RESEARCH ARTICLE

RSP Science Hub

International Research Journal on Advanced Science Hub
2582-4376
www.rspsciencehub.com
Vol. 07, Issue 04 April

Check for updates

http://dx.doi.org/10.47392/IRJASH.2025.034

Efficient Net with Adaptive Siberian Tiger Optimization Based Image Steganography and Steganalysis for Biometric Image

Vijitha G[1], Dr.B. Sargunam[2]

[1]Research Scholar, ECE,School of Engineering, Avinashilingam Institute for Home Science & Higher Education for Women, Coimbatore, India.

[2]Professor, ECE, School of Engineering, Avinashilingam Institute for Home Science & Higher Education for Women, Coimbatore India.

Emails: *20phelp003@avinuty.ac.in[1], sargunam_ece@avinuty.ac.in[2]*

Article history

Received: 05 March 2025
Accepted: 15 March 2025
Published: 06 April 2025

Keywords:
Steganography, biometric cover image, Steganalysis, Deep Learning, Embedded image

Abstract

In today's modern world, the need for secure communication has become more paramount particularly in situations where confidentiality is important. Steganalysis intends to determine whether a digital media file comprises concealed data by detecting and analyzing hidden information within the file. The difficulty is effectually differentiating among stego and non-stego files while adapting to increasingly sophisticated steganographic techniques. In this research, an Adaptive Siberian Tiger Optimization_EfficientNet (ASTO_EfficientNet) is designed for image steganography and steganalysis. Firstly, a bit map image is attained from the input biometric cover image. Next, the message to be hidden in the image and bit map image is subjected to the Exclusive-OR (XOR) operation. Thereafter, the XOR-ed outcome is passed to the embedding processes for the generation of the embedded image. Next, the steganalysis process is done to determine the hidden message after the steganography process. The embedded image is converted into a bit map image and is applied to EfficientNet for detecting the hidden message. The performance of EfficientNet is fine-tuned by tuning the optimum weights employing ASTO. The experimental outcomes demonstrated that the ASTO_EfficientNet acquired superior performance with a maximal Peak-Signal-to-Noise Ratio (PSNR) of 40.765 dB and minimum Bit Error Ratio (BER) of 1.147x10-5.

1. Introduction

Steganography is regarded as the advancement of secret communication through the obvious embedding of encrypted data into simple digital media, such as audio, videos, and images. The encrypted messages could be text, audio, video, or images in the bit stream structure [11]. Images, a popular alternative for message descriptions, require less storage than videos and are easier to understand than text. In most cases, the steganographic technique only modifies a single decimal pixel value. [12]. Images are altered in the transformation domain employing techniques, like Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and so on. The transform's coefficients are changed so to accommodate the hidden data. The spatial domain in which steganography operations were performed is indicated by altering the image element. The standard approaches for

steganography are Pixel Value Differencing (PVD) and LSB matching. In addition, the compression domain includes some other steganography approaches [1]. In digital media, steganalysis is exploited for determining the hidden information. The major aim of Steganalysis is to identify questionable messages, determine the information's circumstances, and retrieve the information by chance. To minimize the risk generated by those who utilize steganography mechanisms for malicious uses, steganalysis is typically employed to identify and excerpt hidden messages in digital media. The primary intent is to forecast the secret message by classifying steganography and then excerpting the hidden message, although it is present on the digital platforms under evaluation. The widely employed method is image steganalysis, which eliminates features and prepares various classifiers to increase the mechanism's flexibility [13]. A hand-crafted system is often the foundation of a classical steganalysis approach. The most widely utilized features are the Gaussian Markov random field [1], Local Binary Patterns (LBP) [14], and Gray Level Co-Occurrence Matrix (GLCM) [15]. The field of steganalysis and image perception frequently employs Deep Learning (DL) approaches because they can effectually handle the issues caused by manual feature design. Without the need for expert knowledge, the DL method automatically recognizes features, eradicates aspects exploiting deep networks, and forms steganalysis techniques. This procedure has accelerated with the development of parallel computing and the Graphics Processing Unit (GPU) [1]. Convolutional Neural Networks (CNNs) are regarded as the DL approach that has recently attained significant advantages over traditional access in several regions. With a huge volume of secret information, DL steganography has made significant progress in comparison to traditional steganography and efficiently transformed secret data to obtainable portions of the cover image steganography. However, secret information is restricted to images by lossy deep steganography [3]. Recent studies have frequently employed DL methods for steganalysis in order to overcome the difficulties of aspect-dependent steganalysis. End-to-end learning is made possible by DL, which trains neural networks by commonly employing gradient-based optimization. This assists to generate results directly from the input data without the need to manually extract features [11].

An innovative technique termed ASTO_EfficientNet is introduced in this article for image steganography and steganalysis. The input biometric cover image is primarily utilized to produce a bit map image during the steganography process. Subsequently, the message to be hidden in the image, and the bit map image are fed to the XOR process. Next, the XOR-ed outcome is passed to numerous embedding methods for the generation of the embedded image. Following this, steganalysis process is carried out after the steganography process. In this case, the embedded image is transformed into a bit map image, and the secret hidden message is detected by exploiting EfficientNet. The EfficientNet is fine-tuned by training the ideal weights utilizing the proposed ASTO algorithm. The devised ASTO is formulated by incorporating the adaptive concept in Siberian Tiger Optimization (STO).

The contribution of this article is designated as,

1.1. Proposed ASTO_EfficientNet for Steganalysis

A novel ASTO_EfficientNet is devised in this work for image steganography and steganalysis. Moreover, EfficientNet is fine-tuned by training the optimal weights utilizing the ASTO algorithm, which is engineered by merging the adaptive concept and STO.The residual part of this work is ordered below: Section 2 deliberates a detailed review of the classical steganalysis approaches. Section 3 explains the ASTO_EfficientNet. Section 4 explicates the investigational results and their evaluation. Finally, Section 5 concludes the work.

2. Motivation

Steganalysis is the procedure of finding and assessing hidden data that is contained in media files (audio, video, and images). The task is to determine if data has been concealed and, if so, identify or classify the method used. A major difficulty is addressing the continuous advancement of steganographic methods, which utilize increasingly advanced approaches to obscure hidden data, complicating detection and analysis. Thus, this work designs an effective methodology for image steganalysis called ASTO_EfficientNet. [1]

3. Literature Survey

A novel spatial domain image steganalysis model named Wang-Net was introduced by Wang, Z., et al. [1]. Wang-Net demonstrated superior detection efficiency and minimized complexity. This technique was able to capture important steganographic traces under various embedding

rates and effectually express the features. Nevertheless, this approach considered only gray level images. For image steganalysis, Ren, W., et al. [2] established a Densely Connected Convolutional Neural Network (DCNN). Here, this technique handled hyperparameter training problems and overfitting. However, this strategy was not tested on various databases, which reduced its generalization capability. Zhong, S., et al. devised a Feed-Forward Denoising Convolutional Neural Network (DnCNN) in [3] for image steganalysis. This technique was a highly robust and adaptable weightless DL steganography noise extraction technique. Despite this, this approach suffered from high computational complexity and high expenses. A CNN model was introduced by Agarwal, S., et al. [4] in order to identify context-aware steganography methods. This approach minimized the cost by limiting the amount of available kernels, resulting in a smaller kernel set. However, the lack of single pooling layers reduced the model's ability to effectually capture hierarchical features. Forensics-Aided Content Selection Network (FACSNet) was developed by Huang, S., et al. [5] for heterogeneous image steganalysis. This method enhanced generalization and usefulness while achieving faster convergence. Nonetheless, the network's detection performance and training efficacy were not enhanced by this technique.

3.1. Major challenges

The limitations faced by the baseline steganography methods are signified below,

- An efficient approach termed Wang-Net established in [1] for steganalysis improved the generalization ability and improved the detection accuracy by leveraging advanced feature extraction methods and minimizing overfitting. Nonetheless, this approach was not suitable for the steganalysis of color images.
- DCNN model was devised in [2] for image steganalysis. Here, this method utilized fewer parameters and prevented overfitting issues. Nevertheless, this technique did not attain accurate results and required more parameters for enhancing the outcomes further.
- In [3], the DnCNN approach was introduced for steganalysis, and this model had better scalability and adaptability with low computational complexity. Nonetheless, this method failed to consider wavelet embedding techniques for detecting hidden information within the cover media.
- CNN model was devised in [4] for steganalysis and image steganography and it attained higher detection accuracy and minimized the computational cost. However, this method did not consider efficient optimization algorithms for enhancing the model's performance.
- Despite the development of several steganalysis methods, effectually handling images of altering sizes remains a significant challenge. Furthermore, the emergence of robust steganographic systems has made the task of detecting hidden messages increasingly complicated and time-consuming.

3.2. Proposed Adaptive Siberian Tiger Optimization EfficientNet for Image Steganography and Steganalysis

The proposed work is carried out under two processes, namely steganography and steganalysis process.

3.3. Steganography

The steganography process first creates a bit map image from an input biometric cover image. The bit map image and the message to be hidden in an image are then passed to the XOR operation for the generation of XOR-ed output. Then, the resultant output is passed to various embedding processes, like DWT-based embedding [6], Least-Significant Bit **(**LSB) embedding [7], and DCT-based embedding [6] for the generation of the embedded image. Following this, the steganalysis process is carried out, here the embedded image is again converted into a bit map image and the detection of secret hidden messages is established using the EfficientNet [8]. Furthermore, the EfficientNet model is fine-tuned by training the optimal weights by exploiting the ASTO algorithm. The proposed ASTO is developed by the incorporation of the adaptive concept in STO [9]. Figure 1 signifies the schematic representation of ASTO_EfficientNet for Image steganography and steganalysis

3.4. Image acquisition

In this case, the cover image that contains the hidden message is obtained from the biometric database [10], which is designated below,

$$N = \{N_1, N_2, ..., N_h, ..., N_Q\} \quad (1)$$

Here, N_h represents the h^{th} cover image, which is exploited for embedding and Q indicates the total amount of images in the database N final embedded image is η_w. The subsequent describes the steps involved in embedding using these techniques:

3.5. Wavelet Based Embedding

3.5.1. Bit Map Image

The binary data that signifies pixel values in an image is termed a bitmap image. Generating and storing image patterns is a common use for this image format in computer graphics. For the purpose of generating the final image outcome, the data is organized in rows and columns, with a null or numeric value assigned to every cell. Each component of cover image is converted into binary format to produce bitmap image output . When embedding, the hexadecimal pattern of the secret message is contemplated and converted to binary. The binary and hexadecimal values are XORed to attain the outcome . The bit map portrait , and the XOR-ed output are further allowed to the embedding methods.

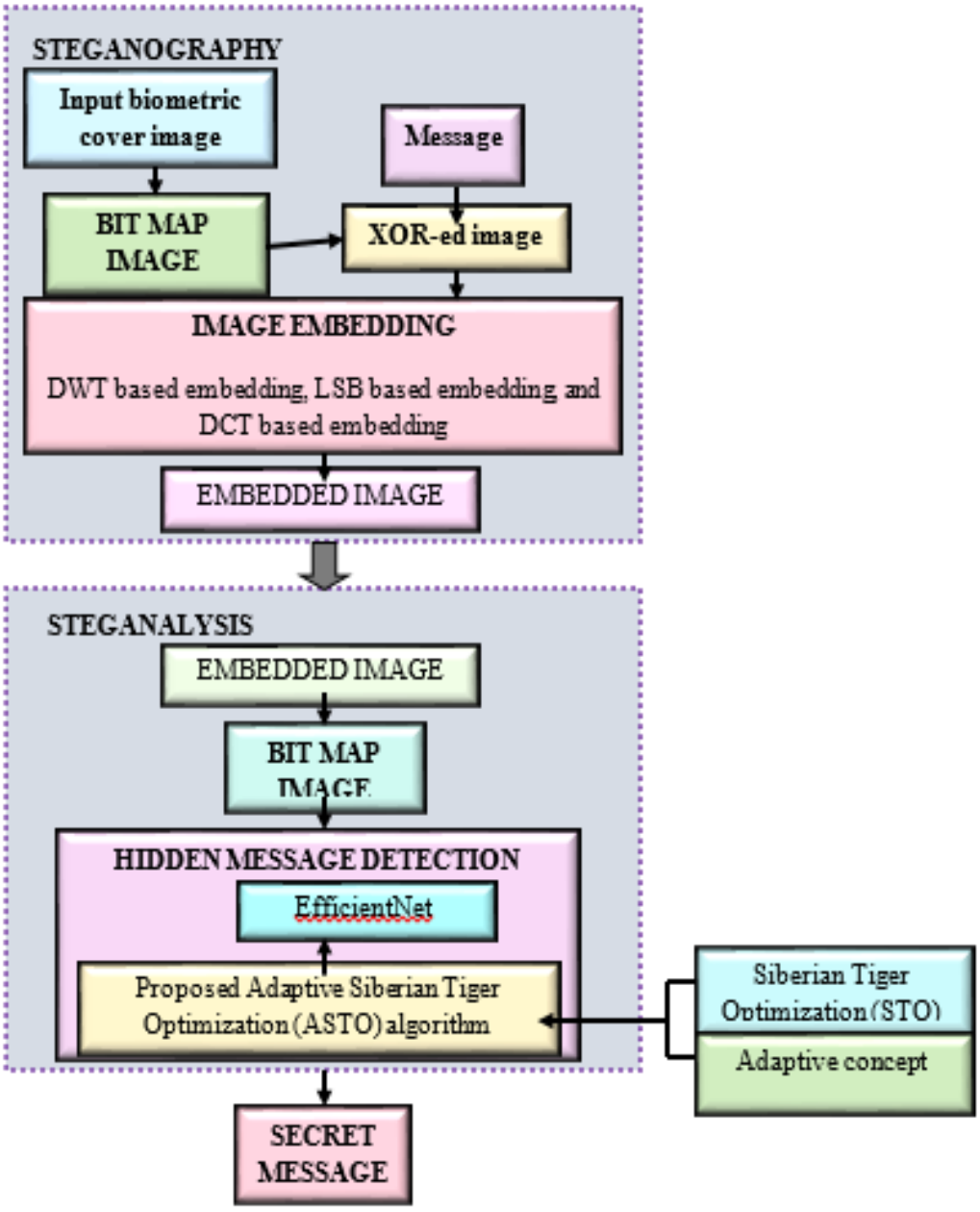


Figure 1 Pictorial Representation of ASTO_EfficientNet for Image Steganography and Steganalysis

3.5.2. Embedding techniques

The message z_b and bitmap image N_{bit} are employed for embedding methods, including LSB-based embedding, DWT, and DCT. Image embedding is a substantial technique in image steganography, which intends in implanting secret message into the cover image. The bit map image that is received is N_{bit} and XOR-ed output z_b are subjected into many embedding techniques to produce the An image can be watermarked by converting it from the pixel domain to the frequency domain employing the popular DWT-based embedding [6] model. This method down-samples the image into sub-bands, including Low High (LH), High Low (HL), Low-Low (LL), and High-High (HH). The secret message is generally embedded in a low-resolution image, which is signified by the LL sub band. The DWT coefficients of the bit map image are modified to encode the secret message.

3.5.2.1. LSB based embedding

The LSB-based embedding [7] technique hides data from plain view rather than employing a denser cover image area by simply applying data bits for the targeted coordinate. This approach makes it much simpler for hiding the secret message in the cover image without making variations. An LSB-based model is exploited to replace LSB with a high-bit image employing the resulting XOR-ed information and bit map image . The inverse LSB method is utilized to find actual image after the final image is fed to several noises.

3.5.2.2. DCT based embedding

A DCT-based embedding approach is utilized to convert the spatial domain image into the frequency domain [6]. The image is compressed using quantization, transforming it into a series of cosine waves across various frequencies. The image is generally converted into sub-bands in frequency domains by DCT, and the band is selected based on the image's content information in the blocks.

The output is obtained by individually embedding the resulting XOR-ed information in the bit map image using DWT, DCT, and LSB-based embedding methods. The obtained embedded image is represented as . Thereafter, each output image that contains secret information is fed separately to steganalysis technique for identifying secret messages. [2] for the generation of the embedded image

3.6. Steganalysis

The Steganalysis method intends to determine the secret message hidden within digital media files. This step is performed to excerpt the hidden message from the embedded image. The input is considered as the embedded image , which is then changed to the bitmap image . The bitmapped image is transferred to EfficientNet [8], which detects the secret hidden message. The performance of EfficientNet model is trained by using proposed ASTO algorithm, which is the amalgamation of adaptive concept and STO.

3.6.1. Architecture of EfficientNet

The EfficientNet [8] is fed with the embedded bitmap image as input and generates an output . EfficientNet is a scaling model, which utilizes a compound coefficient to compute image resolution, width, and depth equally. Further, EfficientNet consists of various layers, namely Activation, Conv layer, Squeeze-and-Excitation (SE) Layers, Batch Normalization, Dense layer Mobile Inverted Bottleneck (MBConv), and Global Average Pooling (GAP). MBConv layers are utilized in the EfficientNet model for enhancing efficiency by using depth wise separable convolutions, which minimalize parameters and computations. GAP is generally found to be highly robust and it calculates a simple average with equal weights, and neither receptive fields nor areas of the embedded image are explicitly given any particular significance. EfficientNet models attain high performance with fewer parameters and lower computational cost. Consequently, the GAP function performs the operation stated beneath.

$$R_{\mu} = GAP\left(R_{\mu-1}\right) = \frac{1}{z \times z} \sum_{w=0}^{z \times z} \eta_w \qquad (2)$$

Here, GAP operation's input layer is designated by and signifies output layer. Moreover, count of feature vector is indicated as .

In order to calculate attention, a weighted average is computed and signified below:

$$R_{\mu} = GAP\,atn\left(R_{\mu-1}\right) = \sum_{w=0}^{z \times z} F_w * \eta_w \qquad (3)$$

Here, typifies the weights that this technique will automatically learn. In this technique, a specific branch of network layers is enclosed, and each image concentrates attention on its equivalent areas to learn about more suitable weights. Finally, the attention approach selects a subset of the feature vectors and assigns them several weights. Generally, attention is articulated as,

$$G = f_{\zeta}(b) \quad (4)$$

$$d = G \otimes D \quad (5)$$

wherein, attention network is signified as , the value of attention weight amongst range null and one, i.e. , feature map is represented as , parameters are specified as , and element-wise multiplication is specified by . Hard attention occurs when is neither zero nor one, whereas soft attention occurs when the weights hold ranges between one and null, and here, soft attention mechanism is used. The outcome produced in the EfficientNet model is typified as . The architectural value of EfficientNet is denoted in Figure 2

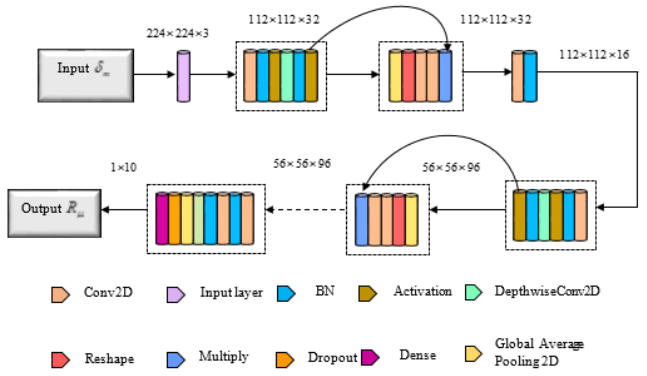


Figure 2 Structural Outlook of EfficientNet

3.7. Training using Adaptive Siberian Tiger Optimization

The devised ASTO technique enhances EfficientNet's performance when detecting secret messages. The adaptive concept is integrated into the STO [9] algorithmic approach for the design of the ASTO. The natural hunting and fighting behavior of the Siberian tiger served as the inspiration for the STO metaheuristic algorithm. The algorithm achieves a balance among exploitation and exploration, which is essential for effectually handling challenging optimization issues. Moreover, adaptive concepts can modify the learning process to avoid overfitting. Integrating the adaptive concept with STO, ASTO enhances the reliability, scalability, and convergence rate. The mathematical modeling of ASTO is explained beneath [3]

3.7.1. Initialization

In the ASTO population, every Siberian tiger is a potential solution, and its location in the search space corresponds to the variable values of the issue. Equation (6) represents the mathematical representation of the population as a matrix with every tiger being modeled as a vector.

$$J = \begin{bmatrix} J_1 \\ \vdots \\ J_n \\ \vdots \\ J_{\varpi} \end{bmatrix}_{\varpi \times L} \quad (6)$$

Here, J represents the population matrix that defines the position of the Siberian tigers, the overall amount of Siberian tigers is specified as ϖ and J_n indicates the n^{th} Siberian tiger. The Siberian tigers' initial position in the search space is arbitrarily determined by employing equation (7).

$$k_{n,\vartheta} = lb_{\vartheta} + \beta_{n,\vartheta} \cdot (ub_{\vartheta} - lb_{\vartheta}), \quad n = 1,2,...,\varpi, \ \vartheta = 1,2,...,L \quad (7)$$

Here, the count of problem variables is typified by L, a random number within the interval of [0,1] is specified by $\beta_{n,\vartheta}$, $k_{n,\vartheta}$ implies ϑ^{th} dimension of J_n in the search space, upper and lower bounds of ϑ^{th} problem variable is stipulated as ub_{ϑ} and lb_{ϑ}

3.7.2. Fitness calculation

Once the Siberian tiger's location has been updated into the search space, their fitness is calculated employing the ensuing expression:

$$MSE = \frac{1}{q}\sum_{\mu=1}^{q}\left(R_{\mu}^{*} - R_{\mu}\right)^2 \quad (8)$$

Here, the outcome from EfficientNet is denoted as R_{μ}, R_{μ}^{*} designates the expected outcome, Mean Square Error is denoted as MSE, and the training sample count is specified by q.

3.7.3. Prey hunting phase

The first phase is to update ASTO members by imitating the hunting technique of the Siberian tiger, which involves choosing and tracking its prey before capturing it. In addition, the selection and attack of prey update the positions of ASTO members, resulting in significant variations that improve global search and exploration. Members with better objective function values are selected for prey positions. The novel location of the Siberian tiger determined by simulating the attack on the prey is expressed as, [4]

$$k_{n,\vartheta}(E+1) = k_{n,\vartheta}(E) + \beta_{n,\vartheta} \cdot \left(TP_{n,\vartheta} - B_{n,\vartheta} \cdot k_{n,\vartheta}\right) \quad (9)$$

wherein, $TP_{n,\vartheta}$ indicates targeted prey by the n^{th} Siberian Tiger and ϑ^{th} dimension,

$k_{n,\vartheta}(E+1)$ signifies the new location of n^{th} member and ϑ^{th} dimension at $(E+1)^{th}$ iteration, and a random number ranging among $\{0 to 5\}$ is represented as $B_{n,\vartheta}$, and is made adaptive here. Further, $B_{n,\vartheta}$ is given by,

$$B_{n,\vartheta} = 2.5*\left(1+\sin\left(H\left(0.2\pi\right)\right)\right) \qquad (10)$$

where, H represents a random number.

The location of the ASTO members is also modified in this phase in accordance with the chase procedure, in which the Siberian tiger approaches its prey. This improves the algorithm's ability to search and exploit locally. The novel location near the attack site is determined using equation (11). wherein, maximum iteration is represented by $E_{\max}$.

3.8. Fighting with a bear

Siberian tigers and bears battle for food and survival. In the second phase, ASTO members are updated by simulating the tiger's ambush and attack strategies utilized in these conflicts. The attack and conflict phases are replicated in the conflict, which lasts until the tiger defeats the bear. Equation (12) is used to determine the new location for the n^{th} ASTO member, $n=1,2,...,\varpi$.

$$k_{n,\vartheta}(E+1)=\begin{cases} k_{n,\vartheta}+\beta_{n,\vartheta}\cdot\left(k_{s,\vartheta}-B_{n,\vartheta}\cdot k_{n,\vartheta}\right), & M_s < M_n \\ k_{n,\vartheta}+\beta_{n,\vartheta}\cdot\left(k_{n,\vartheta}-B_{n,\vartheta}\cdot k_{s,\vartheta}\right), & else \end{cases}$$

wherein, $k_{s,\vartheta}$ indicates the ϑ^{th} dimension of a bear position, $\vartheta=1,2,...,L$, wherein s is arbitrarily selected from the set $\{1,2,...,n-1,n+1,...,\varpi\}$. The second phase involves minor adjustments that enhance local search and exploitation by updating the positions of ASTO members based on simulated combat conflicts. Equation (13) is utilized to determine a random location in nearby areas of the fight.

$$k_{n,\vartheta}(E+1)=k_{n,\vartheta}+\frac{\beta_{n,\vartheta}}{E}\left(ub_{\vartheta}-lb_{\vartheta}\right),\ n=1,2,...,\varpi,\vartheta=1,2,...,L,\ and\ E=1,2,...,E_{\max} \qquad (13)$$

3.9. Re-evaluation of fitness

Following modification of the solutions, the viability of the solution is evaluated utilizing expression (8) to compute fitness. [7]

3.10. Termination

The aforementioned procedures are continuously done till the final requirement is attained. Integrating the adaptive concept into the STO algorithm increases the proposed ASTO algorithm's exploratory capabilities. Moreover, ASTO enhances steganalysis by enabling faster convergence and avoiding local optima. This improvement allows the algorithm to better handle evolving steganographic methods, enhance PSNR, and minimize the BER required to detect hidden messages or data. [5]

3.11. Results and discussion

The outcomes acquired from the experimentation of ASTO_EfficientNet are briefly presented in this section. Moreover, this section outlines the discussion conducted to evaluate the supremacy of the devised ASTO_EfficientNet model in performing steganalysis. [6]

3.12. Experimental Setup

The designed steganalysis scheme, termed as ASTO_EfficientNet model is executed employing Python tool with a Biometric database [10]. The simulation parameters of EfficientNet are demonstrated in Table 1.

Table 1 Simulation Parameter of EfficientNet

Parameter	Values
Pre-trained weights	ImageNet
dropout_rate	0.5
Epoch	60
Batch_size	64
optimizer	ASTO
activation	softmax
loss	MSE

Table 2 presents the simulation parameters of ASTO.

Table 2 Simulation Parameter of ASTO

Parameter	Values
Population size	50
UB	10
Dimension	100
LB	-10
Maximum iteration	1000

3.13. Dataset Description

The biometrics of 49 different subjects were collected among April 2009 and April 2013 and are included in the Biometric dataset [10]. Scanners for shelf experiments and other sensors are utilized to

take the images. This dataset also includes each subject's fingerprint images that were collected periodically, which includes a folder containing individual sensors and subjects. [8]

3.14. Evaluation Metrics

Performance measures, including PSNR and BER are employed to compute the superiority of the ASTO_EfficientNet model, and are described below, ***-PSNR*:** PSNR measures the proportion of the maximum signal power to the noise power distorted, the input's quality and embedded images that are recorded is validated. PSNR is calculated below,

$$PSNR = 10 * \log_{10}\left[\frac{(255)^2}{\frac{1}{W\times\varsigma}\sum_{w=0}^{W-1}\sum_{p=0}^{\varsigma-1}\left[\chi(w,p)-\chi^*(w,p)\right]^2}\right]$$

wherein, image size is designated as $W\times\varsigma$, cover fame is indicated by χ, and stego frame is represented as χ^*. ***-BER:*** The BER measure is employed to evaluate the robustness of the ASTO_EfficientNet method and is articulated beneath,

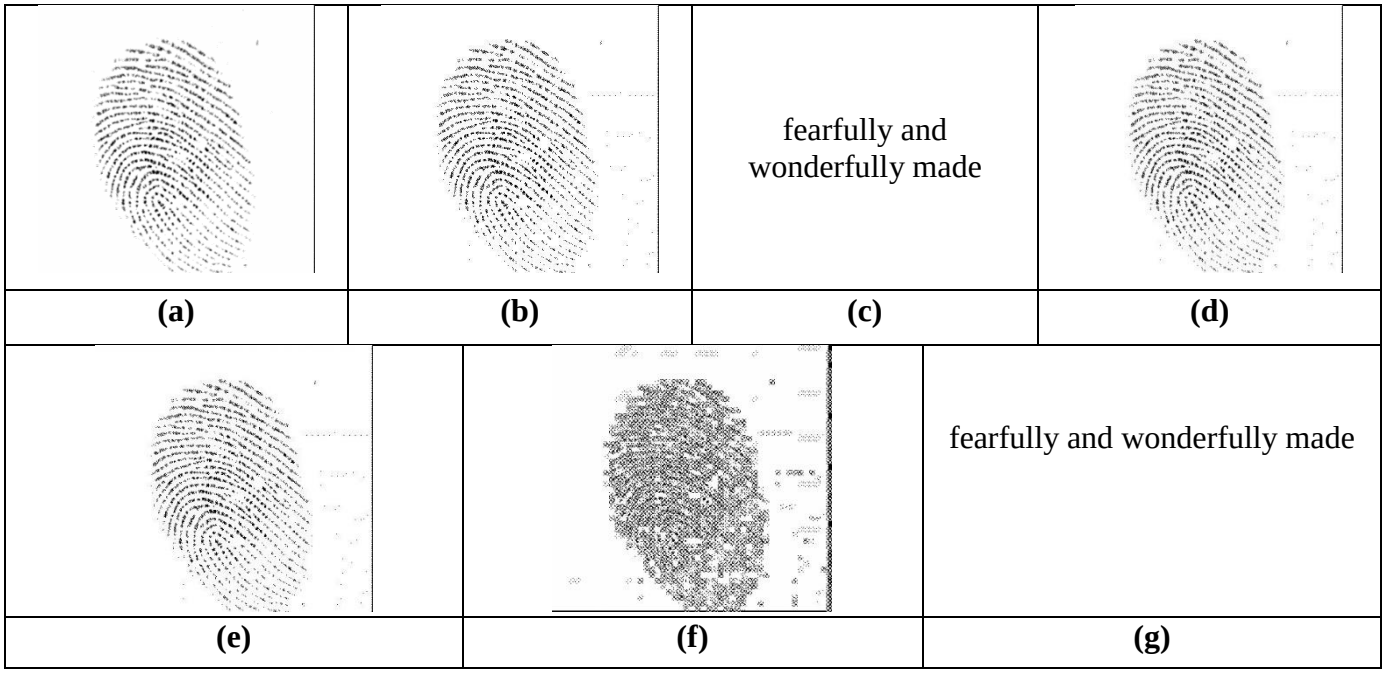
$$BER = \frac{\sum_{w=0}^{W}\sum_{p=0}^{\varsigma}\left[\chi(w,p)-\chi^*(w,p)\right]^2}{W\times\varsigma}$$

3.15. Image results

This section deliberates the investigational consequences of the ASTO_EfficientNet for key sizes 32 and 128.

3.15.1. For key size 32

This section demonstrates the ASTO_EfficientNet's experimental outcomes for key size 32, which are depicted in Figure 3. Figure 3a) displays the input image. The bit map image and secret message are specified in Figure 3b) and Figure 3c). Further, wavelet-based embedding is represented in Figure 3d). Also, Figure 3e) and Figure 3f) indicate the DCT-based embedding image and recovered message. [9]



(a)	(b)	(c)	(d)
(e)	(f)	(g)	

Table 3 Sample Images of ASTO_Efficientnet for Key Size 32 Based on A) Input, B) Bit Map Image, C) Secret Message, D) Wavelet-Based Embedding, E) LSB-Based Embedding, F) DCT-Based Embedding, And G) Recovered Message

3.15.2. For key size 128

The sample images of the ASTO_EfficientNet for key size 128 are demonstrated here and are depicted in Figure 4. The input image and bit map images are signified in Figure 4a) and Figure 4b). The secret image and wavelet-based embedded image are represented in Figure 4c) and Figure 4d). Moreover, Figure 4e) and Figure 4f) depicts LSB-based embedding and DCT-based embedding. The

recovered message is specified in Figure 4g). [10]

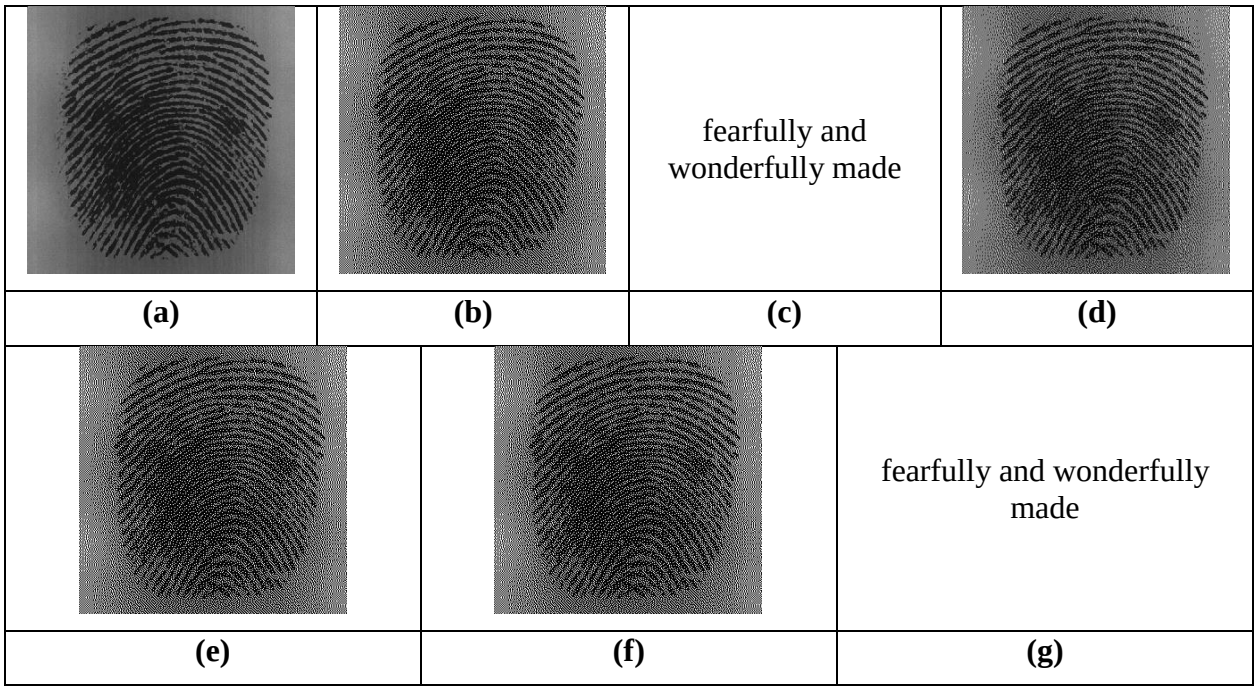


Table 4 Experimental Results of the ASTO_Efficientnet for Key Size 128 in Terms of A) Input Image, B) Bit Map Image, C) Secret Message, D) Wavelet-Based Embedding, E) LSB-Based Embedding, F) DCT-Based Embedding, and G) Recovered Message

4. Comparative methods

The superiority of the established ASTO_EfficientNet is calculated by contrasting it with baseline steganalysis strategies, such as Wang-Net [1], DCNN [2], DnCNN [3], CNN [4], CAViaR Student Psychology based Optimization- Deep Maxout network (CSPBO-DMN), and Efficient Quantum Convolutional Network (EQC-Net).

4.1. Comparative assessment

An explicit valuation of the superiority of the devised ASTO_EfficientNet model employing various embedding models, including LSB-based, DWT-based, and DCT-based embedding is presented here. [11]

4.2. DCT-based embedding

Figure 5 signifies the investigation of ASTO_EfficientNet on the basis of DCT-based embedding. The PSNR-based evaluation of the ASTO_EfficientNet is depicted in Figure 5a). At a key size of 256, the PSNR attained by ASTO_EfficientNet is 43.654dB, whereas prior approaches including CSBPO-DMN, DnCNN, Wang-Net, CNN, DCNN, and EQC-Net computed PSNR of 39.765dB, 33.754dB, 28.754dB, 36.654dB, 30.865dB, and 41.765dB. Similarly, the evaluation based upon BER of the ASTO_EfficientNet is represented in Figure 5b). In this case, the BER of 6.79999×10^{-5} is acquired by the ASTO_EfficientNet for key size of 256. The classical approaches measured BER of 1.278×10^{-4} by CSBPO-DMN, 6.479×10^{4} by DnCNN, 8.468×10^{-4} by Wang-Net, 3.579×10^{-4} by CNN, 7.654×10^{4} by DCNN, and 7.579×10^{-5} by EQC-Net.

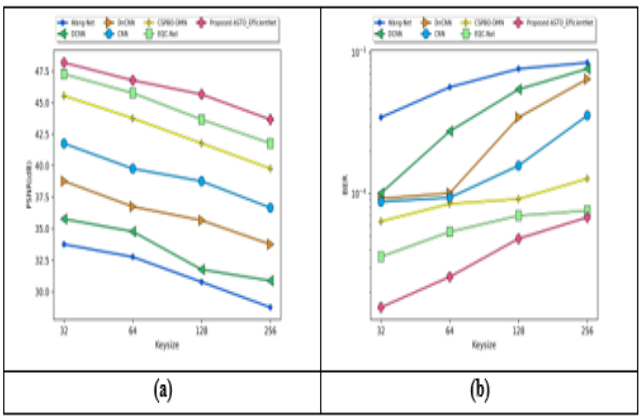


Figure 5 Appraisal of ASTO_EfficientNet Concerning DCT-Based Embedding a) PSNR and b) BER

4.3. DWT-Based Embedding

Figure 6 specifies the comparative valuation of

ASTO_EfficientNet with DWT-based embedding. In Figure 6a), the appraisal of the ASTO_EfficientNet regarding PSNR is demonstrated. Here, the ASTO_EfficientNet achieved a PSNR of 42.654dB for key size of 256, and PSNR calculated by the existing models, including CSBPO-DMN is 38.765dB, DnCNN is 34.765dB, Wang-Net is 29.654dB, CNN is 36.765dB, DCNN is 31.754dB, and EQC-Net is 40.654dB. Likewise, the BER-based analysis of the ASTO_EfficientNet is signified in Figure 6b). Foe key size of 256, the BER recorded by the ASTO_EfficientNet is 5.477x10-5, while the BER obtained by CSBPO-DMN is 7.479x10-5, DnCNN is 1.268x10-4, Wang-Net is 6.900x10-4, CNN is 1.257x10-4, DCNN is 3.579x10-4, and EQC-Net is 4.577x10-4. [13]

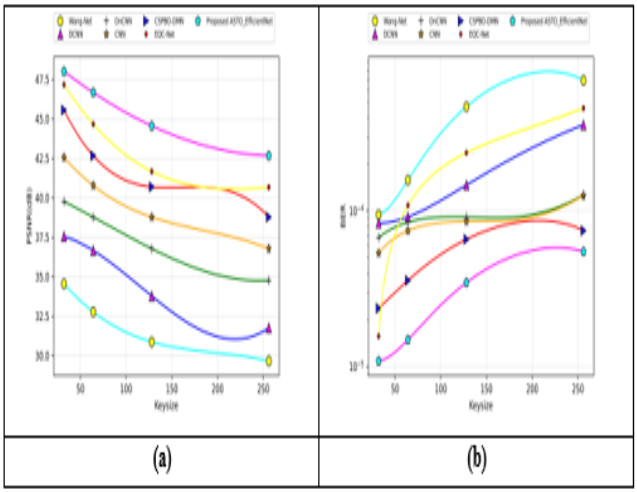


Figure 6 Appraisal of ASTO_EfficientNet Concerning DWT-based embedding a) PSNR and b) BER

4.4. LSB based embedding

Figure 7 implies the appraisal of ASTO_EfficientNet based upon LSB-based embedding. Figure 7a) denotes the appraisal of the ASTO_EfficientNet concerning PSNR. The ASTO_EfficientNet gained a PSNR of 40.765dB with key size of 256, but the traditional schemes, like CSBPO-DMN, DnCNN, Wang-Net, CNN, DCNN, and EQC-Net obtained a lower PSNR of 34.754dB, 30.765dB, 26.765dB, 31.755dB, 28.578dB, and 37.7654dB. In Figure 7b), the investigation of ASTO_EfficientNet with respect to BER is specified. The ASTO_EfficientNet quantified a BER of 1.147x10-5, while BER recorded by the classical models is 5.689x10-5 by CSBPO-DMN, 8.755x10-5 by DnCNN, 2.346x10-4 by Wang-Net, 8.755x10-5 by CNN, 9.654x10-5 by DCNN and 1.877x10-5 by EQC-Net for key size of 256.

1.1. Comparative Discussion

Table 3 demonstrates the comparative discussion of the ASTO_EfficientNet for image steganalysis, correlating it with several steganalysis approaches, such as CSBPO-DMN, DnCNN, Wang-Net, CNN, DCNN, EQC-Net on the basis of BER and PSNR. Here, the ASTO_EfficientNet attained a superior PSNR of 40.765dB and minimum BER of 1.147x10-5 for the LSB-based embedding method. Furthermore, traditional schemes, namely CSBPO-DMN, DnCNN, Wang-Net, CNN, DCNN, and EQC-Net obtained PSNR of 34.754dB, 30.765dB, 26.765dB, 31.755dB, 28.578dB, and 37.7654dB. Also, the BER recorded by the classical models are 5.689x10-5 by CSBPO-DMN, 8.755x10-5 by DnCNN, 2.346x10-4 by Wang-Net, 8.755x10-5 by CNN, 9.654x10-5 by DCNN and 1.877x10-5 by EQC-Net for the key size of 256. Further, STO provides a strong global search and robustness, while the adaptive concept allows for continuous refinement and faster convergence. Thus, the performance of EfficientNet is enhanced and boosting both its embedding capacity and its ability to detect steganographic content, making it highly efficient in steganography tasks. [14]

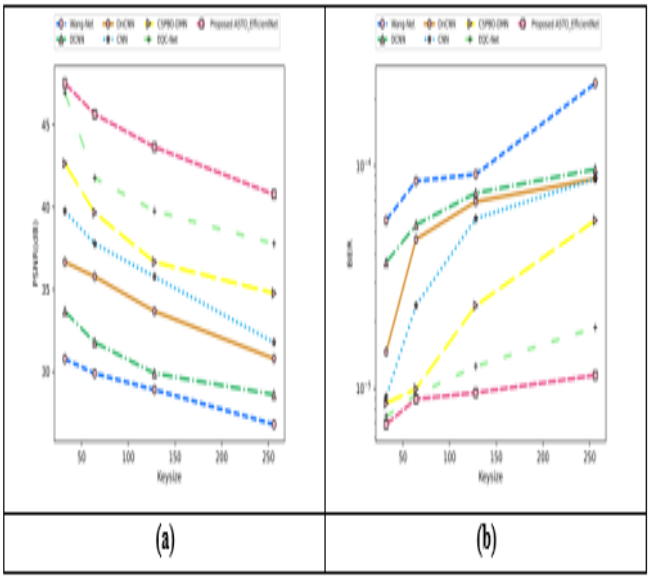


Figure 7 Evaluation of ASTO_EfficientNet Considering LSB-Based Embedding A) PSNR and B) BER

Table 3 Comparative Discussion of ASTO Efficient Net

Embedding technique	Metrics	Techniques						
		Wang-Net	DCNN	DnCNN	CNN	CSPBO-DMN	EQC-Net	Proposed ASTO_EfficientNet
DCT based embedding	*PSNR (dB)*	28.754	30.865	33.754	36.654	39.765	41.765	43.654
	BER	$8.468x10^{-4}$	$7.654x10^{4}$	$6.479x10^{4}$	$3.579x10^{-4}$	$1.278x10^{-4}$	$7.579x10^{-5}$	$6.79999x10^{-5}$
DWT based embedding	*PSNR (dB)*	29.654	31.754	34.765	36.765	38.765	40.654	42.654
	BER	$6.900x10^{-4}$	$3.579x10^{-4}$	$1.268x10^{-4}$	$1.257x10^{-4}$	$7.479x10^{-5}$	$4.577x10^{-4}$	$5.477x10^{-5}$
LSB based embedding	*PSNR (dB)*	26.765	28.578	30.765	31.755	34.754	37.7654	**40.765**
	BER	$2.346x10^{-4}$	$9.654x10^{-5}$	$8.755x10^{-5}$	$8.755x10^{-5}$	$5.689x10^{-5}$	$1.877x10^{-5}$	**$1.147x10^{-5}$**

Conclusion

Steganalysis involves detecting and examining hidden messages within digital media, like images, audio, or video. This process focuses on identifying variations made by steganographic approaches, which secures the information that are difficult to analyze and detect. This article presents ASTO_EfficientNet to recover the original message via steganalysis and steganography. Firstly, in the steganography process, the bit map image is produced from an input biometric cover image. Next, the message to be hidden in the image and bit map image is subjected to the XOR operation. Later, XOR-ed outcome is fed to the various embedding processes for the generation of the embedded image. Next, the steganalysis process is done for identifying the hidden message. Further, the embedded image is changed into a bit map image and thus the secret hidden messages is established is detected by EfficientNet. The performance of EfficientNet is fine-tuned by training the optimal weights using ASTO. The experimental outcomes proved that ASTO_EfficientNet attained higher performance with a maximum PSNR of 40.765dB and minimal BER of 1.147x10-5. Future work aims to consider Transfer Learning (TL) techniques for boost the model's accuracy. [15]

References

[1]. Wang, Z., Chen, M., Yang, Y., Lei, M. and Dong, Z., "Joint multi-domain feature learning for image steganalysis based on CNN", EURASIP Journal on Image and Video Processing, pp.1-12, 2020.

[2]. Iskanderani, A.I., Mehedi, I.M., Aljohani, A.J., Shorfuzzaman, M., Akther, F., Palaniswamy, T., Latif, S.A. and Latif, A., "Artificial intelligence-based digital image steganalysis", Security Artificial intelligence-based digital image steganalysis and Communication Networks, pp.1-9, 2021.

[3]. Zhong, S., Weng, W., Chen, K. and Lai, J., "Deep-learning steganalysis for removing document images on the basis of geometric median pruning", Symmetry, vol. 12, no. 9, pp.1426, 2020.

[4]. Agarwal, S., Kim, C. and Jung, K.H., "Steganalysis of Context-Aware Image Steganography Techniques Using Convolutional Neural Network", Applied Sciences, vol. 12, no. 21, pp. 10793, 2022.

[5]. Huang, S., Zhang, M., Kong, Y., Ke, Y. and Di, F., "FACSNet: Forensics aided content selection network for heterogeneous image steganalysis", Scientific Reports, vol. 14, no. 1, pp. 26258, 2024.

[6]. Garg, P. and Kishore, R.R., "An efficient and secured blind image watermarking using ABC optimization in DWT and DCT

domain", Multimedia Tools and Applications, vol. 81, no. 26, pp.36947-36964, 2022.

[7]. Kumar, A., "A review on implementation of digital image watermarking techniques using LSB and DWT", Information and Communication Technology for Sustainable Development: Proceedings of ICT4SD 2018, pp.595-602, 2020.

[8]. Alhichri, H., Alswayed, A.S., Bazi, Y., Ammour, N. and Alajlan, N.A., "Classification of remote sensing images using EfficientNet-B3 CNN model with attention", IEEE access, vol. 9, pp.14078-14094, 2021.

[9]. Trojovsky, P., Dehghani, M. and Hanus, P., "Siberian tiger optimization: A new bio-inspired metaheuristic algorithm for solving engineering optimization problems", IEEE Access, vol.10, pp.132396-132431, 2022.

[10]. The Biometric dataset was taken from "http://biometrics.idealtest.org/findTotalDbByMode.do?mode=Fingerprint", accessed on February, 2025.

[11]. Ren, W., Zhai, L., Jia, J., Wang, L. and Zhang, L., "Learning selection channels for image steganalysis in spatial domain", Neurocomputing, vol. 401, pp.78-90, 2020.

[12]. Agarwal, S., Kim, H. and Jung, K.H., "High-Pass-Kernel-Driven Content-Adaptive Image Steganalysis Using Deep Learning", Mathematics, vol. 11, no. 20, pp. 4322, 2023.

[13]. Kheddar, H., Hemis, M., Himeur, Y., Megías, D. and Amira, A., "Deep Learning for Diverse Data Types Steganalysis, A Review", arXiv preprint arXiv:2308.04522, 2023.

[14]. Qu, Z., Cheng, Z., Liu, W. and Wang, X.,"A novel quantum image steganography algorithm based on exploiting modification direction", Multimedia Tools and Applications, vol. 78, pp. 7981-8001, 2019.

[15]. Qu, Z., Wu, S., Wang, M., Sun, L. and Wang, X., "Effect of quantum noise on deterministic remote state preparation of an arbitrary two-particle state via various quantum entangled channels", Quantum Information Processing, vol. 16, no. 12, pp. 306, 2017.