Journal of Information Systems Engineering and Management
2025, 10(13s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Gaussian Iterated Map-Lyrebird Optimization Algorithm (GIM-LOA) and SPIHT Encoding Based Blind Dual Watermarking Scheme for Image

M. Subashini[1], P.V Ravindranath[2]

[1]*School of Computer Studies, Bharathiar University, India. E-mail: subaphd1217@gmail.com*

[2]*School of Computer Studies, Bharathiar University, India. E-mail: ravindranath@rvsgroup.com*

ARTICLE INFO

Received: 27 Nov 2024
Revised: 05 Jan 2025
Accepted: 30 Jan 2025

ABSTRACT

A prominent area of study in digital Multimediaresearch is the Digital Watermarking (DWM) method, which has shown promise as a copyright protection tool. Blind watermarking schema and non-blind Water mark schema are the two classifications under which watermarking algorithms fall. The dual blind WaterMark (WM) technique in this work employs the Stucki Kernel halftone (SKH) algorithm, Set Partitioning in Hierarchical Trees (SPIHT), and selfrecoveries in images to detect tampering. and the Gaussian Iterated Map-Lyrebird Optimization Algorithm (GIM-LOA). SPHIT is used to rebuild the image. SPHIT can produce a bitstreams at desired rates including coefficientsof Wavelet Transforms. In the event that the received bit stream is interrupted, sound progressive transmission can be used to reconstruct the image. GIM-LOA is introduced for watermark bit mapping in an iteration-based method, utilizing its members' searching skills in water embedding. Each lyrebird, as a member of the LOA, determines the values of the Watermark bits according to its bit position. Updating the optimal bit solution should also be made easier by comparing the Objective Function (OF) values and authentication bit are generated using recovery bits prior to inserting the watermark, shuffle the WM components using GIM-LOA and Arnold Cat Mapping (ACM) and thus improving security and quality of the image recovery. The suggested algorithm performs better than current methods in terms of many statistical metrics and security elements of Tampering Detection (TD) techniques, and it is protected against various attacks.

Keywords: Arnold Cat Map (ACM), Stucki Kernel halftone technique, Gaussian Iterated Map-Lyrebird Optimization Algorithm (GIM-LOA), authentication bit (Auth bit), image self-recovery, Set Partitioning in Hierarchical Trees (SPIHT).

INTRODUCTION

Multimedia data is becoming a significant information source for individuals these days. Multimedia data tampering occurs when people take advantage of Digital Technology's ease. If tampered data is used in formal settings, our lives will be negatively impacted. It is necessary to protect these digital assets. To identify the integrity and validity of digital data, Digital Watermark has been a crucial component of the solution. Multimedia communication has undergone a significant change due to Information Technology. Along with the other advantages, it risks the secure ownership of digital media, as it makes digital data easier to distribute, operate, and replicate. Robust Watermarking approaches that can withstand related attacks are crucial because, in real-world applications, Digital Images with watermarks may be vulnerable to various attacks, including compression, cropping, tampering, rotation, and scaling.

The Watermark image is created by hiding a secret mark in the host multimedia and communicating it through a physical transmission channel by a technique called Digital Image Watermark [1-3]. Digital content can now be readily recovered, copied, and distributed without authorization. From the recovered image, the Watermarking is then detected or extracted. Ensuring authorization and tamper resistance were considered to be Watermark's objectives. The safety of copyright and content authentication are the two most crucial aspects of the image Watermark. Depending on the kind of data being watermarked, the Watermark might be image, audio, video, or text-based.

The three primary categories of Digital Imagewatermarking schemes are semi-fragile Watermark, Fragile watermark (FWM), and robust Watermark [5], which are based on the various application scenarios [4]. A robust Water Mark system can thwart most attacks, including malicious and signal processing attempts [6]. Robust watermark schemes are often utilized in copyright protection because of this property [7]. On the other hand, the FWM method, frequently used to authenticate image or video content, is vulnerable to many attacks [8]. Based on the sensitivity level, the FWM scheme can be divided into semi-fragile Watermarks and FWM.

On the other hand, self-recovery schemes have become an essential field of study. During the authentication process, extracted Watermarksof original imagesare compared with content data to determine if images' contents have changes. Analyzing the tampered image and its region allows for the restoration of the Tampered Region (TR). The image's TR is restored using a self-recovery FWM technique. The method used to recover the watermark affects the image quality. Watermark generations (WMG), embedding location selections, and TD performances all contribute effectively in recovering tampered images.

In robust Water Mark algorithms, the WMG is the main step. The WMG or Water Mark pre-processing can enhance the Water Mark algorithm, as it randomly scrambles water mark. The process of embedding binary strings containing the author or copyright data in the original image via a particular embedding algorithm is called Watermark embedding.The balance between the Watermark's resilience and invisibility must be considered in the embedding algorithm.

Authentication WMG and recovery WMG are the two categories into which WMG falls. For instance, using bit substitutions or other mathematical operations, using a cover image, the Least Significant Bit (LSB) based approaches apply the Watermark [9]. The invisibility of LSB-based approaches is enabled by easy replacement; however, statistical examination reveals that these methods are less robust. The Watermark is placed on different image domains by more sophisticated Watermark systems. While maintaining fidelity, the frequency domain capacity was enhancedby Shih and Zhong [10]. Nevertheless, the Watermark image has significant distortion after embedding since it requires additional embedding capacity.

Qin et al. [11] were the first to propose image hashes with folds for the purpose of creating authentication bits. Each block's recovered bits are encoded using an adaptive bit allocation algorithms based on lower frequencies of Non-Subsampling Contour Transform (NSCT) coefficients.

A method for compressing watermark data was suggested by Ansari et.al. [12] to reduce the watermark embedding ability. After extraction, this compressed Water Mark data can be decoded. However, this algorithm attains low efficiency. But this algorithm lost some of its efficiency. In general, the original image may be considerably distorted by the conventional techniques of inserting Water Mark data into the host image. However, self-recovery is another benefit it offers. The low packet signal noise ratio of recovered images and small attack resistance area are problems that most algorithms have faced. The study introduces a blind dual watermark strategy for image self-recovery and TD. It uses the Stucki Kernel halftone technique, GIM-LOA, and SPIHT. This application enhances the accuracy of the TD, and the self-recovery quality is also ensured.

SPIHT encoding produces the primary recovery bit, and the Stucki Kernel halftone approach produces the secondary recovery bit [13]. Apply the logical operation to generate the authentication bit based on this basis. Moreover, to increase security and tamper recovery rate, ACM [14–16] and GIM-LOA are introduced during embedding [17]. At last, the LSB method is used to embed the Watermark into the original image. In order to protect the Water mark information from different types of attacks, a more robust Watermark is used.

LITERATURE REVIEW

Haghighi et al. [18] introduced dual delicate watermarks for TD and self-recoveries which generated two image digests from host images by utilizing rising wavelets and half-toning them. As a result, for every 2 x 2 non-overlapping block, there are two opportunities for recovering tampered blocks. Next, the image digests are used to obtain the authentication bit. For every image block, two LSBs contain a total of eight bits encoded in them. To improve the digest's quality, the LSB Rounding approach is suggested. The mapping blocks and LSB scrambling are determined using the ACM. Shift-aside measures are recommended to increase the rate of recuperation. Because the data stored in each block depends on the key allocated to it, copy-move, vector-quantization, and other LSB manipulation are avoided. Therefore, the test results show that the recommended TRLH outperforms alternative techniques..

Image TD and Image recovery using Lifting Wavelet Transform (LWT) and Genetic Algorithm (GA) is made possible by Haghighi et al.'s [19] effective fragile blind quad Water mark system, called TRLG. By identifying the different kinds of image blocks, TRLG produces four extremely high-quality compact digests using the LWT and halftoning techniques. A unique parameter estimate technique is used with the GA for enhaning and optimizing qualities of digests and the Watermark images. In addition, the mapping block for the information's Embedding, encryption, and shuffle is found using the Chebyshev System. To increase the recovery rate, partner-block and mirror-aside are suggested.

To demonstrate how TRLG is superior to SOTA techniques, tests are conducted on the security, tamper region (TR), and watermark and recovered image quality. The data indicates that the image with Watermark has a Structural Similarity Index Measure (SSIM) of 1 and an average Peak Signal-to-Noise Ratio (PSNR) of around 46 dB. Roughly 90% of the restored images had average PSNR values. and SSIM have damaged about 24 dB and 0.86.

A self-recovery-based FWM system was suggested by Chang et al. [20] for enhancing watermark image qualities.A bit-reduction method called Absolute Moment Block Truncation Coding (AMBTC) uses fewer bits to create a watermark. Watermarks are incorporated into original images using concealed turtle shellbased data. TD phases use dual levels to achieve high accuracy for tampered localized areas.

To further enhance restored IQ, an image inpainting method and an efficient self-adaptive weight-based recovery strategy are used. 34.65 dB was attained by average PSNR recovered images and it is > than other standard methods. Water mark images exhibitadvanced quality upto 49.76 dB and it was revealed in the test outcomes.

Gul and Ozturk [21] introduced a novel self-embedded FWM technology that employs a triple recovery information embedding mechanism. Their schema divided host images into 16 main pieces and generated Look-Up tables for recovering highly tampered images in groups of four partner blocks from main blocks.

The three extra partner blocks of recovery data are combined to provide triple recovery data for each partner block. Rec bits were added to 1st and 2ndLSBs of initial 3 sub-blocks in partnering blocks.

Using the Message Digest Algorithm 5 (MD5) Hash Function (HF), the pixels of the 16 × 16 embedded image blocks with Rec bits are used to retrieve Auth bits.

Watermark technology is the basis of a strategy put forth by Liu and Yuan [22] to safeguard image content from malicious tampering where different check bits were used to identify tampered region localizations and Rec bitswere placed into original images' three LSB planes for image recoveries. Using Parity Check Bits (CB) Labelled method, first CB was initially created for each pixel and second check bit obtained by hashing each block onimage decompositions.The likelihood of false-negative errors is partially reduced by the superposition result found from the two CBs. Additionally, post-processing techniques raised the accuracy of TD results. Their experimental data showed that their strategy worked well for both improving TD resultaccuracy while maintaining better recovered image qualities.

Faheem et al. [23] presented digital watermarks based on the LSB utilizing Image Gradients (IG) and Chaotic Maps (CM), where the WM was scrambled using Piecewise Linear CM (PWLCM) and a chaotic substitution box (S-Box). PWLCM has a positive Lyapunov exponent and a greater balancing characteristic than other CMs. The generated sequence with high nonlinearity can be produced by this S-Box approach. Direct pixel manipulation and a large payload capacity were offered by the LSB embedding technique. The balance between resilience and imperceptibility is introduced by the embedding payload. In order to prevent image degradation, the IG approach can be used to determine where a Watermark should be embedded. As long as the Watermark signal remains undetectable, the experimental outcomes demonstrate a reasonable level of development in robustness against several geometrical attacks and image processing.

Quantum Water Marking (QWM) incorporates the image self-recovery water mark suggested by Wang et al. [24]. A novel self-recovery Watermark approach with tamper localization is presented for quantum images. For image recovery, TD, WMG, and Embedding, the suggested approach uses a 2x2 non-overlapping image block as the fundamental building block. Recovery qubits for image recovery and authentication qubits for TD are among the Watermark qubits placed in the carrier image. TD accuracy is improved by designing a two-level TD and tamper localization approach. Two distinct image recovery models are developed based on the outcome of TD to improve the quality of recovered images. Quantum circuits are used to put the suggested QWM algorithm into practice. The testing results show that the new approach works well and performs well in self-recovery against various malicious attacks as well as image TD.

SPIHT and SKH technique was employed for the TD and image self-recovery known as TRSSKH by Zhang et al. [25] in their study who suggested blind dual Water mark strategies with Watermarksgenerated from recovered bits for image restorationswhile authentication bits identified tampered areas. In images. Two Rec bits ensured that altered images were recovered properly. Their primary Rec bitswere SPIHT encoded while secondary recovery bit were produced using Stucki Kernel halftones. Subsequently, the recovery bits are used to generate the authentication bit. Before inserting the water mark, shuffle its components using diagonal and ACM forbetter security and quality of restored images. The Water mark image's invisibility is ensured by embedding it into the original image using an LSB-based Water mark approach. The suggested approach can achieve good restoration quality, according to the results of experiments done on two datasets: Break Our Watermarking System 2 (BOW2) and USC Signal and Image Processing Institute (SIPI), or USC-SIPI. The suggested method performs better and is superior when compared to the current works.

Fan [26] proposed a blind dual image water mark method for self-recovery, copyright protection, and Tamper Proofing (TP). For copyright protection, use a robust watermark in the form of a binary handwritten signature that is highly correlated with the owner. Next, include the Watermark into a hybrid domain that was made with Discrete Cosine Transform (DCT) and Dual Tree Complex WT (DT-CWT). Source encoding output bits generated by SPIHT encoding are inserted into the image based on LSB replacement, whereas hash-based check bits are employed for TP. Furthermore, the approach of recurrent encoding is employed to enhance the resilience of self-recovery.

The suggested Water mark mechanism has the ability to discriminate between tampered areas of an image and survive various IP attacks, as demonstrated by experimental results. Additionally, the system can detect and recover tampered areas of an image with accuracy. It has the ability to synchronously locate applications for content authentication and joint ownership.

The authenticity of every block is confirmed by the three-level hierarchical TD techniques developed by Singh et al. [27]. Thus, there is a substantial possibility that each block's authenticity can be verified. The results of the experiment demonstrate the high-quality restoration that can be accomplished by the planned plan. Up to 50.00% tampering rate and a high PSNR and Normalized Correlation Coefficient make recovery possible. Because the suggested technique uses smallest size non-overlapping blocks, it also removes blocking artefacts and enhances the precision of TR.

Li et al. [28] reported a water mark method for image authentication with self-recovery capability based on dual-matrix and block mapping. Their integrated Water Marksencompassedrecovery data with authentications. Their introduced Authentication Feature Composition Calculation approach generated authentication data for image TD and localizations. Additionally, recovery data of tampered areas hadmapped-Rec bits andself-Rec bits. SPIHT encodes generated self-recovery bits, while Rehashing Modelbased Block Maps obtained mapped-Rec bits for rescuing tampered codes. Subsequently, using dual-matrices Water mark data had DWM incorporated into original images. With a big Water mark payload of up to 3.169 bpp, ideal IQ over 40 dB, and effective protection against malicious attacks like collage and copy-move attacks, it provides all of these benefits.

PROPOSED METHODOLOGY

The TD and image self-recovery known as TRSGSKH is achieved in this study by using the SPIHT and GIM with Stucki Kernel halftone approach. The Stucki kernel can serve as authentication data in addition to offering a second opportunity at recovery. To further improve security, the coefficients in each block are also scramble and encrypted using the GIM-LOA and ACM. Figure 1 illustrates the generation and Embedding of the Water mark. After the Rec bits are formed, a logical operation among 2 recovery bits provides the Auth bits, providing a more dependable and accurate detection technique. In the end, the host image's LSB planes include the Water mark, which is made up of recovery bits and authentication bits.

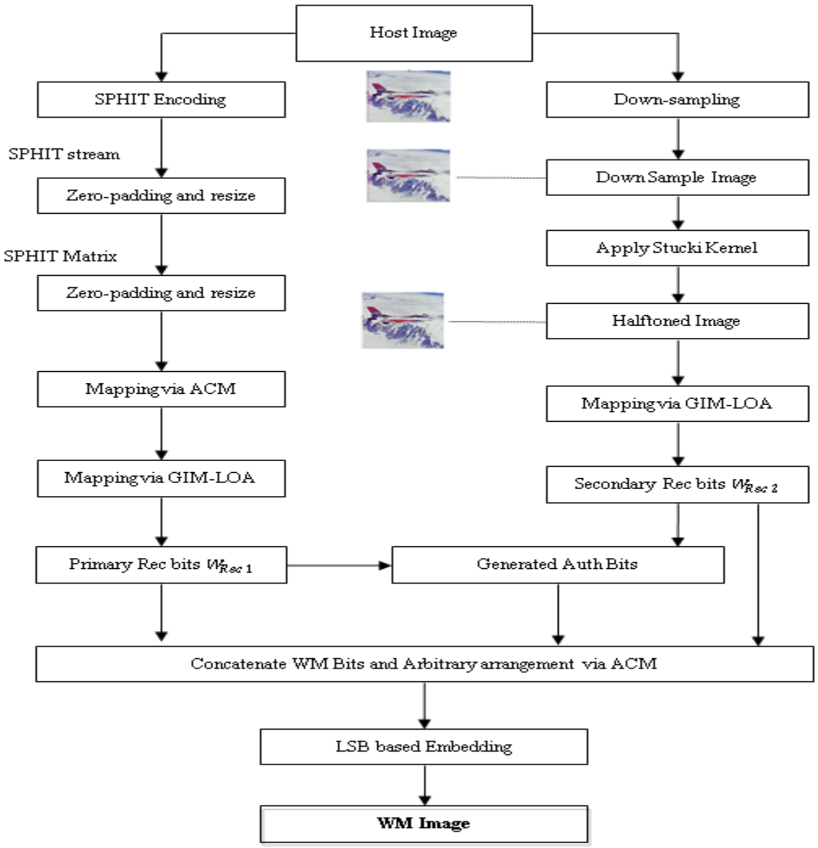


FIG 1. DIAGRAM OF CREATING AND EMBEDDING Water Mark

1.1. GENERATING AND EMBEDDING Water Mark

The Rec bits are generated by introducing the SPIHT and Stucki kernels, to the host image, generating the primary Rec bits, W_{Rec1}, and secondary Rec bits, W_{Rec2}.

When compressing digital signals, SPIHT is a commonly used embedded compression technique.

1.1.1. SPIHT encoding

SPIHT can create a bitstream of Wavelet Transform coefficients at a desired rate when there is suitable progressive transmission.If the bit stream that is being received is interrupted, it can still be utilized to recreate the image.W_{Rec1} is generated using SPIHT. The multi-resolution Wavelet Transform coefficients that are normalized are categorized by SPIHT based on their magnitudes. For improved quality, send them after following a significant bit order. Due to the fact that the output rate employed affects the quality of the reconstruction [22].

The decoder will also be able to use the same procedure in inverse.

Given that the host image is 512 ×512, the bit stream length should be 393172 and the compression rate should be set to 1.5 bpp in order to meet the requirement. Consequently, Zeros-Padding (ZP) and resizing will result in the generation of the 256x256 SPIHT matrix.

1.1.2. ACM and GIM-LOA based mapping

To shuffle the outcome, ACM and GIM-LOA are introduced in this work.

ACM: Starting from the left, split the matrix into 4 equal columns (p1, p2, p3, and p4). These are the particular steps. when the ACM-created coefficients are located at position p1. Next, distribute them across positions p3, p2, and p4. The process will be repeated on the right side of the matrix. When the TR are on the left or right side, they might be saved and utilized to recreate the original image. The suggested method can therefore be strengthened against vector quantization and copy-move attacks with the use of the mapping procedure.

GIM-LOA: Based on the Wavelet Transform coefficients, lyrebirds make up the population in the population-based metaheuristic method known as the GIM-LOA technique. By leveraging the members' search capacity in the tampered regions, GIM-LOA can offer appropriate solutions for tampered regions in an iteration-based approach.

Based on its location in the tampered regions, each lyrebird as a member of GIM-LOA decides the values of the recovery bits. A vector that represents each element of the vector as a recovery bit can be used to model every lyrebird. Equation (1) states that the Wavelet Transform of coefficients that the method represented using a matrix are composed of the GIM-LOA members. Equation (2) is used to randomly initialize each GIM-LOA member's position in the tampering recovery rate [29].

$$X = \begin{bmatrix} x_{1,1} & \cdots & x_{1,d} & \cdots & x_{1,m} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ x_{i,1} & \cdots & x_{i,d} & \cdots & x_{i,m} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ x_{N,1} & \cdots & x_{N,d} & \cdots & x_{N,m} \end{bmatrix}_{N\times m} \quad (1)$$

$$x_{i,d} = lb_d + r.(ub_d - lb_d) \quad (2)$$

Here, the GIM-LOA population matrix is denoted as X. The i^{th} member of the LOA (Candidate Solution (CS)) is X_i. In tampered regions, its d^{th} dimension is $x_{i,d}$. Number of lyrebirds is denoted as . A random number (r) in the interval [0,1], and the number of Rec bits is denoted as m . The lower bound of the d^{th} tampered region is denoted as $lb_d$and the upper bounds of the d^{th} tampered region is denoted as ub_d. The OF of the tampered region can be assessed based on the TD rate, given that every GIM-LOA member corresponds to a potential solution to the tampered region. Equation (3) [29] can be used to express the collection of evaluated values for the OF of the TD as a vector.

$$F = \begin{bmatrix} F(X_1) \\ \vdots \\ F(X_i) \\ \vdots \\ F(X_N) \end{bmatrix}_{N\times 1} \quad (3)$$

$F_i$represents the evaluated OF depending on thei^{th} GIM-LOA member, while F is the vector of the evaluated OF. The two phases of the population update process are (i) hiding (exploitation phase) and (ii) escaping (exploration phase), based on the lyrebird's decision in this case. Equation (4) simulates the lyrebird's tampered region procedure, which determines which escape or hiding strategy to employ in an emergency situation in the GIM-LOA design. Consequently, only one of the first or second phases is used to update each GIM-LOA member's position during an iteration [29].

$$Update\ process\ for\ X_i: \begin{cases} Phase\ 1, r_p \le 0.5 \\ Phase\ 2, else \end{cases} \quad (4)$$

r_p is a random number that falls between 0 and 1.(i.e., [0, 1])

Phase 1: Escaping Strategy (Exploration Phase)

In GIM-LOA phase, the population member's location is updated in the TR space by modeling the lyrebird's (LB) departure from the recovery bit locations and the danger location of the tampered region.

GIM-LOA's exploration capability in Global Search (GS) is demonstrated by the numerous modifications and scanning of many regions in the tampered region that occur when the lyrebird is moved to a safe location. In the GIM-LOA design, each member's Rec bit is considered to be a position of other population members with greater OF values.

Equation (5) can therefore be used to identify the set of recovery bit areas for every GIM-LOA member.

$$SA_i = \{X_k, F_k < F_i \ and \ k \in \{1, \dots, N\}\}, where\ i = 1, \dots, N \quad (5)$$

Here, Thek^{th} row of X matrix is denoted as X_k. Then, $F_k < F_i$, as it has good OF value (F_k) than the i^{th} LOA member. One of these safe areas (SA) (the recovery bit) is considered to be the LB's random path of escape in the GIM-LOA concept. The set of SA for the i^{th} LB is denoted as SA_i..Based on the LB displacement modeling finished in this stage, a new modified region location is calculated for every GIM-LOA member using equation (6). Equation (7) then illustrates how the new tampering region location is substituted for the previous one of the appropriate member by enhancing the OF.

$$x_{i,j}^{P1} = x_{i,j} + r_{i,j}.(SSA_{i,j} - I_{i,j}.x_{i,j}) \quad (6)$$

$$X_i = \begin{cases} X_i^{P1}, F_i^{P1} \le F_i \\ X_i, else \end{cases} \quad (7)$$

Here, the OF value is represented as F_i^{P1}, random numbers within the range [0, 1] is represented as $r_{i,j}$, The integers that are randomly selected as 1 or 2 is represented as $I_{i,j}$. Then, the selected SA for thei^{th} lyrebird is denoted as SSA_i.Its j^{th} dimension is denoted as $SSA_{i,j}$. For the i^{th} lyrebird, X_i^{P1} is the new position calculated based on escaping strategy of the GIM-LOA.

Phase 2: Hiding Strategy (Exploitation Phase)

During this GIM-LOA phase, the population member's position is changed in the tampering region space according on the lyrebird's modeling strategy for concealing itself in the surrounding SA. As a result of accurately scanning the environment and taking little steps to reach an efficient hiding location, the lyrebird's position shifts slightly, demonstrating the effectiveness of GIM-LOA for local search (LS). Drawing from the simulation of the LB's migration towards a nearby area suitable for concealing wavelet coefficients, equation (8) is utilized to compute a new TR position for every GIM-LOA member. If this new position increases the value of the OF as per equation (9), it substitutes the prior tampered region location of the related member.

$$x_{i,j}^{P2} = x_{i,j} + (1 - 2r_{i,j}).\frac{ub_j - lb_j}{t} \quad (8)$$

$$X_i = \begin{cases} X_i^{P2}, F_i^{P2} \le F_i \\ X_i, else \end{cases} \quad (9)$$

Here, t implies iteration counters, $r_{i,j}$stands for random values between [0, 1], F_i^{P2} represents OF values, X_i^{P2}stands for TR positions determined for i^{th}LBs based on GIM-LOA hiding strategies, and $x_{i,j}^{P2}$implies theirj^{th} dimensions. In first iterations of GIM-LOA LB positions are updated based on equations (4)–(9) then moves on to the following iteration of the algorithm, which runs until the last iteration. The optimal CS is updated and saved after every iteration. The optimal CS that was saved during the algorithm's iterations is output as a recovery bit to the tampered region following the complete execution of GIM-LOA.

The coefficients in each block are encrypted as real intervals determined by Gaussian functions using Gaussian Iterated Maps, nonlinear iterated maps of shuffles [30],

$$x_{n+1} = \exp(-\alpha x_n^2) + \beta \quad (10)$$

The recovery bits and real parameters for the tampered region are represented by α and β. Algorithm 1 presents the GIM-LOA pseudocode.

ALGORITHM 1. PSEUDOCODE OF GIM-LOA

```
Start
Input recovery bits, tampered regions, and Wavelet Transform coefficients
Set up the GIM-LOA iterations (T) and population size (N).
Using Wavelet, create the initial population matrix. Use Equation (2) to transform coefficients.
Use Equation (3) to determine  OF.
Depending on the affected location, determine the optimal CS.
For t = 1 to T
For i= 1 to N
Obtain lyrebird defense strategies against predators withEqn (4)
If $r_p$  ≤  0.5 (chose Phase 1)
Determine the candidate SA for i^th lyrebird based on Equation (5).
Use Eqn (6) to calculate the ith LOA member's new altered region location.
    Use Equation (7) to update the GIM-LOA member.
Else (choose Phase 2)
```

```
Compute tampered regions of $i^{th}$ GIM-LOA memberswith Eqn (8)
    Update $i^{th}$GIM-LOA membersusing equation (9)
End (If)
End For i
  Save best CSas tampered regionsand compute GIM
End for t
Output best quasi-optimal solutionsfound by GIM-LOA
End
```

1.1.3. Stucki Kernel Halftoning Technique

However, the original image is compressed to half its original size using the halftoning approach, which results in the W_{Rec2}, which are needed to refine the restoration quality. When a continuous tone image is quantized to a small number of colors, the resultant image retains its original appearance and is referred to as halftone. The $W_{Rec2}$are obtained after GIM-LOA in the suggested technique, which uses the Stucki kernel.

1.1.4. Authentication

The authentication bits are then computed using the W_{Rec1} and W_{Rec2} that have been created. The suggested approach calculates one authenticate bit from each block of $b \times b$ that is created when blocking is first applied to a host image of size $M \times N$. This implies that every 2x2 block will have one bit created as the authenticate bit. The $Num_{i,j}$ can be computed using equation (11), which requires expressing the generated W_{Rec1} in binary form and expressed it as $c_{i,j}^{k}, \dots c_{i,j}^{o}$.

$$Num_{i,j} = \sum_{n=o}^{k} c_{i,j}^{n} \tag{11}$$

Here, k is the number of bits and the coefficients is represented as $c_{i,j}$. Equation (12) can then be used to calculate the corresponding $Flag_{matrix}$.

$$Flag_{matrix} = \left[Num_{i,j}, mod2\right] \tag{12}$$

In conclusion, the logical operation employing equation (13), the authentication bits W_{auth} was generated.

$$W_{Auth} = Flag_{matrix} \bigoplus W_{rec2} \tag{13}$$

The Water mark data can be created by concatenating W_{Rec1}, W_{Rec2}, and W_{Auth} after W_{Rec1}, which are 6 bits per block (bpb), W_{rec2}, which is 1 bpb, and the W_{Auth}, which are 1 bpb, have been generated. The Water mark data will subsequently be added in the host image's 2 LSB planes.

DETECTING AND RECOVERING TR

To identify and retrieve the TR, the Water mark data from the received Water mark image is extracted.

The Rec bits and W_{Auth} will be created using the ACM, in a manner similar to that of the previously stated Water mark generation.

Similar to the process for generating a Water mark, the W_{Auth} can be computed once the recovery bits have been extracted. By contrasting the extracted $W_{Auth}$with the calculatedAuth bits, locate the TR. Based on this, the extracted Rec bits can be used to recover the TR. First, the image is blocked into 2x2 blocks that contain the Water mark information. Then, each block's 2 LSB of each pixel is extracted to extract the Water mark information.

Eight bits can be recovered from each block once the information is extracted by ACM and permuted and decrypted. $W_{Ext_{Rec1}}$, the W_{Rec1}, is the first six bits in each block. $W_{Ext_{Rec2}}$, the sW_{Rec2}, is the seventh bit, and $W_{Ext_{Auth}}$, the extracted W_{Auth} , is the eighth bit. Equations (11–13) can be used to determine the corresponding W_{Auth}, $W_{Cal_{Auth}}$ based on the extracted recovery bits. Equation (14) can be used to identify the tampered regions from $W_{Ext_{Auth}}$ and $W_{Cal_{Auth}}$. It is mentioned that in order to increase the TD rate, morphological procedures like closing operations should be applied to the $Tamp_{region}$.

$$Tamp_{Region}(i,j) = W_{Ext_{Auth}}(i,j) \oplus W_{Cal_{Auth}}(i,j) \quad (14)$$

Utilizing the recovery bits, the tampered regions are recovered once they have been located. ACM and GIM-LOA should de-map the Watermark as a number of mapping procedures have been used to improve the security of the Water mark data. Firstly, the 256×256 matrix $W_{Ext_{Rec1}}$ is created by retrieving six bits from each block in the Water mark image, which correspond to the coefficients of SPIHT. In spare bits put 0 during the Water mark generation and embedding stages to meet capacity needs. To obtain the original bitstream, the matrix must be resized and the crucial bits must be removed. Using SPIHT coefficients to decode SPIHT and rebuild the image.

Use the Stucki Kernel approach on $W_{Ext_{Rec2}}$for reconstructing the halftone image effectively [25].

The detected TR can be removed and then rebuilt into the input image, creating the reconstructed image, using the halftone image and the SPIHT decoded image.

EXPERIMENTAL RESULTS AND DISCUSSIONS

BOW2 from https://data.mendeley.com/datasets/kb3ngxfmjw/1and USC-SIPI image database from https://sipi.usc.edu/database/ to assess both the suggested method's and the current methods' performance. The metrics given in equations (15)–(17) are Precision, Recall, and F1score. To assess the TD results, these metrics are computed.

The total effectiveness of the detecting method is represented by the F1score. Here, Precision and Recall are combined to compute the F1 score.

Recall measures the capacity to identify tampered pixels correctly, whereas Precision measures the percentage of actually tampered with pixels among those that are labeled as tampered with. Equations (18) and (20) are used, respectively, to compute the PSNR and SSIM [18] as a means of assessing the quality of recovered images.

An IQ can be assessed using the PSNR index, which measures how similar the original and recovered images are to one another. The greater the PSNR, the better the recovered image. Three comparative measures: luminance, contrast, and structure are utilized by SSIM to determine how similar two images.

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \quad (15)$$

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} \quad (16)$$

$$\text{F1 score} = \frac{2\text{TP}}{2\text{TP} + \text{FP} + \text{FN}} \quad (17)$$

Here, TP stands for True Positive, indicating that the classifier successfully identified the sample and regarded it as positive. The symbol TN stands for True Negative, indicating that the classifier properly identified the sample and regarded it as negative. False Positive abbreviated FP, indicates that the classifier's identification result is incorrect and that the sample is regarded as positive. False Negative abbreviated FN, indicates that the classifier misinterpreted the recognition result and regarded the sample as negative.

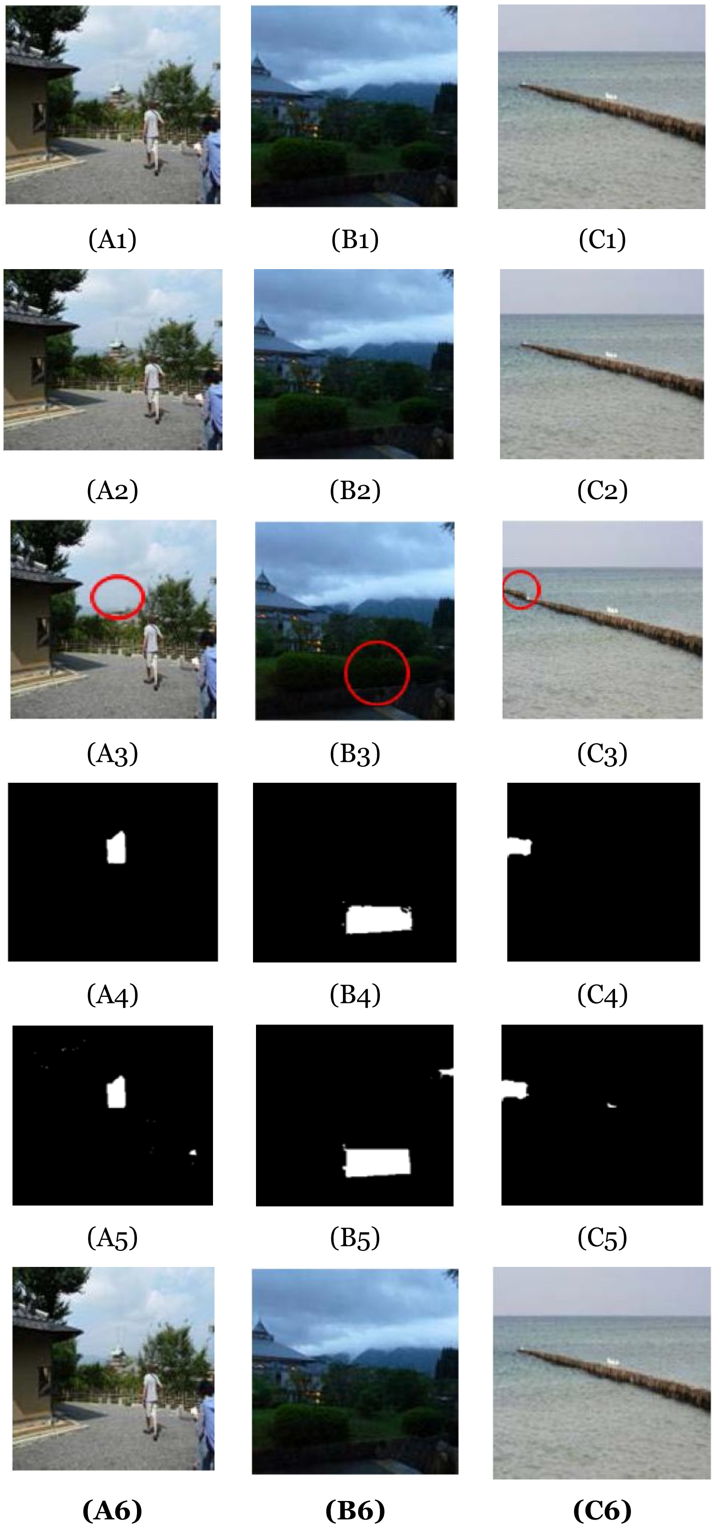
$$\text{PSNR} = 10 \log_{10}\left(\frac{MAX^2}{MSE}\right) \quad (18)$$

$$\text{MSE} = \frac{1}{\text{a} \times \text{b}} \sum_{\text{a}=0}^{\text{a}-1} \sum_{\text{b}=0}^{\text{b}-1} \left(\text{f}(\text{x},\text{y}) - \text{f}'(\text{x},\text{y})\right)^2 \quad (19)$$

Here, $a \times b$ denotes the image size and Mean Square Error (MSE) is determined by equation (19),

$$SSIM = \frac{(2\mu_1\mu_2 + c_1)(2\sigma_{12} + c_2)}{(\mu_1^2 + \mu_2^2 + c_1)(\sigma_1^2 + \sigma_2^2 + c_2)} \quad (20)$$

Here, the variance of 2 images is represented as σ_1 and σ_2. Mean values for two images are denoted asμ_1,μ_2. The covariance of two images is represented by the σ_{12} . Two constant values are $c_1$and c_2.



(A1) (B1) (C1)

(A2) (B2) (C2)

(A3) (B3) (C3)

(A4) (B4) (C4)

(A5) (B5) (C5)

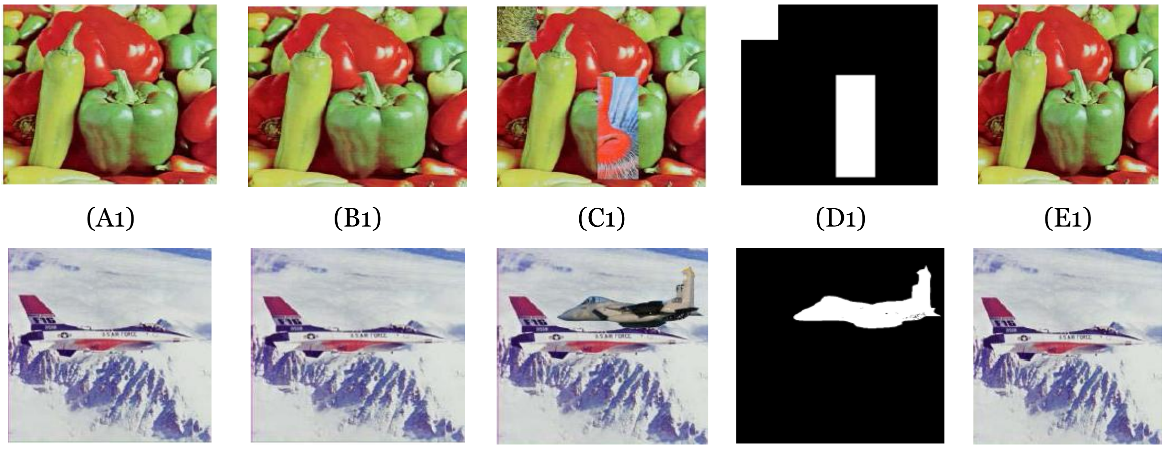
(A6) (B6) (C6)

FIGURE 2. IILUSTRATION OF THE OUTCOMES OF THE SUGGESTEDSYSTEM

First row: (A1) ~(C1) the original images, "barrier," "hedge," and "japan tower," Second row: the watermarked image (A2) ~ (C2); Third row: tampered images (A3) ~ (C3); Fourth row: the ground truth (A4) ~ (C4) Fifth row: (A5) ~ (C5) the altered results found; Sixth row: comparable recovered images (A6) ~ (C6). The suggested scheme is demonstrated in Figure 2 using the examples of "japan tower," "hedge," and "barrier" from the BOW2 dataset. The host images with varying textures can be seen in the first row. The equivalent Water mark images, which are near to the host image and acceptable to the human visual system, are presented in the second row.

The tampered images are presented in the third row. It is clear that there are different kinds and degrees of tampering because the tampered areas are marked with a red circle.

The ground truth is presented in row four, detected results are presented in row five, and recovered images are presented in row six. The outcomes demonstrate the extent to which the suggested strategy works for both image recovery and TD. In addition to the subjective assessment, reliable metrics are used to evaluate the performance.



(A1) (B1) (C1) (D1) (E1)

(A2) (B2) (C2) (D2) (E2)

FIGURE 3. PERFORMANCE OF SUGGESTEDSYSTEM UNDER MULTIPLE TAMPERING AND SPLICING TAMPERING

Figure 3: First row: multiple tampering (A1) ~(E1), Second row: splicing tampering (A2) ~(E2). First column: initial images (A1) (A2); second column: Water mark images (B1) (B2); third column: tampered images (C1) (C2); Fourth column: ground truth (D1) (D2); fifth column: detected tampered regions (E1) (E2); and sixth column: recovered images (F1) (F2). PSNR and SSIM are used for assessing the quality of the Water mark and recovered images, while F1score, Precision, and Recall are employedfor assessing the TD outcomes, and it is presented in Table 1.

TABLE 1. SUGGESTEDSYSTEMEFFICIENCYFOR VARIOUS METRICS

Test Images	Precision (%)	Recall (%)	F1-Score (%)	Water Mark Image	Recovered Image	
				PSNR (dB)	PSNR (dB)	SSIM
Japan Tower	92.55	96.77	94.62	49.4521	45.3718	0.9954
Hedge	91.23	95.96	93.54	49.6763	42.7815	0.9875
Barrier	92.36	93.41	92.88	49.6585	42.3483	0.9936

TABLE 2(A).CURRENTAPPROACHES VS. PSNR AND SSIM

Image	TRLH				TRSSKH			
	Color		GS		Color		GS	
	PSNR (dB)	SSIM	PSNR (dB)	SSIM	PSNR (dB)	SSIM	PSNR (dB)	SSIM
Baboon	46.3251	0.9985	46.3514	0.9951	46.3841	0.9991	49.5412	0.9974
Barbara	46.3294	0.9978	46.3583	0.9942	46.3847	0.9983	49.4454	0.9965
Lena	46.2353	0.9925	46.2894	0.9905	46.3756	0.9942	49.4175	0.9956
Pepper	46.2047	0.9917	46.2588	0.9908	46.3792	0.9959	49.3312	0.9959
Lake	46.2819	0.9921	46.3251	0.9910	46.3685	0.9963	49.3023	0.9967
F16	46.3054	0.9905	46.3347	0.9872	46.4126	0.9921	49.3255	0.9948

TABLE 2(B).SUGGESTED METHOD VS. PSNR AND SSIM

Image	TRSGSKH			
	Color		GS	
	PSNR (dB)	SSIM	PSNR (dB)	SSIM
Baboon	46.4218	0.9995	49.6536	0.9979
Barbara	46.4259	0.9987	49.4565	0.9972
Lena	46.4064	0.9956	49.4289	0.9961
Pepper	46.4075	0.9964	49.3624	0.9963
Lake	46.3992	0.9968	49.3338	0.9972
F16	46.4341	0.9937	49.3541	0.9954

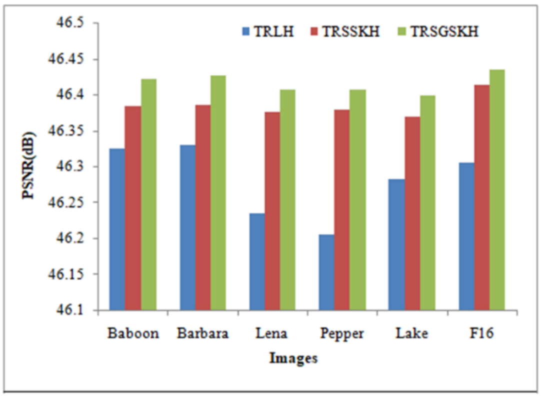


FIGURE 4. PSNR COMPARISON VS. WATERMARKING SCHEMES (COLOR IMAGES)

The samples from the USC-SIPI image dataset under various color images, as shown in Figure 4, to demonstrate the effectiveness of the suggested strategy. TRLH has lowest PSNR comparison of 46.3251 dB, 46.3294 dB, 46.2353 dB, 46.2047 dB, 46.2819 dB and 46.3054 dB for Baboon, Barbara, Lena, Pepper, Lake and F16 images (Table 2(a)). TRSSKH has lowest PSNR comparison of 46.3841 dB, 46.3847 dB, 46.3756 dB, 46.3792 dB, 46.3685 dB and 46.4126 dB for USC-SIPI image dataset (Table 2(a)). For the images of USC-SIPI image dataset, the highest PSNR comparison for the suggested schema is 46.4218 dB, 46.4259 dB, 46.4064 dB, 46.4075 dB, 46.3992 dB, and 46.4341 dB (Table 2(b)). The recovered outcomes are presented in the final column, with the associated PSNR estimated as 46.4341 dB for `F16', based on the TD outcomes.

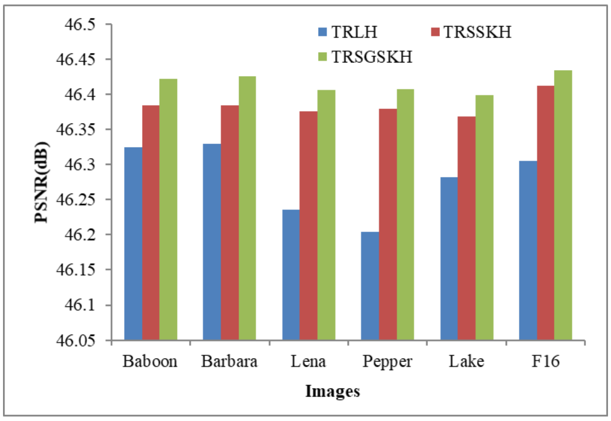


FIGURE 5. PSNR COMPARISON VS. WATERMARKING SCHEMES (GRAY-SCALE IMAGES (GSI))

As shown in Figure 5, use the USC-SIPI image dataset as an example to demonstrate the effectiveness of the suggested approach for various GS images.

TRLH has lowest PSNR comparison of 46.3514 dB, 46.3583 dB, 46.2894 dB, 46.2588 dB, 46.3251 dB and 46.3347 dB for Baboon, Barbara, Lena, Pepper, Lake and F16 images (Table 2(a)). TRSSKH has lowest PSNR comparison of 49.5412 dB, 49.4454 dB, 49.4175 dB, 49.3312 dB, 49.3023 dB and 49.3255 dB for Baboon, Barbara, Lena, Pepper, Lake and F16 images (Table 2(a)). The proposed schema has highest PSNR comparison of 49.6536 dB, 49.4565 dB, 49.4565 dB, 49.3624 dB, 49.3338 dB and 49.3541 dB for Baboon, Barbara, Lena, Pepper, Lake and F16 images (Table 2(b)).

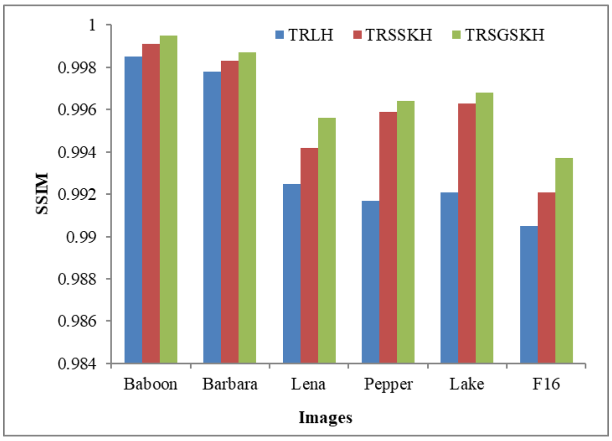


FIGURE 6. SSIM COMPARISON VS. WATERMARKING SCHEMES (COLOR IMAGES)

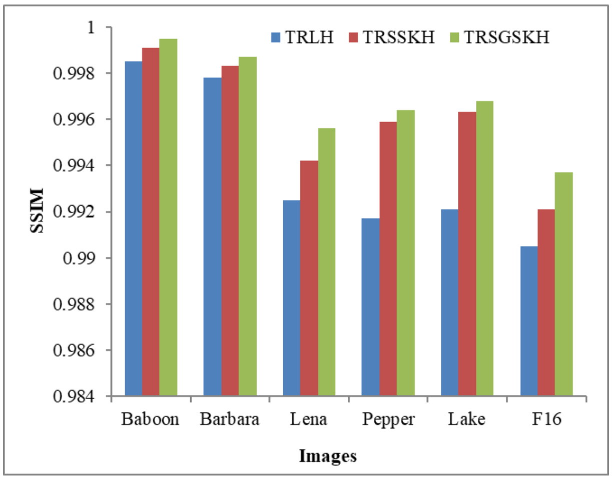


FIGURE 7. SSIM COMPARISON VS. WATERMARKING SCHEMES (GRAY-SCALE IMAGES)

Using images from the USC-SIPI dataset, the suggested approach was compared to the current SSIM-based techniques.For color and GSI (Table 2(a)&(b)), figures 6 and 7 provide the SSIM values of the Water mark images for these methods. The host images are color and GSI, from which the corresponding findings are computed. Better outcomes are indicated in bold, and it is clear from these that the suggested scheme outperforms TRLH [18] and TRSSKH [25] in terms of Water mark IQ. The best outcomes clearly demonstrate that, in comparison to TRLH [18] and TRSSKH [25], the suggested approach can obtain superior quality of the Water mark images.

TRLH has lowest SSIM comparison of 0.9985, 0.9978, 0.9925, 0.9917, 0.9921 and 0.9905 for images from the USC-SIPI dataset (Table 2(a)). Theimages from the USC-SIPI dataset, TRSSKH has the lowest SSIM comparison of 0.9991, 0.9983, 0.9942, 0.9959, 0.9963, and 0.9921 (Table 2(a)). According to Table 2(b), the suggested schema has the highest SSIM comparison for the images of Baboon, Barbara, Lena, Pepper, Lake, and F16 at 0.9995, 0.9987, 0.9956, 0.9964, 0.9968, and 0.9937. Figure 7 (Table 2(a)&(b)) shows the SSIM comparison of the suggested technique with the current methods utilizing images from the USC-SIPI dataset for GSI.

TRSSKH has lowest SSIM comparison of 0.9951, 0.9942, 0.9950, 0.9908, 0.9910 and 0.9872 for images from the USC-SIPI dataset(Table 2(a)). TRLH has lowest SSIM comparison of 0.9974, 0.9965, 0.9956, 0.9959, 0.9967 and 0.9948 for images of USC-SIPI dataset (Table 2(a)). The proposed schema has highest SSIM comparison of 0.9979, 0.9972, 0.9961, 0.9963, 0.9972 and 0.9954 for images from the USC-SIPI dataset (Table 2(b)).

CONCLUSION AND FUTURE WORK

Utilizing SPIHT, GIM-LOA, and Stucki Kernel halftone, this work proposes a fragile Water mark and blind dual Water mark technique to identify the TR and restore it to its original state. First, create and embed theWater mark; second, identify and retrieve the tampered regions are the two primary phases of the suggested methodology. DI commonly employ SPIHT as an embedded compression method.

Wavelet transform coefficients are generated and it has been used to reconstruct the image with good progressive transmission. Then, ACM and GIM-LOA are introduced to shuffle the result. The original image's left or right side contains ACM-tampered regions; GIM-LOA can preserve the recovery bits. Based on the Wavelet Transform coefficients, lyrebirds make up the population in the population-based metaheuristic method known as the GIM-LOA technique. GIM-LOA member, the tampered detection rate can be used to evaluate the OF of the tampered region. The two phases of the population update process are (i) hiding and (ii) escape, based on the lyrebird's decision in this case. Improved security and unpredictability are features of Water mark bits ACM and GIM-LOA. The suggested technique may obtain good performance 465 in TD and tampered regions recovery, with BOW2 and USC-SIPI numerous tests were conducted on that two available datasets,provided outcomes. It is evident that both color and GSI generate superior outcomes when using the suggested strategy. It is possible that the authentication bits are the reason why the detected region is bigger than the ground truth when the host image is slightly smooth. Work on improving the generation of authentication bits will continue in the future.

REFERENCES

[1] Wan, W., Zhou, K., Zhang, K., Zhan, Y., Li, J., 2020. JND-guided perceptually color image watermarking in spatial domain. IEEE Access 8, 164504–164520.

[2] Yu, X., Wang, C. and Zhou, X., 2018. A survey on robust video watermarking algorithms for copyright protection. Applied Sciences, 8(10), pp.1-26.

[3] Hwang, M.J., Lee, J., Lee, M., Kang, H.G., 2017. SVD-based adaptive QIM watermarking on stereo audio signals. IEEE Transactions on Multimedia 20, 45–54.

[4] Wan, W., Wang, J., Zhang, Y., Li, J., Yu, H. and Sun, J., 2022. A comprehensive survey on robust image watermarking. Neurocomputing, 488, pp.226-247.

[5] Asikuzzaman, M.; Pickering, M.R. An overview of digital video watermarking. IEEE Trans. Circuits Syst. Video Technol. 2017, 1–23.

[6] Asikuzzaman, M.; Alam, M.J.; Lambert, A.J.; Pickering, M.R. Robust DT CWT-based DIBR 3D video watermarking using chrominance embedding. IEEE Trans. Multimed. 2016, 18, 1733–1748.

[7] Huynh-The, T.; Hua, C.H.; Tu, N.A.; Hur, T.; Bang, J.; Kim, D.; Bilal Amin, M.; Kang, B.H.; Seung, H.; Lee, S. Selective bit embedding scheme for robust blind color image watermarking. Inf. Sci. 2018, 426, 1–18.

[8] Sreenivas, K.; Prasad, V.K. Fragile watermarking schemes for image authentication: A survey. Int. J. Mach. Learn. Cybern. 2017, 1–26.

[9] Shih F. Y., Digital Watermarking and Steganography: Fundamentals and Techniques Second Edition, Boca Raton, FL, USA: CRC Press, 2017.

[10] Shih F. Y. and X. Zhong, “Intelligent watermarking for high-capacity low-distortion data embedding,” Int. J. Pattern Recognit. AI, vol. 30, no. 5, p. 1654003 (17 pages), 2016.

[11] Qin C., P. Ji, X. Zhang, J. Dong, and J. Wang, ``Fragile image watermarking with pixel-wise recovery based on overlapping embedding strategy,'' Signal Process., vol. 138, pp. 280-293, Sep. 2017.

[12] Ansari I. A., M. Pant, and C. W. Ahn, ``SVD based fragile watermarking scheme for tamper localization and self-recovery,'' Int. J. Mach. Learn. Cybern., vol. 7, no. 6, pp. 1225-1239, Dec. 2016.

[13] Singh, Y.K. and Vanlalhruaia, 2020. Performance Evaluation of Different Halftone Kernels for Binary Face Recognition. In Intelligent Techniques and Applications in Science and Technology: Proceedings of the First International Conference on Innovations in Modern Science and Technology 1 (pp. 278-286). Springer International Publishing..

[14] Tora, H., Gokcay, E., Turan, M. and Buker, M., 2022. A generalized Arnold’s Cat Map transformation for image scrambling. Multimedia Tools and Applications, 81(22), pp.31349-31362.

[15] Turan, M., Gökçay, E. and Tora, H., 2024. An unrestricted Arnold’s cat maptransformation.Multimedia Tools and Applications, pp.1-15.

[16] Khudzaifah, M. and Hakim, M.L., 2024, Implementation of Hill Cipher Algorithm and Arnold Cat Map (ACM) algorithm on Iris digital image security. In AIP Conference Proceedings (Vol. 3083, No. 1). AIP Publishing.

[17] Dehghani, M., Bektemyssova, G., Montazeri, Z., Shaikemelev, G., Malik, O.P. and Dhiman, G., 2023. Lyrebird optimization algorithm: a new bio-inspired metaheuristic algorithm for solving optimization problems. Biomimetics, 8(6), pp.1-62.

[18] Haghighi, B.B., Taherinia, A.H. and Harati, A., 2018. TRLH: Fragile and blind dual watermarking for image tamper detection and self-recovery based on lifting wavelet transform and halftoning technique. Journal of Visual Communication and Image Representation, 50, pp.49-64.

[19] Haghighi, B.B., Taherinia, A.H. and Mohajerzadeh, A.H., 2019. TRLG: Fragile blind quad watermarking for image tamper detection and recovery by providing compact digests with optimized quality using LWT and GA. Information Sciences, 486, pp.204-230.

[20] Chang, C.C., Lin, C.C. and Su, G.D., 2020. An effective image self-recovery based fragile watermarking using self-adaptive weight-based compressed AMBTC. Multimedia Tools and Applications, 79(33), pp.24795-24824.

[21] Gul, E. and Ozturk, S., 2020. A novel triple recovery information embedding approach for self-embedded digital image watermarking. Multimedia Tools and applications, 79, pp.31239-31264.

[22] Liu T. and X. Yuan, ``A dual-tamper-detection method for digital image authentication and content self-recovery,'' Multimedia Tools Appl., vol. 80, no. 19, pp. 29805-29826, Aug. 2021.

[23] Faheem, Z.B., Ali, M., Raza, M.A., Arslan, F., Ali, J., Masud, M. and Shorfuzzaman, M., 2022. Image watermarking scheme using LSB and image gradient. Applied Sciences, 12(9), pp.1-12.

[24] Wang, M.X., Yang, H.M., Jiang, D.H., Yan, B., Pan, J.S. and Wang, T., 2022. A novel quantum image watermarking scheme for tamper localization and self-recovery. Quantum Information Processing, 21(8), p.277.

[25] Zhang, Q., Yuan, X. and Liu, T., 2022. Blind dual watermarking scheme using stucki kernel and SPIHT for image self-recovery. IEEE Access, 10, pp.96100-96111.

[26] Fan, M., 2023. Blind dual image watermarking for copyright protection, tamper proofing and self-recovery. Multimedia Tools and Applications, 82(29), pp.45503-45518.

[27] Singh, D., Singh, S.K. and Udmale, S.S., 2023. An efficient self-embedding fragile watermarking scheme for image authentication with two chances for recovery capability. Multimedia Tools and Applications, 82(1), pp.1045-1066.

[28] Li, X., Chen, Q., Chu, R. and Wang, W., 2024. Block mapping and dual-matrix-based watermarking for image authentication with self-recovery capability. Plos one, 19(2), pp.1-12.

[29] Dehghani, M., Bektemyssova, G., Montazeri, Z., Shaikemelev, G., Malik, O.P. and Dhiman, G., 2023. Lyrebird optimization algorithm: a new bio-inspired metaheuristic algorithm for solving optimization problems. Biomimetics, 8(6), pp.1-62.

[30] Sahay, A. and Pradhan, C., 2017, Multidimensional comparative analysis of image encryption using gauss iterated and logistic maps. In 2017 International Conference on Communication and Signal Processing (ICCSP), pp. 1347-1351.