karimi and S.Samavi, "BlessMark: a blind diagnostically-lossless watermarking framework for medical applications based on deep neural networks," *Multimedia Tools and Applications*, vol. 79, no. 31, pp. 22473-22495, 2020, doi: https://doi.org/10.1007/s11042-020-08698-9.

[56] F. Y. Shih, X. Zhong, I. C. Chang and S. Satoh, "An adjustable-purpose image watermarking technique by particle swarm optimization," *Multimedia Tools and Applications*, vol. 77, no. 2, pp. 1623-1642, 2018, doi: https://doi.org/10.1007/s11042-017-4367-9.

[57] M. Arsalan, A. S. Qureshi, A. Khan and M. Rajarajan, "Protection of medical images and patient related information in healthcare: Using an intelligent and reversible watermarking technique," *Applied Soft Computing*, vol. 51, pp. 168-179, 2017, doi: https://doi.org/10.1016/j.asoc.2016.11.044.

[58] K. Balasamy and S. Ramakrishnan, "An intelligent reversible watermarking system for authenticating medical images using wavelet and PSO," *Cluster Computing*, vol. 22, no. 2, pp. 4431-4442, 2019, doi: https://doi.org/10.1007/s10586-018-1991-8.

[59] L. M. Vargas, "Watermarking based on Difference Expansion and Genetic Algorithms," in *Second International Conference on Advances In Computing, Control And Networking - ACCN 2015,* Bangkok, Thailand, 2015, pp. 12-16.

[60] R. R. Kumari, V. V. Kumar and K. R.Naidu, "Optimized DWT Based Digital Image Watermarking and Extraction Using RNN-LSTM", *International Journal of Interactive Multimedia and Artificial Intelligence*, vol. 7, no. 2, pp. 150-162, 2021, doi: 10.9781/ijimai.2021.10.006

[61] A. Habib and M. Khalil, "QAM-DWT-SVD Based Watermarking Scheme for Medical Images", *International Journal of Interactive Multimedia and Artificial Intelligence*, vol. 5, no. 3, pp. 81-90, 2018, doi: 10.9781/ijimai.2018.01.001

[62] S. Kaur, G. Chaudhary, J. D. Kumar, M. S. Pillai, Y. Gupta, M. Khari, V. García-Díaz and J. Parra Fuente, "Optimizing Fast Fourier Transform (FFT) Image Compression using Intelligent Water Drop (IWD) Algorithm," *International Journal of Interactive Multimedia and Artificial Intelligence*, vol. 3, no. 7, pp. 48-55, 2022, doi: http://dx.doi.org/10.9781/ijimai.2022.01.004

[63] S. Mirjalili, S. M. Mirjalili and A. Lewis, "Grey wolf optimizer," *Advances in engineering software*, vol. 69, pp. 46-61, 2014, doi: https://doi.org/10.1016/j.advengsoft.2013.12.007.

[64] H. Y. Mahmoud, H. M. Hasanien, A. H. Besheer, and A. Y. Abdelaziz, "Hybrid cuckoo search algorithm and grey wolf optimiser-based optimal control strategy for performance enhancement of HVDC-based offshore wind farms," *IET Generation, Transmission & Distribution*, vol. 14, no. 10, pp. 1902-1911, 2020, doi: https://doi.org/10.1049/iet-gtd.2019.0801

[65] C. Banchhor and N. Srinivasu, "Integrating Cuckoo search-Grey wolf optimization and Correlative Naive Bayes classifier with Map Reduce model for big data classification," *Data & Knowledge Engineering*, vol. 127, pp. 101788, 2020, doi: https://doi.org/10.1016/j.datak.2019.101788.

[66] H. Xu, X. Liu and J. Su, "An improved grey wolf optimizer algorithm integrated with Cuckoo Search,", in *2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, Bucharest, Romania, 2017, pp. 490-493.

[67] C. Li and A. C. Bovik, "Three-component weighted structural similarity index," in *Image quality and system performance VI*, vol. 7242, San Jose, California, United States, pp. 252-260, SPIE, 2009.

[68] S. P. Maity and H. K. Maity, "Optimality in distortion control in reversible watermarking using genetic algorithms," *International Journal of Image and Graphics*, vol. 17, no. 03, pp. 1750013, 2017, doi: https://doi.org/10.1142/S0219467817500139.

[69] J. T. Akagi, C. F. Gaona, F. Mendoza, M. P. Saikia and M. Villagra, "Hard and easy instances of L-tromino tilings," *Theoretical Computer Science*, vol. 815, pp. 197-212, 2020, doi: https://doi.org/10.1016/j.tcs.2020.02.025.

[70] X. Yang and X. Jiang, "A hybrid active contour model based on new edge-stop functions for image segmentation," *International Journal of Ambient Computing and Intelligence (IJACI)*, vol. 11, no. 1, pp. 87-98, 2020, doi: 10.4018/IJACI.2020010105.

[71] A. E. H. Saad, Z. Dong and M. Karimi, "A comparative study on recently-introduced nature-based global optimization methods in complex mechanical system design," *Algorithms*, vol. 10, no. 4, pp. 120, 2017, doi: https://doi.org/10.3390/a10040120.

[72] A. Jain and V. Bhatnagar, "Concoction of ambient intelligence and big data for better patient ministration services," *International Journal of*

Ambient Computing and Intelligence (IJACI), vol. 8, no. 4, pp. 19-30, 2017, doi: 10.4018/IJACI.2017100102.

[73] P. Kaur, S. Gupta, S. Dhingra, S. Sharma and A. Arora, "Towards content-dependent social media platform preference analysis," *International Journal of Ambient Computing and Intelligence (IJACI)*, vol. 11, no. 2, pp. 30-47, 2020, doi: 10.4018/IJACI.2020040102.

[74] S. Khan, L. Han, H. Lu, K. K. Butt, G. Bachira and N. -U. Khan, "A New Hybrid Image Encryption Algorithm Based on 2D-CA, FSM-DNA Rule Generator, and FSBI," in *IEEE Access*, vol. 7, pp. 81333-81350, 2019, doi: 10.1109/ACCESS.2019.2920383.

[75] A. Alghafis, F. Firdousi, M. Khan, S. I. Batool and M. Amin, "An efficient image encryption scheme based on chaotic and Deoxyribonucleic acid sequencing," *Mathematics and Computers in Simulation*, vol. 177, pp. 441-466, 2020, doi: https://doi.org/10.1016/j.matcom.2020.05.016.

[76] Y. He, Y. Q. Zhang, X. Y. Wang, "A new image encryption algorithm based on two-dimensional spatiotemporal chaotic system," *Neural Computing and Applications*, vol. 32, no. 1, pp. 247-260, 2020, doi: https://doi.org/10.1007/s00521-018-3577-z.

Lakshmi H R

Lakshmi H R completed her B. E. from Dayananda Sagar College of Engineering (affiliated to Visvesvaraya Technological University - VTU) in Electronics & Communication. She did her M. Tech in VLSI Design & Embedded Systems from B N M Institute of Technology (affiliated to VTU). She is currently pursuing her Ph.D. from K. S. Institute of Technology Research Center (affiliated to VTU). She has over 6 years of experience in her capacity as Assistant Professor and Researcher with topics of interest being – Image Processing, Information Security, VLSI, Embedded Systems. She has won the Young Woman Educator & Researcher Award by National Foundation for Entrepreneurship Development (NFED). She has authored many papers and book chapters in reputed journals and conferences. She has several patent publications. Her peer recognition includes her professional memberships & services in refereed organizations, program committees and review boards.

Surekha Borra

Surekha Borra (Senior Member, IEEE) received her B.Tech. from Nagarjuna University, India, in 2003. MTech. and Ph.D. from Jawaharlal Nehru Technological University, Hyderabad, India in 2007 and 2015. She started her academic career as Assistant Professor in 2004 and served in various engineering colleges for 18 years. Currently, she is Professor in the Department of Electronics and Communication Engineering, K. S. Institute of Technology, Bengaluru, India. Dr Borra's research interests include Image and Video Analytics, Information Security and Signal Processing. She has received Woman Achiever's Award from The Institution of Engineers (India) for her prominent research and innovative contribution(s), and several research grants from the Government of Karnataka, India.