International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Optimizing Data Embedding Through Coati-inspired Discrete Fourier Transform Techniques

Neetha S. S.[1], Dr. Bhuvana J.*[2]

Submitted: 09/12/2023 **Revised**: 18/01/2024 **Accepted**: 02/02/2024

Abstract*:* Information may be stored and retrieved efficiently because to cloud data embedding. Cloud platforms offer adaptable and scalable storage options, making it simple for customers to store and retrieve massive amounts of data as needed. Because of its scalability, businesses may adjust to their evolving data needs without being constrained by physical storage limits. It is mutual practice to manually alter the key limits used by data embedding approaches in an experimental form according to the application scenario and the picture. However, this can be a hassle and not work well in real-world situations. One optimisation technique that has recently been employed to increase performance is robust watermarking, which allows the critical operation parameter to be autonomously adjusted. Improved resilient watermarking approach in discrete Fourier transform via feast spectrum is projected in this research using the Coati optimisation algorithm (COA) in combination with visual info integrity and bit correct rate requirements. In particular, it optimises the watermark strength factor, number of bands, and frequency coefficients.

Keywords: *Bit Error Rate, Cloud Data Embedding, Coati Optimization Algorithm (COA), Discrete Fourier Transform, Resilient Watermarking, Scalable Storage, Visual Information Integrity, Water marking*

1. Introduction

The practise of smoothly integrating and storing data within cloud computing systems is known as "data embedding in the cloud" [1]. By improving accessibility, scalability, and security, solutions are provided by cloud, allowing businesses to take use of cutting-edge processing and storage capabilities [2]. Sensitive data can be protected and privacy laws followed with the use of encryption and data management solutions [3]. Data embedding plays a crucial role in streamlining resource utilisation and promoting teamwork as businesses move more and more to cloud-based infrastructures, which in turn creates a more responsive and flexible digital ecosystem [4].

To improve the security and secrecy of transmitted data, data embedding in encrypted carrier blocks is required [5]. Although data is adequately protected from unauthorised access by encryption, an additional layer of functionality is introduced when additional information is embedded within these encrypted carrier blocks [6]. With data embedding, supplemental information, watermarks, and metadata can be subtly added without jeopardising the underlying encryption [7, 8]. This combination of methods allows tracking, authentication, and secure communication inside a secured environment [9, 10].

When it comes to situations where it is necessary to send sensitive information in a covert manner, data embedding in encrypted carrier blocks becomes essential [11]. This approach strengthens the primary data's confidentiality while enabling auxiliary functions that are essential for content authentication, digital rights management, and traceability [12]. The combination of encryption and data embedding is proving to be a valuable tool in the development of comprehensive solutions that address the ever-changing security landscape, protect digital assets, and maintain the integrity of communication channels [13].

1 School of CS & IT, JAIN(Deemed-To-Be) University, Bangalore – 560069, INDIA
ORCID ID : 0000-0003-3751-9597
2 School of CS & IT, JAIN(Deemed-To-Be) University, Bangalore – 560069, INDIA
ORCID ID : 0000-0002-8372-6311
** Corresponding Author Email: ssneetha.kala@gmail..com*

The main contributions of the paper are:

Effective Data Embedding in Cloud: By utilizing the scalability and flexibility of cloud platforms, this work addresses the effective storage and retrieval of information. This overcomes the limitations of physical storage and enables users to store large volumes of data and retrieve it as needed.

Automated Parameter Optimization: This work presents methods for optimizing a robust watermarking algorithm based on discrete spectrum. Specifically, the Coati optimization algorithm is used to automatically modify key operation parameters. This optimization is focused on factors such as the watermark strength factor, band counts, and frequency coefficients.

Performance Improvement: The optimization criteria are based on bit correct rate and visual information fidelity, which guarantees better watermark retrieval and embedding while preserving original data fidelity.

The remaining sections of the study are prearranged like shadows: Part 2 summarises relevant literature, Part 3 gives a brief description of the suggested model, Part 4 shows the analysis and validation results, and Section 5 concludes with a summary.

2. Review Literature

A watermarking technique based on vertical stability was projected

by Zhang, M., et al. [14]. First, the binary the traceability material code were used to generate watermark info. Second, the watermark index was computed using the data's vertical distribution properties and the length of the watermark information following compression. By altering the relative storage order of the relevant data in accordance with the value, the watermark embedding process was finally finished. The method exhibited good invisibility without compromising the accuracy of the data, according to experimental results. Furthermore, the method showed improved robustness under operations including geographic point cloud data compared to existing algorithms.

E-SAWM, a dynamic intended for edge cloud scenarios, was proposed by Zu, L., et al. [15]. This architecture enabled accurate leakage during the data-sharing procedure by incorporating analysis, E-SAWM produced remarkably plausible pseudo statements that took advantage of the document structure found in OFD files. The purpose of strategically distributing these pseudo statements was to incorporate unnecessary information into the structural documents so that the watermark would not be completely destroyed or removed. The watermarked text occupied less than 15% of the original file size, demonstrating a strong capacity for holding the watermark, according to experimental data showing that the algorithm had no effect on the file size. Furthermore, the suggested watermarking strategy was more appropriate for the technological needs of complicated deployment than the explicit watermarking schemes that are already in use for OFD files based on annotation structure. It successfully addressed issues related to simple deletion and manipulation, offering strong concealment and resilience.

Ye, C., et al.'s main goal [16] was to create a map that connected the social network to the tree structure Haar (TSH) transform. Initially, a social image was subjected to the TSH transform. Second, SNA was used to code every user on a social networking platform. Third, to safeguard the spread of social media images, watermarking and encryption were carried out in a compressed domain. Ultimately, a hybrid multicast–unicast system was used to distribute the watermarked and encrypted data to users. Watermarking and encryption together could offer twofold security for the sharing of social media images. The efficiency of the suggested plan was shown by the results of the experiment and the examination of theory.

Pallaw, V. K., et al. [17] presented a hybrid watermarking strategy that makes use of the Firefly algorithm, randomized-singular value decomposition, and Slantlet transform, among other optimisation techniques inspired by nature. The XOR encryption method was used to encode the watermark image. Based on SSIM, and PSNR, extensive testing showed that the novel strategy performed better techniques. With a scale factor of 0.06, the SSIM and NC values of extracted watermark were nearly or equal to 1, and the PSNR of the suggested scheme ranged from 58 to 59 dB, demonstrating the scheme's superior performance.

A novel method for digital photo makes use of the DCT, DWT, DTO, and SFS algorithms was presented by El-Kenawy, E. S. M., et al. [18]. DWT and DCT were applied to the cover image, DTOSFS was used to optimize the watermarking parameters, and the method produced better results than industry norms. Evaluation parameters like as IF, PSNR, and NCC validated the efficacy of the technique. Its proven robustness against attacks confirms its usefulness. The suggested solution proved to be appropriate for digital picture watermarking applications as it performed noticeably better than previous approaches.

A strong, high-capacity semi-blind picture watermarking method was presented by Yang, Z., et al. [19]. Initially, the carrier image underwent a discrete wavelet transformation (DWT) transformation. In order to save storage space, the watermark pictures were then compressed using a compressive sampling technique. Thirdly, the compressed watermark picture was well secured and the false positive problem (FPP) was significantly reduced by using a Combination of One Logistic map (TL-COTDCM). Ultimately, the embedding process was completed by embedding a singular value decomposition (SVD) component into the decomposed carrier picture. Through the use of this scheme, eight 256x256x256 grayscale watermark images were seamlessly integrated into a 512x512x512 carrier image, whose capacity exceeded that of the watermark techniques in use by an average of eight times. The experiment findings demonstrated the standards. The scheme was evaluated through numerous common attacks on high strength.

2.1. Research Gaps

The need for sophisticated methods to solve security and privacy issues related to cloud-based data embedding is one of the research gaps in cloud data embedding. Current approaches might not be able to manage large-scale datasets well and are frequently not resilient enough against changing cyberthreats. Furthermore, nothing is known about how data embedding affects cloud systems' overall performance and scalability. To ensure data security and system efficiency, more research is needed to create scalable and effective algorithms that can be smoothly integrated with a variety of cloud architectures. Another critical research gap is investigating new strategies to improve embedded data's resistance against sophisticated attacks.

3. Proposed Methodology

Figure 1 shows the projected work flow of the data embedding model.

Fig 1: Work Flow of Data Embedding model

3.1. Background and Contributions

The two-dimensional density-functional theory (DFT) domain has been one of the most investigated frequency spaces within the invisible data embedding area since the dawn of the data embedding age. What follows is an image's 2D DFT transformation. I(x,y) of size N_1×N_2 is given by (1):

$$F(u,v) = \sum_{x=1}^{N_1} \sum_{y=1}^{N_2} I(x,y) e^{-j2\pi(ux/N_1 + vy/N_2)} \quad (1)$$

As demonstrated in (2), one of the well-known features of the DFT is that it does not impact the size of the 2D DFT transform in the spatial domain:

$$\left| DFT\left[I\left(x + x_1, y + y_1 \right) \right] \right| = M(u,v), \quad (2)$$

where M(u,v)=|F(u,v)| and x_1,y_1 are translation parameters. It leads to inverse in the frequency domain with respect to the scrambling in the spatial domain, as demonstrated in (3):

$$\text{DFT}\,[\text{I}(\rho x, \rho y)] = 1/\rho\ \text{F}(\text{u}/\rho, \text{v}/\rho), \quad (3)$$

where ρ is factor. Revolution in the spatial sphere reasons the similar gyration θ in the frequency domain, as revealed in (4):

$$\text{DFT}\,[I(x\cos\,\theta - y\sin\,\theta, x\sin\,\theta + y\cos\,\theta)] = F(u\cos\,\theta - v\sin\,\theta, u\sin\,\theta + v\cos\,\theta). \quad (4)$$

When it comes to typical signal processing, such JPEG noise contamination, among others, watermark embedding in the DFT domain provides invariance [20]. Recent years have seen the proposal of many DFT-based watermarking algorithms in the scientific literature, with encouraging outcomes regarding imperceptibility and resilience. In the case of invisible watermarking, the algorithm typically chooses two radiuses. This area should encapsulate the middle frequency components in the DFT domain, centred around M(0,0). The changes made to the lower frequencies of M(u,v) will lead to noticeable distortion in the image's spatial domain, which is why this is the case. Conversely, JPEG compression could mask watermarks that are contained in the complex M(u,v) frequencies. Because of its resistance to typical signal JPEG compression, and its imperceptibility to the human eye, the watermark is best inserted of M(u,v).

Originally proposed by Solachidis and Pitas in, the traditional embedding region has been refined over the years to incorporate human visual scheme criteria, hybrid domains, feature points, and a wide range of applications. 2D invisible watermarking has a problem that will be discussed in the following paragraphs, despite the fact that the traditional specification of the embedding region offers certain stated benefits in terms of imperceptibility and resilience.

It is standard practice to adapt the critical parameters based on the scenario and the picture database. the experimentally employed watermark strength factor a, the pair r2 in the magnitude M(u,v) that construct A, and the density-functional theory (DFT)-based invisible watermarking solutions. But this kind of manual modification can be a pain in real-world situations and can also need a lot of work. It is well-known that the delivery of spectral information varies between pictures in a heterogeneous image collection, hence it may not be optimal to adjust the same amount of DFT coefficients in all of the photos. The DFT magnitude of the brightness of two colour pictures, one with mostly plain other with mostly texturized content, are shown for demonstration purposes.

Thus, when working with a heterogeneous image database and using fixed standards for the pair of radiuses r1 and r2 in the magnitude M(u,v), it will be necessary to experimentally adjust the watermark strength factor a to ensure watermark imperceptibility while avoiding effects on robustness. Finding the optimal values of the critical parameters is the goal of this proposal, as stated above. To improve the imperceptibility using colour images, it is recommended to use the values that are appropriate for each image when building the annular area.

Using optimisation techniques like the COA algorithm, researchers have been concentrating on improving invisible watermarking technologies' performance and critical parameters in recent years. Here, we take a quick look back at what's currently known about invisible watermarking techniques that optimise using the COA algorithm.

3.2. Embedding Process

There is a linear relationship between the two colour models, and the most correlated components are in model, whilst the least connected components are in the yCbCr model, considering a color image:

1. Perform RGB-YCbCr insulates the luminance component $Y(x,y)$ from $YCbCr$ transformation;
2. Supported by a secret key k_1, produce which binary $\{1,0\}$ arbitrary outline with mean, $W = \{w_b \mid b = 1, \ldots, L\}$, watermark;
3. Apply the 2D DFT transform $F(u,v)$ defined by (1) to the inventive luminance component $Y(x,y)$and obtain the magnitude $M(u,v)$ and phase $P(u,v)$ info;
4. Select a pair of radiuses $r_1$and $r_2$in $M(u,v)$ aand the annular area $A = \pi({r_2}^2 - {r_1}^2)$ between r_1 and r_2 should frequency in $M(u,v)$ around coefficient $M(0,0)$;
5. To surety the security of W, scramble its data key k_2;
6. Encode W using the DS-CDMA: secret key k_3, allocate to each data bit w_b a binary $\{-1,1\}$structureg_b with size $A/2$. Each g_b order is reliant on on w_b in the subsequent way:

$$\begin{matrix} if\ w_b = 0 \rightarrow +g_b \\ if\ w_b = 1 \rightarrow -g_b \end{matrix} \quad (5)$$

The encoded watermark W_(DS-CDMA) is obtained using (6):

$$W_{DS-CDMA} = \sum_{b=1}^{L} \pm g_b; \quad (6)$$

1. Embed W_(DS-CDMA) in the constants of half of M(u,v) in middle manner:

$$M'(u,v) = M(u,v) + \alpha W_{DS-CDMA}, \quad (7)$$

where α is strength factor and M, M'', are the DFT magnitude, correspondingly. Rendering to DFT symmetrical band of $M(u,v)$ proportionally.

2. Return the component $Y'(x,y)$to inverse DFT (IDFT) retaining $M'(u,v)$ and the consistent initial phase $P(u,v)$ as exposed in (8):

$$Y'(x,y) = \text{IDFT}\,(F'(u,v)),\ \text{where}:$$
$$F'(u,v) = M'(u,v) \cdot \cos\,(P(u,v)) + M'(u,v) \cdot (j \cdot \sin\,(P(u,v))); \quad (8)$$

3. Finally, luminance $Y'(x,y)$ and the info, perform YCbCr to RGB the watermarked image I_{w}.

3.3. Coati optimization procedure: The proposed Coati Optimisation Procedure (COA) and its precise phases are detailed in this section.

3.3.1. Inspiration and actions of coatis

Coatis, often spelt coatimundis, are fish that genera Nasuella. South and Central America, Mexico, and the southern United States are home to these creatures, which are active throughout the day. Each coati has its own unique characteristics, although they

all have a small head, a long non-prehensile tail that they use for balance and signalling, and black paws. Their noses are flexible and slightly curved upwards. The be as long as its body, or anything to tail tip [21]. Coatis are about the size of a large house cat, with a shoulder height of around 30 cm and a weight of 2 to 8 kg. With their enormous, pointed canines, males can reach a size nearly double that of females. Both coatis and white-nosed are native to South America, and these dimensions apply to them. Of the two varieties, mountain coatis are smaller. As omnivores, coatis consume both invertebrates and small vertebrates, including tarantulas, lizards, rodents, birds' eggs, crocodile eggs, and rodents. A green iguana is a favourite meal of coatis. Coatis typically hunt iguanas in packs because of how common they are in treetop locations. In order to get the iguana to leap to the ground, some coatis climb trees, while others swiftly assault it. Regardless, predators pose a threat to coatis. The coati is preyed upon by several animals, including jaguarundis, hunt them.

Intelligence is at work in the coati's approach against iguanas and in its behaviour while facing and evading predators. A key motivation for developing the suggested COA method was to model its operation after that of real coatis.

3.3.2. Algorithm initialization process

The coatis are viewed as part of the algorithm's population in the COA technique, which is a population-based metaheuristic. Decision variable values are based on where located in the search space. The COA sees coatis' viewpoint as a possible answer to the situation. The initialization of the coatis point in the search space is done arbitrarily using Eq. (9), at the beginning of the COA implementation.

$$X_i: x_{i,j} = lb_j + r \cdot \left(ub_j - lb_j\right),\ i = 1,2,\dots,N,\ j = 1,2,\dots,m, \quad (9)$$

In this context, X_i represents the i-th space, x_(i,j) stands for the j-th variable's value, N denotes the sum of coatis, m denotes the, r is a randomly chosen real sum between 0 and 1, and lb_j and ub_j denote the j-th decision bounds, correspondingly.

The following matrix X, which is known as the population matrix, mathematically represents the coati population in the COA.

$$X = \begin{bmatrix} X_1 \\ \vdots \\ X_i \\ \vdots \\ X_N \end{bmatrix}_{N\times m} = \begin{bmatrix} x_{1,1} & \cdots & x_{1,j} & \cdots & x_{1,m} \\ \vdots & \ddots & \vdots & . & \vdots \\ x_{i,1} & \cdots & x_{i,j} & \cdots & x_{i,m} \\ \vdots & . & \vdots & \ddots & \vdots \\ x_{N,1} & \cdots & x_{N,j} & \cdots & x_{N,m} \end{bmatrix}_{N\times m} \quad (10)$$

Various values for the function are assessed as possible solutions are placed in decision variables. Equation (11) is used to exemplify these standards.

$$F = \begin{bmatrix} F_1 \\ \vdots \\ F_i \\ \vdots \\ F_N \end{bmatrix}_{N\times 1} = \begin{bmatrix} F(X_1) \\ \vdots \\ F(X_i) \\ \vdots \\ F(X_N) \end{bmatrix}_{N\times 1} \quad (11)$$

The process of modifying the coatis (potential solution) site in the COA relies on simulating two coatis behaviors in nature. Examples of these actions are.

A candidate solution's quality is measured by the value of function in metaheuristic algorithms like the suggested COA. Consequently, the best member of the populace is the one that results in the evaluation of the function's finest value. The method iteratively updates the candidate solutions, which means that member of the populace is also updated with each repetition.

3.3.3. Mathematical perfect of COA

The process of modifying the coatis (potential solution) site in the COA relies on simulating two coatis behaviors in nature. Examples of these actions are:

(i) coatis' policy when aggressive iguanas,

(ii) coatis' escape policy from marauders.

Accordingly, the COA populace is efficient in two diverse phases.

Phase 1: Hunting and attacking approach on iguana (exploration stage)

Modelling the coatis' assault tactic on iguanas is the initial step in updating their population in the search space. Here, a herd of coatis scales a tree in an effort to frighten an iguana into submission. A group of coatis patiently await the iguana's demise beneath a nearby tree. The coatis hunt and attack the iguana as soon as it hits the ground. The COA's capacity to explore the problem-solving space through global search is demonstrated by the strategy's ability to relocate coatis to different spots in space. The iguana is supposed to represent the best member of COA design. Additionally, it is believed that coatis ascend the tree while waits for the iguana to plummet to the ground. So, we use Eq. (12) to imitate the coatis' location as they ascend the tree.

$$X_i^{P1}: x_{i,j}^{P1} = x_{i,j} + r \cdot (Iguana_{\ j} - I \cdot x_{i,j}) \text{for } i = 1,2,\dots,\left\lfloor \frac{N}{2} \right\rfloor \text{ and } j = 1,2,\dots,m. \quad (12)$$

The iguana is dropped to an undetermined spot in the search area when it hits the floor. The ground-dwelling coatis use this arbitrary location to navigate the search space, a virtual environment created by Eqs. (13) and (14).

$$\text{Iguana}^{G}: \text{Iguana}_j^G = lb_j + r \cdot \left(ub_j - lb_j\right), j = 1,2,\dots,m, \quad (13)$$

$$X_i^{P1}: x_{i,j}^{P1} = \begin{cases} x_{i,j} + r \cdot \left(\text{ Iguana }_j^G - I \cdot x_{i,j}\right), & F_{\text{Iguana}} < F_i, \\ x_{i,j} + r \cdot \left(x_{i,j} - \text{ Iguana }_j^G\right), & \text{else,} \end{cases} \quad (14)$$

$$\text{for } i = \left\lfloor \frac{N}{2} \right\rfloor + 1, \left\lfloor \frac{N}{2} \right\rfloor + 2, \dots, N \text{ and } j = 1,2,\dots,m.$$

If each coati's updated position increases the goal function's value, then the update procedure can proceed with the calculation; else, the coati will stay in its former location. Equation (15) is used to simulate this update situation for i=1,2,…,N.

$$X_i = \begin{cases} X_i^{P1}, F_i^{P1} < F_i, \\ X_i, \text{ else.} \end{cases} \quad (15)$$

Here X_i^{P1} is the new position intended for the i th coati, $x_{i,j}^{P1}$ is its j th dimension, F_i^{P1} is its objective function value, r is a accidental real sum in the intermission [0, 1], Iguana represents the member, Iguana j_j is its j th dimension, I is an integer, which is randomly ^{G} is the position of the iguana on generated, Iguana_j^G is its j th dimension, F_{Iguana} " is function, and $\lfloor \cdot \rfloor$ is function.

Phase 2: The process of escaping from marauders (manipulation stage)

Mathematical models based on coati behaviour when from

predators are used in the second step of informing coatis' sites in the search space. Coatis will often jump off their perch when threatened by a predator. Coati's strategic manoeuvres put it in a secure site near its present location, showcasing the COA's abilities.

In order to mimic this action, we use Eqs. (16) and (17) to establish a random position close to where each coati is positioned.

$$lb_j^{\text{local}} = \frac{lb_j}{t}, ub_j^{\text{local}} = \frac{ub_j}{t}, \text{where } t = 1,2,\dots,T. \quad (16)$$

$$X_i^{P2}: x_{i,j}^{P2} = x_{i,j} + (1-2r)\cdot\left(lb_j^{\text{local}} + r\cdot\left(ub_j^{\text{local}} - lb_j^{\text{local}}\right)\right), \quad (17)$$

$$i = 1,2,\dots,N, j = 1,2,\dots,m$$

This condition mimics the goal function using Eq. (18), thus if the newly computed position increases its value, it is acceptable.

$$X_i = \begin{cases} X_i^{P2}, F_i^{P2} < F_i, \\ X_i, \text{else} \end{cases} \quad (18)$$

Here X_i^{P2} is the novel position envisioned for the i th additional stage of COA , $x_{i,j}^{P2}$ is its j th dimension, , F_i^{P2} is its value, r is a chance figure in the intermission [0,1],t is the reiteration counter, lb_j^{local} and ub_j^{local} are the local bound of variable correspondingly, lb_j and ub_j are bound of the j th decision mutable, correspondingly.

3.3.4. Repetition procedure of COA

Each iteration of a COA ends after all coatis' positions in the hunt area have been updated using the data from the prior two stages. The procedure iteratively updates the population using Eqs. (12) to (18) till the last iteration. As soon as COA finishes running, the output is the optimal solution that was acquired during all algorithm iterations.

4. Results and Discussions

4.1. Experimental Setup

An NVIDIA RTX 3090 GPU with 24 GB of on-chip memory and 64 GB of on-board memory was used for the research. The graphics processing unit (GPU) is capable of single-precision floating-point calculations up to 36 TFLOPS.

4.2. Performance Analysis

Table 1. Performance analysis of existing models with proposed model

Geometric attacks	Intensity	Projected Algorithm NC1	Jing L [22] NC2	Fengming Q [23] NC3	Yangxiu F [24] NC4	Ceng X [25] NC5
Rotation (clockwise)	10	1.01	0.91	0.64	1.01	0.82
	20	0.78	0.91	0.64	1.01	0.90
	40	0.78	0.87	0.33	1.01	0.75
Scaling	0.4	1.01	0.94	1.01	1.01	0.26
	0.8	1.01	0.94	1.01	1.01	0.69
	2.0	1.01	1.01	1.01	1.01	0.32
Down Transalation	8%	1.01	0.92	0.90	1.01	0.62
	15%	0.91	0.81	0.51	1.01	0.57
	20%	0.91	0.72	0.46	0.87	0.57
Left Transalation	3%	0.91	0.98	0.73	1.01	1.01
	5%	0.91	0.98	0.53	0.87	1.01
	8%	0.75	0.82	0.53	0.87	1.01
Cropping	12%	1.01	1.01	1.01	1.01	0.56
	23%	0.92	1.01	0.90	0.88	0.42
	35%	0.92	0.62	0.79	0.63	0.34

Table 1 and figures 2 through 6 display the performance evaluation of a number of current techniques (NC1 through NC5) as well as the suggested algorithm under various geometric attacks (clockwise rotation, scaling, down translation, left translation, and cropping). For each form of attack, four different intensities are tested: 0.4, 0.8, and 2.0 for scaling; 8%, 15%, and 20% for down translation; 3%, 5%, and 8% for left translation; and 12%, 23%, and 35% for cropping. These intensities correspond to different attack types. The suggested methodology consistently shows robustness across all attack scenarios and performs better than current approaches in the majority of cases in terms of normalised correlation values. For instance, the recommended algorithm yields a value of 1.01 when rotation is set to 10 degrees, which is greater than the equivalent values, which range from 0.64 to 0.91. It is clear from comparing the proposed algorithm to the other techniques investigated in this paper that in several different circumstances where it consistently maintains higher normalised correlation values, it is more resistant to geometric attacks.

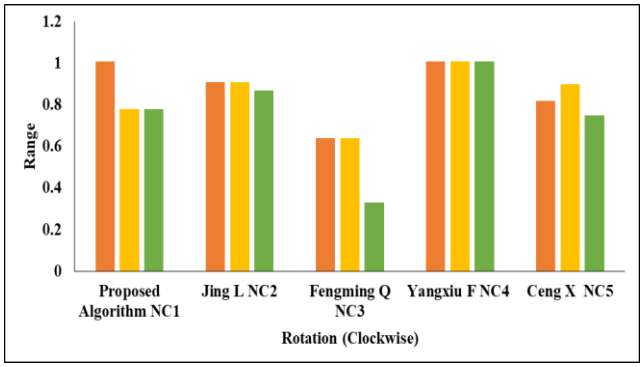

Fig 2. Comparative analysis of existing representations with projected model on rotation

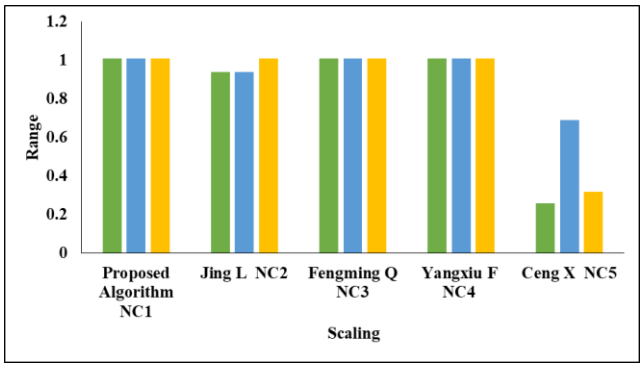

Fig 3. Comparative analysis of existing representations with projected model on Scaling

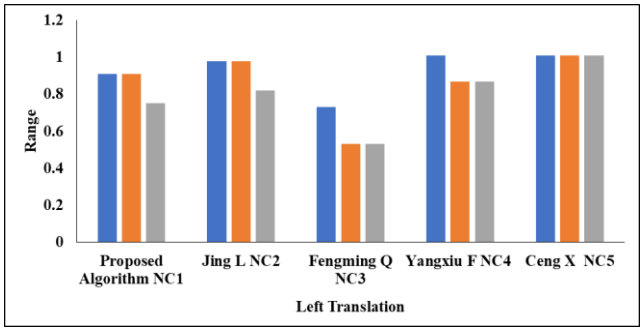

Fig 4. Comparative investigation of existing representations with projected model on Down Translation

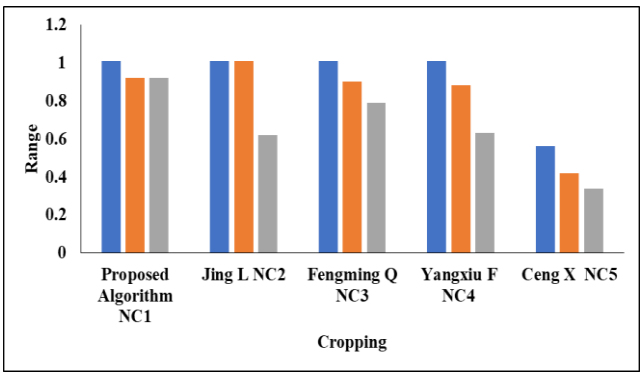

Fig 5. Comparative investigation of existing representations with projected model on Left Translation

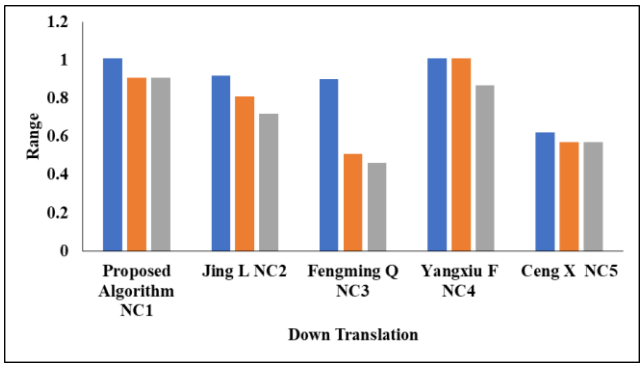

Fig 6. Comparative investigation of existing models with projected model on Cropping

5. Conclusion

Finally, this study presents a new method for improving robust data embedding using the spread spectrum methodology in the discrete Fourier transform domain. In real-world situations, the traditional method of manually modifying important settings for data embedding in the cloud might be time-consuming and unfeasible. Taking note of this difficulty, the suggested method makes use of the Coati optimisation algorithm to automate the modification of critical operation parameters. In particular, it streamlines the procedure and greatly enhances performance by optimising the number of bands, frequency coefficients, and watermark strength factor. The method ensures a balanced optimisation that takes into account both perceptual quality and data integrity by merging bit fidelity. This solves the drawbacks of manual parameter adjustment in addition to improving storage and retrieval efficiency in cloud systems. Robust watermarking has advanced with the introduction of optimisation approaches, which allow for flexibility in a range of application settings. This upgraded and automated watermarking method provides a reliable option for businesses looking for scalable, adaptable, and effective data embedding in cloud-based storage systems as the digital landscape changes. Future study endeavours may concentrate on broadening the algorithm's scope to encompass various forms of multimedia and examining its resilience within the framework of developing cloud-based applications.

6. References

[1]. Ghosh, A. M., & Grolinger, K. (2020). Edge-cloud computing for Internet of Things data analytics: Embedding intelligence in the edge with deep learning. IEEE Transactions on Industrial Informatics, 17(3), 2191-2200.

[2]. Thakkar, H. K., Dehury, C. K., & Sahoo, P. K. (2020). MUVINE: Multi-stage virtual network embedding in cloud data centers using reinforcement learning-based predictions. IEEE Journal on Selected Areas in Communications, 38(6), 1058-1074.

[3]. Zhang, W., Wang, D., Yu, S., He, H., & Wang, Y. (2021). Repeatable multi-dimensional virtual network embedding in cloud service platform. IEEE Transactions on Services Computing, 15(6), 3499-3512.

[4]. Dehury, C. K., & Sahoo, P. K. (2019). DYVINE: Fitness-based dynamic virtual network embedding in cloud computing. IEEE Journal on Selected Areas in Communications, 37(5), 1029-1045.

[5]. Huang, R., Xu, Y., Hong, D., Yao, W., Ghamisi, P., & Stilla, U. (2020). Deep point embedding for urban classification using ALS point clouds: A new perspective from local to global. ISPRS Journal of Photogrammetry and Remote Sensing, 163, 62-81.

[6]. Dai, W., Nishi, H., Vyatkin, V., Huang, V., Shi, Y., & Guan, X. (2019). Industrial edge computing: Enabling embedded intelligence. IEEE Industrial Electronics Magazine, 13(4), 48-56.

., He, H., & Wang, Y. (2021). Repeatable multi-dimensional virtual network embedding in cloud service platform. IEEE Transactions on Services Computing, 15(6), 3499-3512.

[7]. Anil, A., Shukla, V. K., & Mishra, V. P. (2020, June). Enhancing data security using digital watermarking. In 2020 International Conference on Intelligent Engineering and Management (ICIEM) (pp. 364-369). IEEE.

[8]. Fang, X., Lai, R., Zhou, Z., Chen, Z., Zheng, P., & Lu, W. (2022, July). Efficient and secure outsourced image watermarking in cloud computing. In International Conference on Artificial Intelligence and Security (pp. 526-537). Cham: Springer International Publishing.

[9]. Vasanthanayaki, C. (2020). Secure medical health care content protection system (SMCPS) with watermark detection for multi cloud computing environment. Multimedia Tools and Applications, 79, 4075-4097.

[10]. Qin, C., Qian, Z., Feng, G., & Zhang, X. (2019). Special issue on real-time image watermarking and forensics in cloud computing. Journal of Real-Time Image Processing, 16, 559-563.

[11]. Ray, A., & Roy, S. (2020). Recent trends in image watermarking techniques for copyright protection: a survey. International Journal of Multimedia Information Retrieval, 9(4), 249-270.

[12]. Kamili, A., Hurrah, N. N., Parah, S. A., Bhat, G. M., & Muhammad, K. (2020). DWFCAT: Dual watermarking framework for industrial image authentication and tamper localization. IEEE Transactions on Industrial Informatics, 17(7), 5108-5117.

[13]. Dong, X., Zhang, W., Shah, M., Wang, B., & Yu, N. (2020). Watermarking-based secure plaintext image protocols for storage, show, deletion and retrieval in the cloud. IEEE Transactions on Services Computing, 15(3), 1678-1692.

[14]. Zhang, M., Dong, J., Ren, N., & Guo, S. (2023). Lossless Watermarking Algorithm for Geographic Point Cloud Data Based on Vertical Stability. ISPRS International Journal of Geo-Information, 12(7), 294.

[15]. Zu, L., Li, H., Zhang, L., Lu, Z., Ye, J., Zhao, X., & Hu, S. (2023). E-SAWM: A Semantic Analysis-Based ODF Watermarking Algorithm for Edge Cloud Scenarios. Future Internet, 15(9), 283.

[16]. Ye, C., Tan, S., Wang, Z., Shi, B., & Shi, L. (2023). Hybridized Hierarchical Watermarking and Selective Encryption for Social Image Security. Entropy, 25(7), 1031.

[17]. Pallaw, V. K., Singh, K. U., Kumar, A., Singh, T., Swarup, C., & Goswami, A. (2023). A Robust Medical Image Watermarking Scheme Based on Nature-Inspired Optimization for Telemedicine Applications. Electronics, 12(2), 334.

[18]. El-Kenawy, E. S. M., Khodadadi, N., Khoshnaw, A., Mirjalili, S., Alhussan, A. A., Khafaga, D. S., ... & Abdelhamid, A. A. (2022). Advanced dipper-throated meta-heuristic optimization algorithm for digital image watermarking. Applied Sciences, 12(20), 10642.

[19]. Yang, Z., Sun, Q., Qi, Y., Li, S., & Ren, F. (2022). A hyper-chaotically encrypted robust digital image watermarking method with large capacity using compress sensing on a hybrid domain. Entropy, 24(10), 1486.

[20]. Cedillo-Hernandez, M., Cedillo-Hernandez, A., & Garcia-Ugalde, F. J. (2021). Improving dft-based image watermarking using particle swarm optimization algorithm. Mathematics, 9(15), 1795.

[21]. Dehghani, M., Montazeri, Z., Trojovská, E., & Trojovský, P. (2023). Coati Optimization Algorithm: A new bio-inspired metaheuristic algorithm for solving optimization problems. Knowledge-Based Systems, 259, 110011.

[22]. Jing L, Jingbing L, Jixin M et al (2019) A robust multi-watermarking algorithm for medical images based on DTCWT-DCT and Henon Map. Appl Sci 9:701–723.

[23]. Fengming Q, Jingbing L, Hui L, .et al (2020) A Robust Zero-Watermarking Algorithm for Medical Images Using Curvelet-Dct and RSA Pseudo-random Sequences. In: International Conference on Artifcial Intelligence and Security, Dublin, Ireland 179–190.

[24]. Yangxiu F, Jing L, Jingbing L,et al, (2022) Robust zero-watermarking algorithm for medical images based on SIFT and Bandelet-DCT. Multimedia Tools and Applications 81:16863–16879.

[25]. Cheng Z, Jing L, Jingbing L,et al, (2022) Multi-watermarking algorithm for medical image based on KAZE-DCT. J AMB INTEL HUM COMP 4:1–9.