Egyptian Informatics Journal 24 (2023) 100385

Contents lists available at ScienceDirect

Egyptian Informatics Journal

journal homepage: www.sciencedirect.com

Toward secret data location via fuzzy logic and convolutional neural network

Ntivuguruzwa Jean De La Croix [a,b], Tohari Ahmad [a,*]

[a] Department of Informatics, Institut Teknologi Sepuluh Nopember (ITS), Kampus ITS Keputih Sukolilo, Surabaya 60111, Indonesia
[b] African Center of Excellence in the Internet of Things, College of Science and Technology, University of Rwanda, Kigali 3900, Rwanda

ARTICLE INFO

Article history:
Received 16 March 2023
Revised 9 May 2023
Accepted 22 May 2023
Available online 30 May 2023

Keywords:
Fuzzy logic
Spatial domain
CNN
Network infrastructure
Steganalysis
Information security

ABSTRACT

Locating hidden data in digital images, otherwise called steganalysis, is a process of identifying the existence of secret messages within digital images. Steganalysis is used to manage digital data transmission by detecting the possible hidden information that can be used to violate the network policy; hence, it helps the development of policies and regulations aimed at strong protection from cyber threats to individuals' and organizations' data. The research works in the field of information security commonly focus on developing the locating approaches for non-adaptive steganography, which present a problem of less investigation of the complex challenge of locating the payload embedded with an adaptive steganographic algorithm. In this article, we propose a method to locate hidden data in a digital image in three stages: a) Identification of the modification maps between the carrier and final images. b) Using the modification maps as input to Mamdani fuzzy inference with four input membership functions: covariance map matrix, compass mean matrix, distance vector matrix, and pixel intensity matrix, and one output membership function, notably the fuzzy correlation maps. c) Feeding the fuzzy correlation maps to a convolutional neural network to identify the pixels with confidential data from the innocent pixels. By experimenting with our method against four steganographic algorithms, namely, HILL, HUGO-BD, WOW, and S-UNIWARD, the recall rates for the four algorithms initially increase in a similar range and improve with increasing payload capacity, which justifies the outperformance of the proposed strategy over the existing methods.

1. Introduction

Steganography is a subdomain of the information security domain which mainly works on ensuring the covert transmission of secret messages using multimedia content as carriers. Generally, a steganographic technique adopts data-hiding methods to conceal the confidential data in the spatial content of an original digital medium, such as an image referred to as a cover to result in a transformed image, also referred to as a stego [2,7,8,30]. The recent two decades marked a significant advancement of steganography in digital images where various schemes have been proposed for content-adaptive paradigms [3,11,19]. The adaptive steganographic models mainly consider confidential data as a fidelity constraint for the source coding practice rather than considering the carrier media. A reverse scheme to steganography has also been developed to detect the presence of secret information in a digital image or even extract confidential data. This counter-art to steganography has been referred to as steganalysis.

For any steganographic scheme, the main purpose is to maximize the imperceptibility of additional data in the content, making a cover media. In digital images, the data are hidden, avoiding any visual or statistical distortion of the stego by ensuring its closest similarity to the cover image. In the past decade, various modern steganographic schemes for both spatial and JPEG domains have been presented; among them, the mostly known spatial adaptive steganographic schemes we can say HIgh-pass Low-pass Low-pass (HILL) (B [24]. Highly Undetectable steGO Gibbs construction with Bounding Distortion (HUGO-BD) [13], Wavelet Obtained Weights (WOW) [17], the Spatial version of the UNIversal WAvelet Relative Distortion (S-UNIWARD) [18], and among the JPEG domain we can say Uniform Embedding Distortion (UED) (Linjie [26], Uniform Embedding Revisited Distortion (UERD) [16], and JPEG Universal WAvelet Relative Distortion (J-UNIWARD) [16].

* Corresponding author.
E-mail addresses: 7025221024@mhs.its.ac.id (N.J. De La Croix), tohari@if.its.ac.id (T. Ahmad).

https://doi.org/10.1016/j.eij.2023.05.010
1110-8665/

Based on the high imperceptibility of a stego image, which is a challenge to detect its nature, it is impossible to distinguish with a human eye between the cover and stego image; hence the main task of a steganalyst is to identify a cover from a stego image. Steganalysis is mainly classified into three categories based on the output of the process. A steganalysis process that outputs image classification (as cover or stego) is known as detective steganalysis or binary classification [21]; a steganalysis scheme that targets to provide the locations of the hidden data is known as locative steganalysis [20]; a steganalysis scheme that aims to predict the payload size is also known as quantitative steganalysis [29]; and a steganalysis process that aims to extract the secret bits of the confidential message is called forensic steganalysis [41]. In the existing works on steganalysis, several researchers focused on the binary classification of inquiry images into cover or stego [6,33,47], and some others focused on locative steganalysis but mainly working with LSB replacement and LSB matching [36,42] due to the possibility of discovering the impurities with these types of steganography. Based on the use of Rich Models (RM), and Ensemble Classifiers (EC), most of the state-of-the-art [39,44,45] showed a significant performance in classifying images into cover and stego and relying on the deep learning paradigm, the steganalysis of digital images knew a gradual widespread [6,35,47].

Many prior steganalysis algorithms have given much attention to detective steganalysis, and tasks like steganographic payload location and payload size prediction have yet to be explored considerably. Hence in this study, we mainly focus on the payload location process based on the general idea of steganalysis. Furthermore, based on the cover image prediction (or simply computing for differences between the confirmed stego and the cover images), several works have been proposed targeting a specific type of steganography, such as Least Significant Bit Replacement (LSBR) or the Least Significant Bit Matching (LSBM) [22,23,32] to locate the steganographic payloads which become invalid when these targeting algorithms are applied for universal payload location. Moreover, keeping the same generality, the problem of secret data location, which is also considered as a binary classification departing from a threshold value to classify image's pixels into altered and innocent pixels, most prior locative steganalysis schemes show invalidity when handling modern versions of adaptive steganography which is also a critical limitation with them [20,27,31].

Our study proposes a steganalysis model that uses fuzzy logic and CNN to detect confidential data's location in stego images universally. Our main goals are to provide: i) a universal steganalysis approach to locate the payload embedded using an adaptive steganographic algorithm departing from only one inquiry image, ii) an improved precision while exploring the relationship between the inquiry image's pixels, and iii) improved accuracy in locating the altered pixels (pixels holding steganographic payloads) using the binary classification paradigm of deep learning. To achieve our goals, we depart from the common idea of modern adaptive steganography to conceal the data in the image's texture region. Our method combines fuzzy logic to generate fuzzy correlation maps, which make a fingerprint matrix of an image and a CNN to predict areas with confidential data. Specifically, i) we initially use Syndrome-trellis codes (STCs) [14] to embed the data with a modern adaptive steganography algorithm in a cover image to obtain a stego image and calculate the modification map between the cover and the stego, ii) we use Mamdani fuzzy inference system to compute for the fuzzy correlation maps of the modification maps which enhances the precision in exploring the relationship between the inquiry image's pixels, and iii) we consider the fuzzy correlation maps for classification using CNN which yields an accurate binary classification of the pixels of the inquiry image (referring to the paradigm by Yalcinkaya and Erbas [40].

The main tasks performed in our work to accomplish our aims and reach the targeted theoretical contributions are listed as follows:

(1) Based on the intrinsic features of modern adaptive steganography, we propose a steganalysis scheme that departs from the modification map between the cover and the stego as initial input to the fuzzy inference system that then provides the fuzzy correlation maps that are used for classification in a CNN, unlike the existing approaches, which input a whole image.
(2) To improve the location accuracy by narrowing down errors, we apply fuzzy logic on the modification maps to generate the fingerprint matrix (fuzzy correlation maps) to increase the precision of the relationship between a pixel and its neighbors.
(3) We train our CNN with fuzzy correlation maps to address the scarcity of the training images and the high cost of several operations needed to preprocess the training images to yield reliable payload location accuracy.
(4) We conduct numerical experiments considering two scenarios to locate the steganographic payload, notably known and unknown steganographic payload scenarios. Our method is tested with HILL, HUGO-BD, WOW, and S-UNIWARD.

The next parts of this paper are as follows: In Section 2, we discuss the existing literature focusing on the features of the current methods and their challenges. Section 3 describes our approach and the proposed model, followed by the presentation and discussion of the experimental results in Section 4. In Section 5, we conclude our works and suggest the future takes in line with our model.

2. Related works

Dynamism and innovative discoveries in steganographic algorithms made it imperative to the counter art to steganography for forensic purposes to adapt the same speed to avail new steganalysis approaches. In recent years, the steganalysis of digital images improved significantly due to the introduction of CNNs in solving the classification problem of images into cover (when they don't hold any confidential data) or stego (When they are used as carriers for sensitive information) classes. Several steganalysis techniques, such as detective steganalysis to detect the presence of confidential data in an image [33,38,47], quantitative steganalysis [5,41,46] to estimate the payload size have been proposed. These techniques are mainly used to identify any alteration in the pixels of an image when adding some confidential bits. In fact, they achieved a promising performance but have not been able to identify the location of the altered pixel, which remains a vital practice for digital image forensics. Steganographic payload location has become the most important form of steganalysis, which enables the classification of image pixels based on whether they have been changed by steganography. As per other forms of steganalysis, this locative steganalysis also adopts the paradigm of binary classification among the image's pixels which is rooted in the traditional machine learning pattern recognition algorithms and adopted in CNN-based steganalysis tasks as of Fig. 1.

Liu et al. (2015) introduced a steganalysis scheme to locate concealed information using steganography in the spatial domain. The method involves the retrieval of most cover pixels through recompression, then analyzing the differences in pixel distribution between the cover and stego images. This scheme finally employs the hypothesis testing theory to prove the correctness of locating the embedding positions. Inspired by Liu et al. (2015), Hu et al.

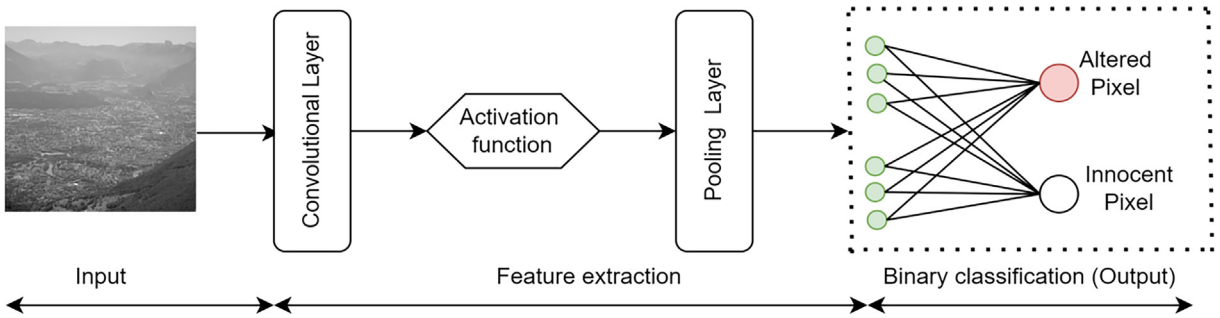


Fig. 1. Architecture of a locative CNN-based steganalysis framework.

[20] proposed an algorithm to locate the secret data hidden with modern adaptive steganography with a hybrid approach based on region selection and CNN. This method focuses on the selected regions with a high probability of carrying confidential data. The proposed CNN is made of three independent subnets set with different parameters. The first subnet mainly serves as a preprocessing module using high-pass filters and "SQUARE5 × 5" to generate image residuals. With interconnection, the residuals are fed to the following subnets with respective kernel sizes 1 × 1, 3 × 3, and 5 × 5. After convolutions that include regular and downsampling operations, the resulting features are merged twice using DepthConcat to generate the output.

To improve the steganographic payload location accuracy using the convolutional neural network paradigm, Sun et al. (2019) developed a deep neural network (DNN) utilizing a tailored scheme based on the mean square difference between adjacent pixels, resulting in improved detection accuracy at a lower computational cost. Bedi et al. (2022) proposed an algorithm to locate the hidden data using a combination of the Denoising Autoencoder (DA) and the Local Bit Binary Pattern (LBBP) operator. In this method, DA aims to identify the learnable inter-relationships in the neighborhood coordinates. Their method compares the corresponding pixel blocks from the stego, and the cover image and the yielded differences are considered for the payload locations. The experimental results showed a promising performance compared to the previous algorithms but still showed a need to improve the efficiency of their whole model. Therefore, Qiao et al. [31], to improve the accuracy of the payload location identification, proposed an algorithm to locate the steganographic payload by considering a single inquiry image. The proposed method uses the neighboring weight algorithm to determine the regions with confidential data. Focusing on the spatial image data, this method starts by predicting the steganographic algorithm and the payload and uses this to generate a random bitstream. The performance shown by the results identified an outperformance of the existing methods.

Wang et al. (2020) presented a steganalysis scheme to locate hidden data by constructing 64 co-frequency sub-images and filtering the obtained sub-images. The proposed approach, which concentrates on the JPEG domain, works on blocks of 8 × 8 in an image by combining the same position coefficients of each block to generate 64 co-frequency mini-images and then apply the Markov model by using the maximum a posterior probability to determine the estimated cover co-frequency mini-images. The computation of the dissimilarities between the probable cover and the calculated residual of the discrete cosine transform coefficient in the same cartesian position in multiple mini-images of the stego type is mainly used to locate the altered parts of an inquiry image. Moreover, a new approach to locate the pixels with confidential data hidden with JPEG steganography has been introduced to mainly work on estimating the cover image by assigning various weights to the discrete cosine transform coefficient residuals based on the texture regions obtained by measuring the local variance (Pan et al., 2022).

The introduction of fuzzy logic, a machine learning and mathematical model, have been significant enlightenment to several computer science applications such as metaheuristic algorithms [15,25,37]; self-controlling application [1,9,12], Autonomous solutions generation [28,10,34]. Benefiting from fuzzy reasoning, Liu et al. [27] departed from (Liu et al., 2015) to propose a new method to locate flipped bits resulting from modern adaptive steganography in the spatial domain. This method computes the modification maps between the cover and stego images and extends them to identify the locations of steganographically modified pixels. The proposed method showed better performance with an average of 90% accuracy in determining the location of the modern adaptive steganography but needs to locate the non-adaptive steganography. Failure to accurately change the pixels in non-adaptive steganography because the pixels modification is generally spread randomly to all the inquiry image pixels differs from the pixel modification in adaptive steganography, which targets the same locations.

In light of the existing literature above clarified, our study proposes a locative steganalysis approach that combines fuzzy reasoning and CNN operations in a hybrid fashion to locate the secret bits embedded within the pixels of an inquiry image.

3. Proposed method

In this Section, we first explain our algorithm's significance in locating the hidden data. Secondly, we describe the steps to generate the modification maps used as input to the fuzzy. Thirdly, we describe a step-by-step process for fuzzy logic; fourthly, we describe our CNN; finally, we give the details of our locating algorithm.

3.1. Significance of our algorithm

Our study introduces a novel locative steganalysis technique that employs a hybrid approach of fuzzy logic and CNN operations to identify the confidential data within an image's pixels. By using fuzzy reasoning in the preprocessing phase of our strategy, we aim to improve the detection process's accuracy and efficiency, enhancing our strategy's overall effectiveness in the locative steganalysis task. Fuzzy logic is a scheme that mathematically allows for decision-making in ambiguous and uncertain situations [1,28,15]. The fuzzy correlation map calculation has been proved as a technique in image processing to reduce noise effects and other image distortions [40]. The computation of fuzzy correlation maps is based on various components such as the covariance map matrix, compass mean matrix, distance vector matrix, and pixel intensity matrix. We detail the description of the correlation maps calcula-

tion in Subsection 3. 3. It is worth noting that our strategy prefers to use the modification maps between the two versions of the stego images based on the fact that modification maps present capital importance in recognizing the patterns and changes that are indicative of a steganography effect on the image's content alteration [31]. A step-by-step process to generate the modification maps is further detailed in Subsection 3. 2. Referring to the existing literature, as described in the previous Section, it has been identified that the utilization of CNNs in the steganalysis operations has become efficient and popular based on their capability to extract and learn the relevant features of images considered for steganalysis. CNNs play a significant role in enabling the discovery of patterns and alterations in pixel intensities that show any steganographic change. To improve the ability of the CNN to perform the steganalysis operations, we chose to use it in combination with other schemes, namely the modification maps calculation and fuzzy logic, to identify the fuzzy correlation maps, considered unique features of an image. A flow diagram of the proposed strategy is illustrated in Fig. 2.

Referring to the wide recognition of the neural networks in the final features generating task, cover images are trained in two main types of layers: the convolutional and the downsampling layers combined with other crucial elements of a neural network. The convolutional operation aims to model the correlation between a pixel and its neighboring. For example, if we set a kernel to size 3×3, the steganalysis features will be generated with 8 pixels surrounding it. Referring to the kernel size, which is usually constant in most payload location CNN, two challenges can happen. The first is that with a large convolutional kernel size, information may be redundant because of connecting many pixels, including some irrelevant pixels. The second is that a small kernel may also lose some vital information.

3.2. Modification maps generation

The properties of adaptive steganography algorithms proved the unchangeability of the pixels in a texture region, which means that the same pixel is not changed two times, hence the preservation of the distribution of the cover content. We depart from those properties to identify the most probable pixels using two successive data embedments, checking whether a re-embedding selects the same pixels again. We depart from a property that the cost matrix does not change between the first and second stego images. The following stages define our stages to obtain the modified maps.

(1) We conceal the random secret data in the cover C to obtain the first stego $ST1$.
(2) We re-embed the same secret data in $ST1$ to obtain the second stego $ST2$.
(3) Using Syndrome-Trellis Codes (STCs), we calculate the cost matrix referring to [14], which guides us in selecting the embeddable pixels to obtain $ST1$ and $ST2$.
(4) We define the modification maps Mod_{map} for a pixel at (i,j) referring to (1) as follows:

$$Mod_{map}(i,j) = \begin{cases} 255, foramodifiedpixelat(i,j) \\ 0, otherwise \end{cases} \quad (1)$$

It is worth noting that we compute for two modification maps as of Fig. 3 with Mod_{map1} obtained from a comparative analysis between the cover and $ST1$ and Mod_{map2} obtained from $ST1$ and $ST2$. It is also important to identify that two data concealments with an adaptive steganography algorithm choose pixels almost in the same region, known as a texture region. However, in a challenging case where an algorithm does not always modify the same pixels while there are neighboring pixels during two embedding operations, we proceed with fuzzy logic on the secondly obtained feature map to generate the fuzzy correlation maps.

3.3. Fuzzy correlation maps generation

From Mod_{map2} we calculate the fuzzy correlation map with four basic input variables: the covariance map, the compass mean, the distance vector matrix, and the pixel intensity matrix. The obtained fuzzy correlation map is set to a matrix of a dimension 256×256.

A. Covariance map

The covariance map reflects how variables in pairs alter with respect to each other. Covariance helps in data dependency model-

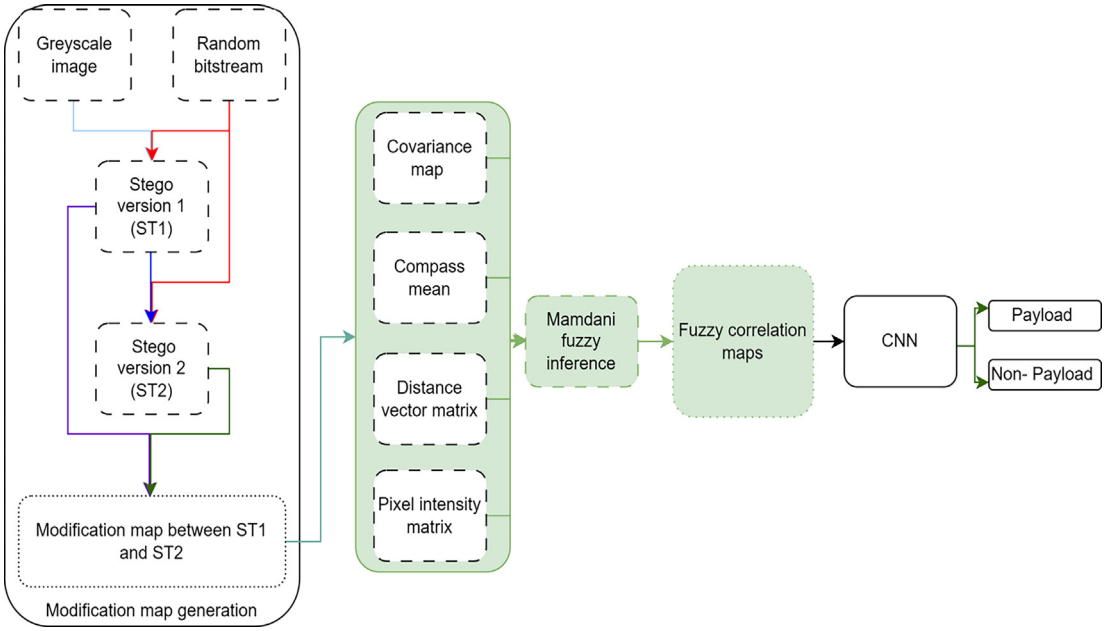


Fig. 2. Flow diagram of the proposed scheme.

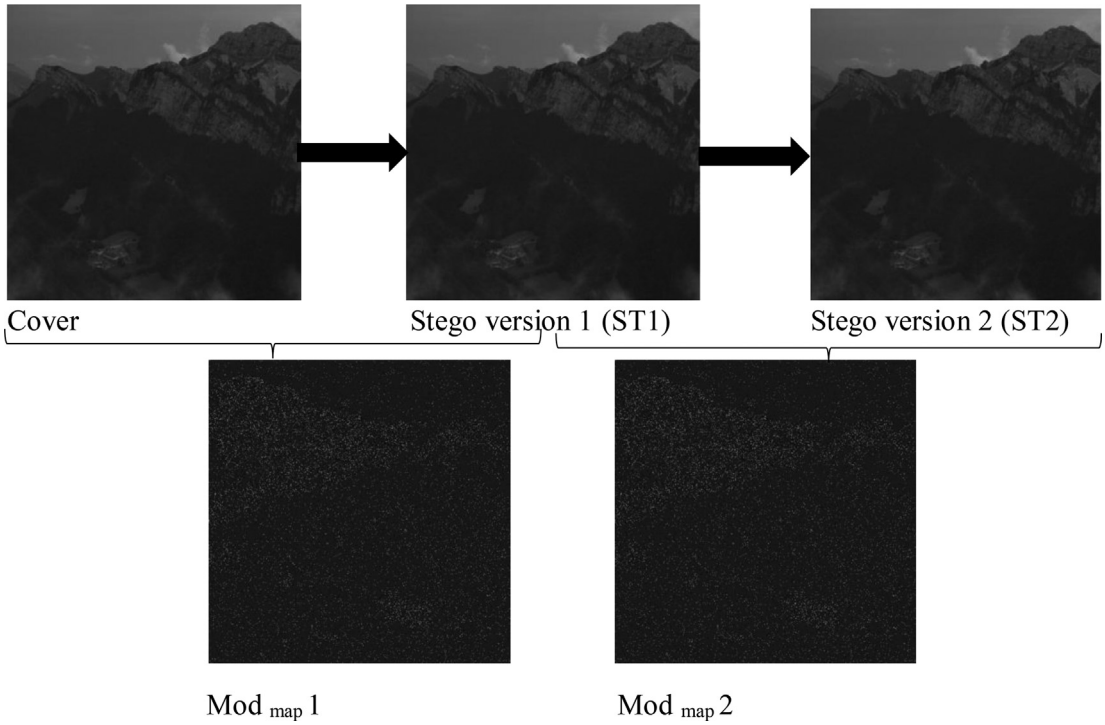


Fig. 3. Illustration of the modification maps generation for two successive S-UNIWARD steganographic algorithms with a payload of 0 4*bpp*.

ing irrespective of their physical meaning. In an image, the covariance is used to show the dependencies among the image's statistical data, such as pixel position and intensity, and how they relate to their derivatives. Based on their capital importance, the covariance maps are primarily used to integrate the gathered data into a deep learning framework [43]. Referring to [5], the covariance $cov(x,y)$ for two variables x and y, whose respective means μ_x and μ_y is got as of (2) using $\times$ a complex conjugate function.

$$cov(x,y) = \sum_{i=1}^{2} (x_i - \mu_x) \times (y_i - \mu_y) \tag{2}$$

B. Compass-mean operation

The compass-mean operation works as a map's top compass to make the operator sign or direct the pixels in its surroundings. It computes the correlation between the neighboring pixels and the pixel in the center to generate the mean intensities with fuzzy logic. The compass mean calculation does not involve the center pixel to differentiate the compass mean from the average mean filters. The compass-mean $C_{mean}(i,j)$ for a pixel $P(i,j)$, with $1 \leq i \leq 227$ and $1 \leq j \leq 227, i \neq j$, at the cartesian position (i,j) is given by (3).

$$C_{mean}(i,j) = \frac{1}{m \times n} \sum_{\substack{-1 \leq m \leq 1 \\ -1 \leq n \leq 1}} P(i,j) \tag{3}$$

C. Distance vector matrix

The distance vector matrix is a matrix of scalar values $DV(i,j)$ expressing the distance between a central pixel $P_0(i_0,j_0)$ and any pixel at the position (i,j) computed by (4).

$$DV(i,j) = \sqrt{(i-i_0)^2 + (j-j_0)^2} \tag{4}$$

D. Pixel intensity matrix

Departing from the modification map presented in a grayscale format because its pixels are set to values from 0 to 255 by (1). The distribution of the pixels modifying map shows the pixel intensity matrix, which is then used as a fuzzy input membership function. We obtain the fuzzy correlation maps using four membership functions: the covariance map, the compass mean, the distance vector matrix, and the pixel intensity matrix as input. Fig. 4 shows the designed Mamdani fuzzy inference system. It is worth noting that the fuzzy output matrix is a grayscale image showing how the total pixels' intensity energy is correlated. It is also important to note that Fig. 5 shows a sample of some of the eighty-one fuzzy rules set based on fuzzy variable sets as of Fig. 6, which illustrates the input membership functions, and Fig. 7, which shows the resulting output membership function.

3.4. Description of the proposed CNN

The proposed CNN has four main layers: regular convolutional layers, average pooling layers, fully connected, and normalization layers. The overall architecture of the proposed CNN is described in Table 1. In relation to the requirements and size of the input, in the first convolutional layer, we use filters of the size 11×11. The size of the input is $224 \times 224 \times 3$, but we set it to $256 \times 256 \times 3$ by padding with zeros. The convolutional operation is independently applied to the filter and the input image, creating a two-dimensional feature map for each operation. The objective of convolving the filter with the image is to enable the filter to identify unique features in the image. To

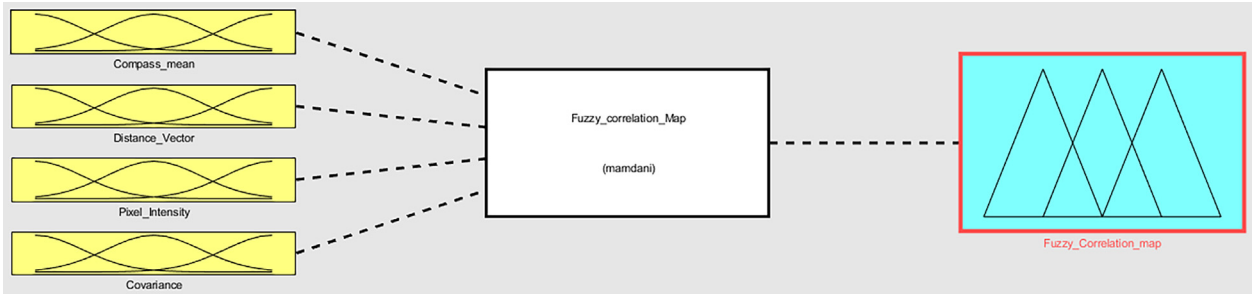


Fig. 4. The designed Mamdani fuzzy inference system.

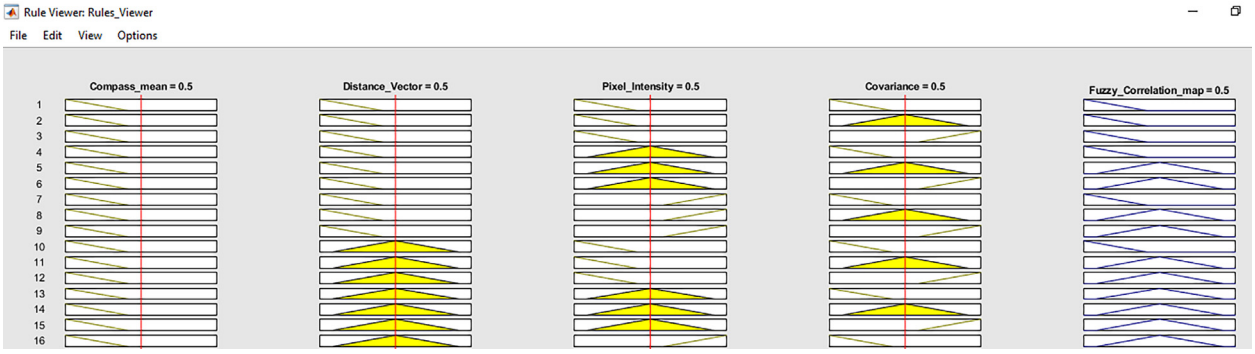


Fig. 5. Sample rules among eight-one designed rules in the rule viewer.

increase the nonlinearity, we use a rectified Linear Unit Layer (ReLU), which is expected to enhance the network's nonlinearity. ReLU-based network training proves to be faster than tanh or sigmoid activation functions.

The pooling layer shrinks the input image's size through downsampling for the pooling operations. It divides the image into non-overlapping rectangles for preprocessing. We use two different pooling operations: average pooling and maximum pooling. Average pooling plays a crucial role in CNNs by shrinking the size of the feature maps, thus lowering the required parameters and computations. This speeds up training and enhances the network's overall performance.

Additionally, average pooling strengthens the feature maps, curbs overfitting through its spatial invariance, and reduces sensitivity to minor shifts in the input image. Switching to average pooling from max pooling also increases the network's invariance to slight variations in image intensity. Maximum pooling selects the maximum value of each rectangle to represent the lesion region. By using maximum pooling, it is possible to achieve a dimensional reduction in the processed data.

The softmax function and the fully connected layer in our CNN collaborate to generate the final prediction. The fully connected layer takes the output from the preceding layer, maximum pooling layer feature maps, and multiplies them by a set of weights. This result goes through a ReLU to generate an intermediate output. The softmax function performs the final step in processing the fully connected layer's output. This mathematical operation transforms the intermediate result into a probability distribution across the output classes, namely innocent and changed pixels. The softmax function calculates the exponential of the intermediate result and normalizes it so that it adds up to 1. The resulting probability distribution shows the possibility of the input image's pixels belonging to each output class. The class with the highest probability becomes the network's final prediction.

3.5. Our approach to locating the suspicious pixels.

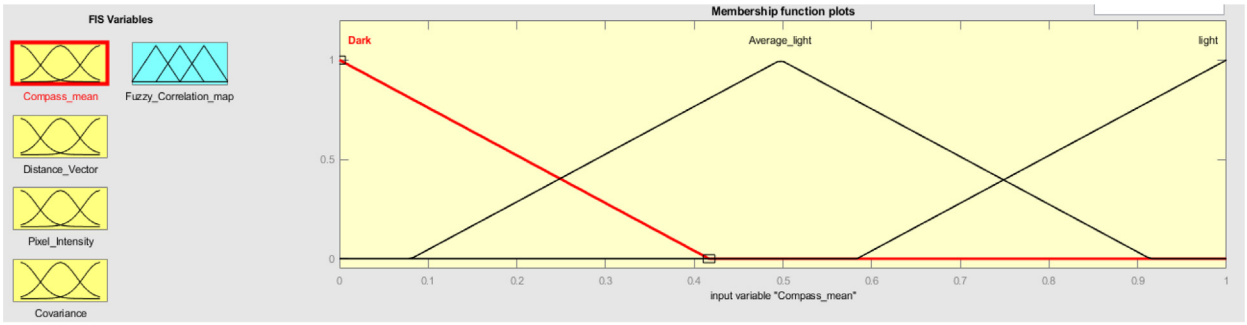
Our algorithm is designed to locate the pixels that likely hold the secret data added by adaptive steganography in the spatial domain. We have drawn inspiration from prior algorithms, and our algorithm performs best when the stego is confirmed. Our algorithm is designed for two scenarios.

1. In the first scenario, we assume that the steganographic payload is known, and we use the acquired payload to locate the modified pixels.
2. In the second scenario, we assume that the steganographic payload is unknown, and we use quantitative strategies to estimate the payload and locate the modified pixels.

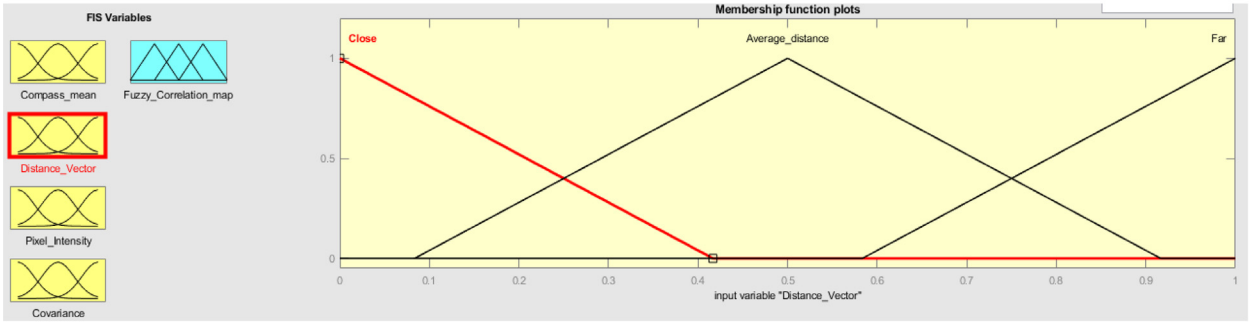
The following steps can generally describe our algorithm:

1. Step 1: Generate a random bit stream.
2. Step 2: Calculate the cost matrix of the cover image using the bank of designed filters based on an adaptive steganographic algorithm.
3. Step 3: Embed a message using STCs to obtain the first stego ST1 based on minimizing the distortion function using a cost matrix.
4. Step 4: Re-embed a message using STCs to obtain the second stego ST2 based on the principle of minimizing the distortion function using the cost matrix from step 2.
5. Step 5: Obtain the modification map between ST1 and ST2 as illustrated in Fig. 3.
6. Step 6: Calculate the correlation of neighboring pixels with the active pixel using fuzzy logic called the "fuzzy correlation maps" from the modification maps obtained in Step 5.

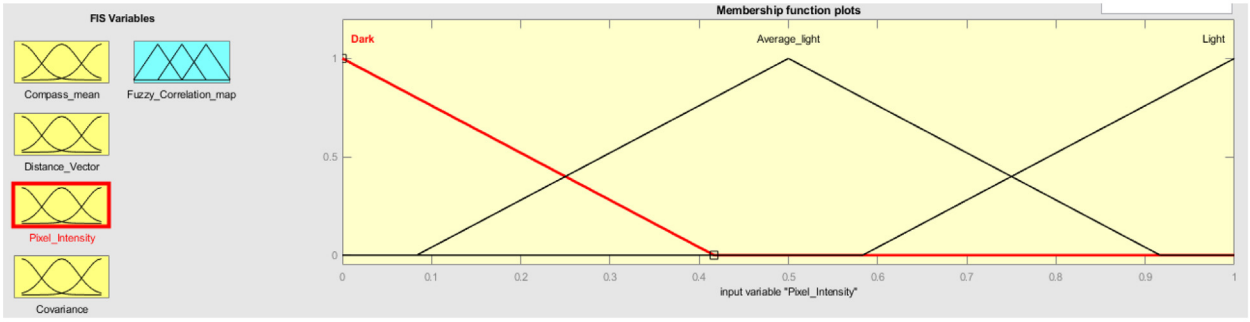
The fuzzy correlation maps are improved versions of the color correlogram, which calculates the color distribution of the altered pixels. The fuzzy correlation maps compute a feature vector of each modification map.



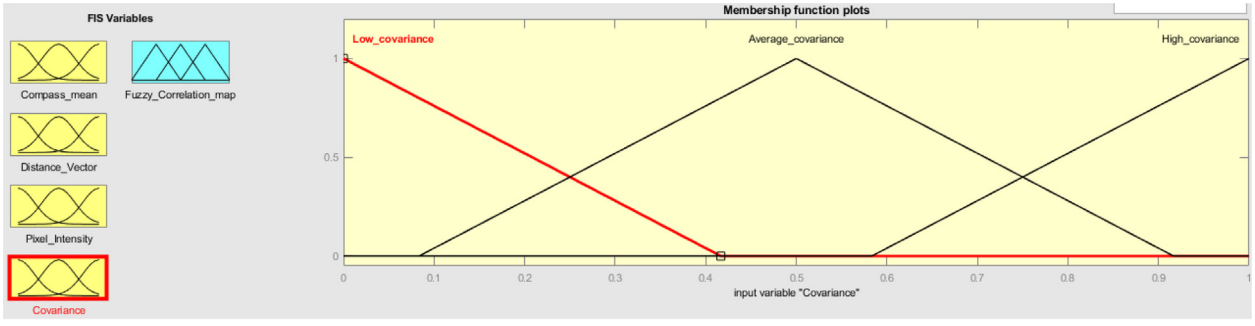
(a)



(b)



(c)



(d)

Fig. 6. Input membership function (a) Compass mean (b) Distance vector (c) Pixel intensity (d) Covariance.

7. Step 7: The fuzzy correlation maps obtained in step 6 are fed to the CNN network. Based on the logic that as each picture is unique, the correlation between the pixels creating the picture is also unique, we select fuzzy correlation maps which express the relationship between the pixels forming the stego image.

It is worth noting that with the fuzzy correlation maps as input to the proposed CNN, the output is the location of the pixels with

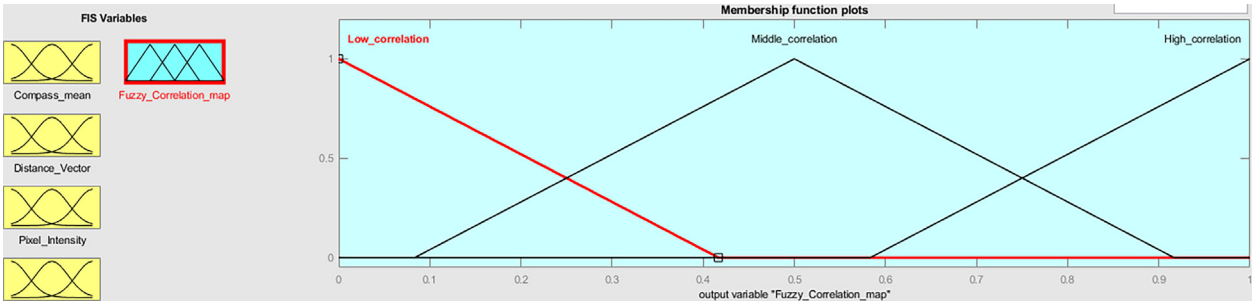


Fig. 7. Output membership function (fuzzy correlation maps).

Table 1
Architecture of the proposed cnn.

Layer	Input size	stride	Kernel size	Padding	Output Class
Convolution	256 × 256 × 1	4	11 × 11	0	96
Average pooling	55 × 55 × 96	2	3 × 3	0	96
Convolution	252 × 252 × 30	1	5 × 5	2	256
Average pooling	55 × 55 × 96	2	3 × 3	0	256
Convolution	2250 × 250 × 90	1	3 × 3	2	384
Convolution	248 × 248 × 30	1	3 × 3	2	384
Convolution	123 × 123 × 30	1	3 × 3	2	256
Convolution	119 × 119 × 32	1	3 × 3	2	256
Maximum pooling	55 × 55 × 96	2	3 × 3	0	256
Fully connected			1 × 1		4096
Fully connected			1 × 1		2
Softmax					2

confidential data, and the location algorithm we propose is summarized as follows:

Input: Fuzzy correlation maps of an inquiry image *F*, height (h) and width (w) of the probable location of altered pixels.

Output: Location of altered pixels (AltP)

1) **Initialize F with SRM weights;**
2) **# Iterate through the pixels in F and compute the locations with a probability of holding the secret data (probable AltP).**
3) **FOR i = 1, number-rows DO**
4) **FOR j = 1, number-column DO**
5) **Compute the alteration costs $A(x,y)$ using (Eq (1));**
6) **Let the probability as $\pi_\alpha(x,y) = f(A(x,y),\alpha)$ departing from (Eq(2));**
7) **Store $\pi_\alpha(x,y)$ in *M*;**
8) **Initialize the AltP to zero;**
9) **#Consider the location with a probability of holding the secret data with coordinates of size $h \times w$.**
10) **FOR i = 1, number-rows-w DO**
11) **FOR j = 1, number-column-h DO**
12) **Compute the sum of the probability with the upper side of the matrix of size $w \times h$ with the left corner of (i,j);**
13) **Extract the relevant information by performing statistical analysis on both the sums and their corresponding coordinates i,j;**
14) **Identify the maximum value of the sums as Max_s;**
15) **Identify the pixels making Max_s based on i and j as AltP;**
16) **Save AltP in PGM format;**

4. Experimental results

This article's primary contribution is locating the pixels altered by adaptive steganography by adding secret bits. We use fuzzy correlation maps obtained from modification maps of stego images to classify the inquiry image's pixels through a CNN. It is worth noting that our experiments to validate our strategy are conducted under two scenarios: the payload location with a known steganographic payload and the payload location with an unknown steganographic payload.

In this Section, we discuss the experimental setups and the considered performance evaluation metrics, obtained results and their discussion, cross-steganographic-algorithm validation results, and ablation study to identify the effectiveness of the components of our strategy and compare our results to the state-of-the-art methods' results.

Table 2
Experimental environment setting.

Dataset	BOSSBase1.01
Image Color, format, and size	Grayscale, uncompressed, and 512 × 512
Dataset cardinality	10000 images
Payload sizes in bits per pixel (bpp)	0.05, 0.1, 0.2, 0.3, 0.4, and 0.5
Steganographic algorithms	HILL, HUGO BD, S-UNIWARD, and WOW
Data embedding and modification maps detection framework	Syndrome Trellis Codes (STCs)
Fuzzy inference system (FIS)	Type='Mamdani' Version = 2.0 NumInputs = 4 NumOutputs = 1 NumRules = 81 AndMethod='min' OrMethod='max' ImpMethod='min' AggMethod='max' DefuzzMethod='centroid'
Payload locating scheme	Our Proposed method (Combining fuzzy and CNN)
Considered locating schemes for benchmark	[20,27,31]

4.1. Experimental setup and evaluation metrics

Table 2 presents detailed information regarding our study's experimental environment setups, including the dataset we utilized, the steganographic algorithms to embed the secret bits of data, fuzzy inference system parameters, and the prior algorithms used as benchmarks to the proposed method for payload locating.

The BOSSBase1.01 dataset [4], containing 10,000 grayscale images with an uncompressed size of 512×512pixels, has been utilized in this study. We use payload sizes ranging from 0.05 to 0.5*bpp*, and the steganographic algorithms we employ for secret data embedding are HILL, HUGO BD, S-UNIWARD, and WOW. We utilize the Syndrome Trellis Codes (STCs) framework for data embedding and modification map computation. Moreover, we employ a fuzzy inference system (FIS) of type 'Mamdani,' version 2.0. In our FIS, we use four input membership functions (MFs) and one output MF, with 81 rules connected based on the input MFs values with 'min' as the and-method, 'max' as the or-method, 'min' as the implication method, 'max' as the aggregation method, and 'centroid' as the defuzzification method. Our strategy to locate the steganographic payload applies a combination of fuzzy and CNN, which is compared and benchmarked to other steganalysis schemes to locate the payload as proposed by Hu et al. [20], Liu et al. [27], and Qiao et al. [31].

To thoroughly evaluate the performance of our payload location scheme, four metrics are considered, namely the Precision ($P_{(i)}$), Recall ($R_{(i)}$), F1-score ($F_{(i)}$), and the classification accuracy ($Acc.$). Our evaluation metrics are computed as of the following mathematical expressions and based on the interpretation of our results departing from the confusion matrix in Table 3. TP represents the number of altered pixels that were correctly classified as modified pixels, FP stands for the number of innocent pixels that were incorrectly classified as modified pixels, TN represents the number of innocent pixels that were correctly classified as innocent pixels, and FN represents the number of altered pixels that were incorrectly classified as innocent pixels.

(i) The $P_{(i)}$ is expressed as the ratio of accurately located pixels with confidential data to the total number of pixels in the inquiry image, which include positive and negative predictions. It is calculated as the division of the number of true positive samples TP, representing the pixels that hold the secret bits correctly located by the sum of TP and the false positive samples FP.

$$P_{(i)} = \frac{TP}{TP + FP} \tag{5}$$

(ii) The $R_{(i)}$ is calculated in (6) as the proportion of correctly located pixels TP out of the total number of samples considered as TP and the samples of innocent pixels that are classified as pixels holding the secret data FN.

$$R_{(i)} = \frac{TP}{TP + FN} \tag{6}$$

(iii) The F1-score $F_{(i)}$ takes precision and recall into account and is calculated using (7).

$$F_{(i)} = 2 \times \frac{P_{(i)} \times R_{(i)}}{P_{(i)} + R_{(i)}} \tag{7}$$

Table 3
Confusion matrix.

	Predicted Positive	Predicted Negative
Actual Positive	TP	FN
Actual Negative	FP	TN

(iv) The Acc is calculated using (8) considering the confusion matrix.

$$Acc = \frac{TP + TN}{TP + TN + FP + FN} \times 100\% \tag{8}$$

5. Results and discussion

The experimental results are arranged based on two scenarios: 1) localizing the hidden bits when the payload size is known, and 2) localization of the hidden bits when the payload size is unknown.

5.1. Payload location with known payload

In this Subsection, we first evaluate our method's performance in locating a steganographic payload when the payload size is known. We use 10,000 images from the BOSSBase 1.01 as a benchmark dataset described in Section 4.1 to generate the stego images using the four state-of-the-art adaptive steganographic methods: HILL, HUGO BD, S-UNIWARD, and WOW. With different cost matrices, we generate six random bitstreams with varying steganographic payloads, notably, 0.05*bpp*, 0.10*bpp*, 0.20*bpp*, 0.30*bpp*, 0.4*bpp*, and 0.5*bpp*. To conceal the secret bitstreams, and we use the syndrome trellis codes referring to [14]. After embedding the random bitstreams, we generate the modification maps from which we depart to generate the fuzzy correlation maps used for binary classification. To evaluate our method's performance, our results are computed based on three metrics: recall, precision, and F1-score.

Fig. 8 illustrates the achieved results in recall rate, which reflects the ability of our strategy to locate the steganographic payload when it is known to locate the existence of secret bits of data correctly. As given in (6), it is defined as the ratio of the true positive rate to the sum of true positive and false negative rates. Moreover, this metric demonstrates the proportion of actual steganographic payload accurately located through our strategy. module. It is worth noting that at the start, the recall rate for the four algorithms increases in the same range and improves based on the payload capacity increase. Based on the same Fig. 8, it is identified that the recall rate in HILL and WOW is higher than in other algorithms and that specifically, the recall rate with WOW reaches approximately 100% with a payload of 0.5*bpp*, which indicates that almost all modified pixels can be located.

Based on the trade-off between the recall rate and the precision, the basic considered metrics to evaluate the performance of our method, we illustrate in Fig. 9 the F1-score as a balancing metric to avoid any imbalance due to miss interpretation. The F1-score, which results from the harmonic mean of the recall and the precision rates, is an evaluation metric that combines both the recall and the precision rates to demonstrate the overall performance of our strategy. Specifically, Fig. 9 shows the performance of our method with HILL, HUGO BD, S-UNIWARD, and WOW under the steganographic payloads ranging from 0.05 to 0.5*bpp*. It is worth noting that this figure identifies that our method is better with WOW with a maximum value F1-score of around 0.4, and that WOW achieves the highest detectability and that S-UNIWARD shows the lowest detectability.

Moreover, the significance of our approach is identified by a comparative analysis of our results in terms of steganographic payload location accuracy, which refers to our strategy's ability to correctly locate the hidden payload when it is known. We calculate the accuracy as of (8) described in Section 4.1 as the ratio of the total number of correctly predicted locations (true positive and true negative) to the total number of all predicted locations of

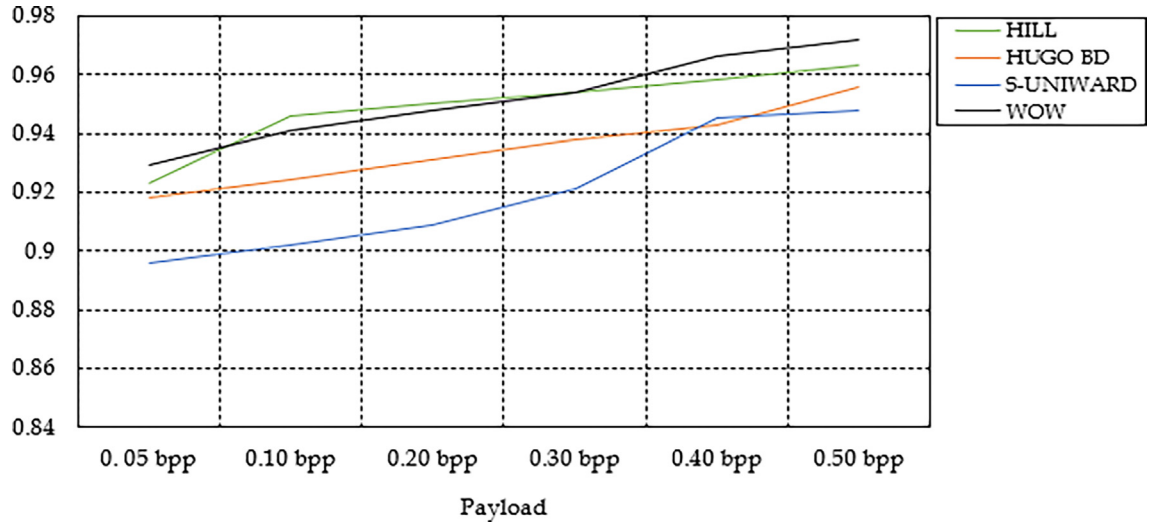


Fig. 8. Recall rate with different steganographic algorithms.

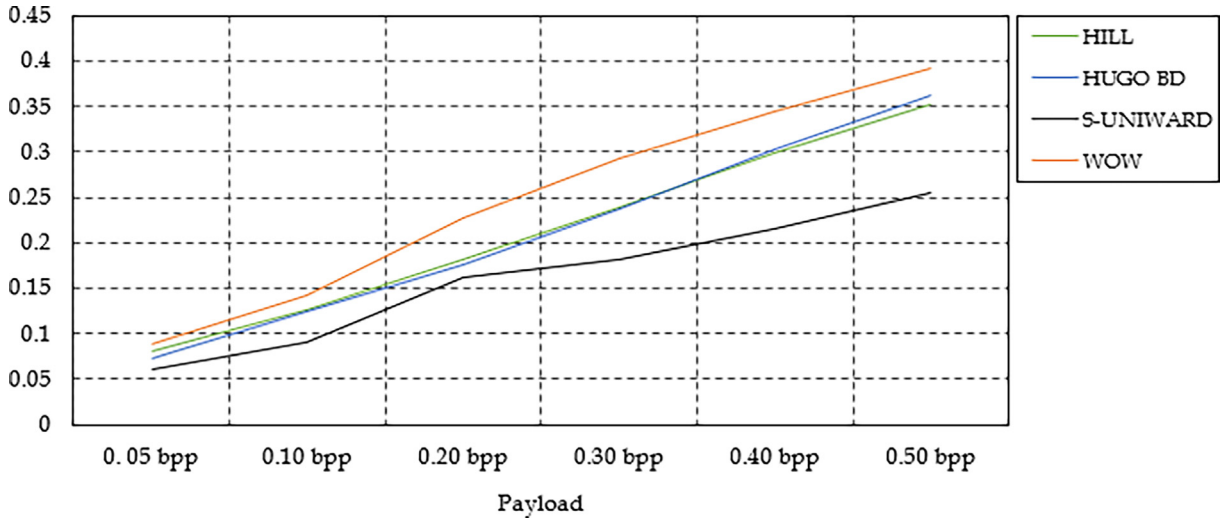


Fig. 9. F1-score comparison for the considered steganographic algorithms.

Table 4
Accuracy of our strategy to locate the steganographic payload when it is known.

Steganographic Algorithm	Payload capacity in ***bpp***					
	0.05	0.10	0.20	0.30	0.40	0.50
HILL	0.4992	0.5904	0.6704	0.7319	0.8506	0.9012
HUGO BD	0.4824	0.5692	0.6492	0.7184	0.8409	0.8978
S-UNIWARD	0.4688	0.5412	0.6288	0.6912	0.8301	0.8621
WOW	0.5093	0.6186	0.6998	0.7960	0.8719	0.9289

the steganographic data. Table 4 shows the accuracy for the four steganographic algorithms, namely HILL, HUGO BD, S-UNIWARD, and WOW, based on the payload capacity in bits per pixel at different levels of data hiding. The results show that our model to locate that hidden data under WOW with 0.50*bpp* yields the highest accuracy with a maximum of 92.89%. With HILL and HUGO BD, our model achieves slightly closer performances to locate all sizes of the steganographic payload, with HILL's hidden data location slightly outperforming that of HUGO BD based on the payload size. Accuracy to locate S-UNIWARD with our model has been identified to be the lowest among the four considered steganographic algorithms, with a maximum of 86.21%. Furthermore, our model reveals that increasing the payload capacity for any steganographic algorithm results in a corresponding increase in steganographic payload location accuracy, as expected.

5.2. Payload location with an unknown payload

In this scenario, we focus on locating the steganographically altered pixels when the payload is unknown. To show the effectiveness of our method in this scenario, we conceal a payload of 0.5*bpp* with HUGO BD and then refer to the second scenario, as

proposed by Liu et al. [27], to quantitatively estimate the steganographic payload. To show the performance of our model in locating unknown steganographic payload, we present the Receiver Operating Characteristic curve (ROC curve) of our model, which is a graphical illustration of the performance of our strategy to show the location of the steganographic payload. In our method, the ROC curve shows a graph of the true positive rate over the false positive rate for various decision thresholds. Our ROC curve plots the true positive rate (TPR) on the y-axis over the false positive rate (FPR) on the x-axis, with the classification threshold variation along the graph.

Fig. 10 shows the ROC test curves for our model to locate the pixels altered by adding the secret bits by HUGO with 0.4 *bpp* on BOSSBase 1.01. Based on the curve, it is recognized that our model yields a high true positive rate (TPR) with a reduced false positive rate (FPR), which means that the rate of the payload correctly located is higher than the rate of the ones incorrectly located. The area under the ROC curve (AUC), which demonstrates an overall summative performance of our proposed method to locate the steganographic payload, yielded with our strategy is 0.842. This scalar value which expresses the AUC,indicates the performance achieved with our strategy to locate the secret bits hidden by HUGO with a payload size of 0.4 *bpp*.

5.3. Ablation study

To assess the effectiveness of the proposed components for locating steganalysis payload, Table 5 compares the performance of different versions of the strategy, including and excluding the new components, namely the modification maps computation module and the fuzzy correlation maps computation module. For this ablation study, we consider S-UNIWARD and WOW, the two adaptive steganographic algorithms to embed the data in a cover image with various sizes of payloads, as generally used in the experimentation of our strategy.

Table 5 presents the accuracy of the proposed scheme to locate the hidden data where the accuracy in locating WOW is generally higher than that of locating S-UNIWARD at different payload capacities ranging from 0.05 to 0.50*bpp*. It is worth noting that the proposed strategy achieves better accuracy for both steganographic algorithms at all considered steganographic payload sizes compared to the versions without computing the modification maps and without the fuzzy correlation maps computation module. Moreover, it is identified that with the modification maps, the proposed strategy's accuracy remained relatively high for both steganographic schemes with all payload sizes. To demonstrate the contribution of the components of our strategy, it is crucial to note that without the fuzzy correlation maps, the accuracy of the proposed strategy decreased significantly for both S-UNIWARD and WOW algorithms with all steganographic payload sizes. Overall, it is identified that the results of our experiments demonstrate the effectiveness of the proposed components in improving the accuracy of the steganalysis strategy to locate a steganographic payload in digital images.

5.4. Cross-steganographic algorithm validation

We conduct a cross-steganographic algorithm validation to verify the proposed method's overall validity and the CNN's stability within the proposed algorithm. For our experiments in this concern, we depart from the results in the previous Subsection 4. 2 and consider two expected possibilities: 1) an accurately located steganographic payload and 2) an incorrectly predicted steganographic algorithm. In this Subsection, we also verify the efficiency of our method to detect adaptive steganographic algorithms, assuming them to be unknown. As stated in our experimental setting, we embed the data with four steganographic algorithms, HILL, HUGO BD, S-UNIWARD, and WOW. Using BOSSBase 1.01 images, we embed the data with a payload capacity of 0.3*bpp*.

In Table 6, we present the results showing that the proposed method performs better for HILL, HUGO-BD, and WOW steganographic algorithms, as the diagonal values for these algorithms represent the F1-scores when the true and predicted steganographic algorithms match, are the highest among the rows. However, for S-UNIWARD, the highest F1 score is achieved when the true steganographic algorithm is HILL.

Particularly, for the HILL steganographic algorithm, the highest F1-score is achieved when both the true and predicted algorithms

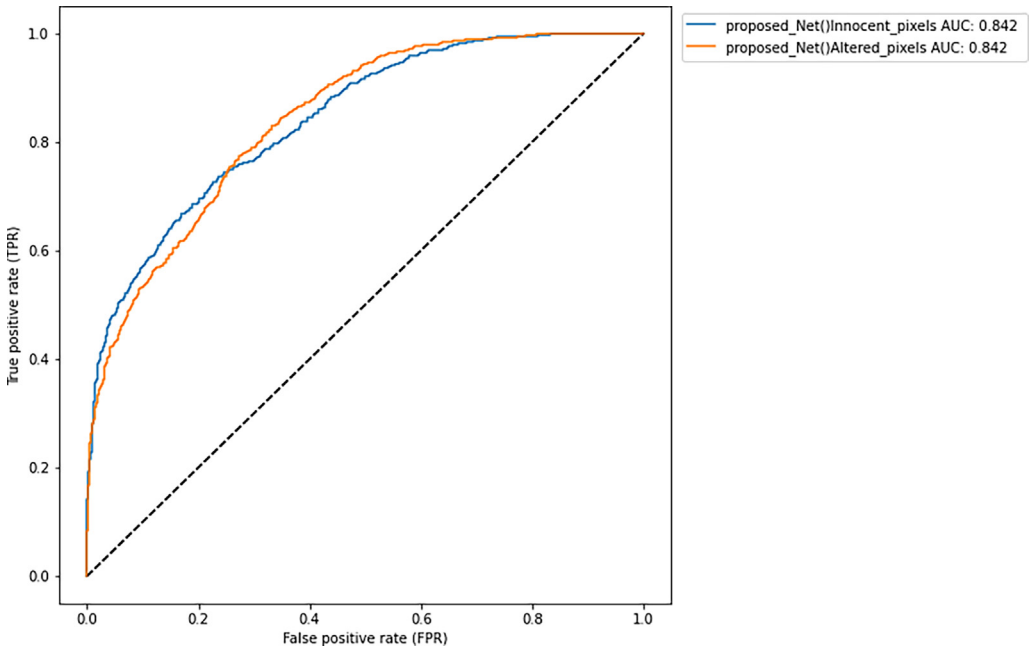


Fig. 10. ROC curves of our model under HUGO BD with payload capacity of 0.4 bpp.

Table 5
Accuracy with and without some components to identify their contributions to the strategy performance.

Architecture	Steganographic Algorithm	Payload capacity in ***bpp***					
		0.05	0.10	0.20	0.30	0.40	0.50
Proposed strategy	S-UNIWARD	0.4688	0.5412	0.6288	0.6912	0.8301	0.8621
	WOW	0.5093	0.6186	0.6998	0.7960	0.8719	0.9289
Proposed strategy without the modification maps	S-UNIWARD	0.4544	0.5299	0.6121	0.6793	0.8099	0.8507
	WOW	0.4998	0.6004	0.6802	0.7601	0.8602	0.9002
Proposed strategy without the fuzzy correlation maps	S-UNIWARD	0.3701	0.4486	0.5295	0.5961	0.7296	0.7666
	WOW	0.4479	0.5495	0.6291	0.7088	0.7798	0.8159

Table 6
F1 for the predicted and true steganographic algorithms with our method.

True steganographic algorithm	Predicted steganographic algorithm			
	HILL	HUGO-BD	S-UNIWARD	WOW
HILL	0.2980	0.2484	0.2198	0.2726
HUGO BD	0.2540	0.3102	0.2502	0.2921
S-UNIWARD	0.2302	0.2140	0.2022	0.2631
WOW	0.2698	0.2822	0.2493	0.3242

are HILL, with a score of 0.2980. For HUGO-BD, the highest F1-score is achieved when the predicted algorithm is HUGO-BD, and the true algorithm is also HUGO-BD, with a score of 0.3102. For S-UNIWARD, the highest F1 score is achieved when the true algorithm is HILL, and the predicted algorithm is S-UNIWARD, with a score of 0.2198. Finally, the highest F1 score for WOW is achieved when the true and predicted algorithms are WOW, with a score of 0.3242.

In fact, the proposed method performs better for most steganographic algorithms, and the highest F1 scores are achieved when the true and predicted algorithms match. However, for S-UNIWARD, the results show that the best performance is achieved when the true algorithm is HILL, which may suggest limitations of the proposed method for this particular steganographic algorithm.

5.5. Results comparison with the state-of-the-art methods

To demonstrate the effectiveness of our method, some state-of-the-art techniques are compared to the results of our approach. Table 7 and Table 8 compare the F1-score of the proposed method with the existing techniques for two payload capacities: 0.3 bpp and 0.5 bpp, respectively.

In Table 7, the proposed method outperforms the current techniques for HILL with an F1-score of 0.2898. At the same time, for S-UNIWARD and WOW steganographic algorithms, the proposed method also performs better than the existing methods reported by Hu et al. [20], Liu et al. [27], and Qiao et al. [31] with an F1-score of 0.2001 and 0.3198, respectively, which show a slight improvement compared to the results with HILL. It is worth noting that the previous algorithms did give the results under HUGO BD with the payload capacity of 0.3*bpp*, which was worked on in our experiments and achieved an F1-score of 0.2902.

Similarly, in Table 8, the proposed method outperforms the existing techniques for all four steganographic algorithms, notably HILL, HUGO-BD, S-UNIWARD, and WOW, with F1-scores of 0.3502, 0.3212, 0.2621, and 0.3796, respectively. For HUGO BD with a payload capacity of 0.5*bpp*, we compare our results to the results of Liu et al. [27], who have only worked on it.

To identify the effectiveness of the proposed strategy, our results in Table 7 show the F1-scores achieved with the existing methods [20,27,31] ranging from 0.1059 to 0.3076. These results are generally inferior to those achieved with the proposed algorithms that range from 0.1265 to 0.3198, based on the adaptive steganography algorithm used to embed the data. It is worth not-

Table 7
F1-score comparison between the proposed method and the existing method with payload capacity of 0.3*bpp*.

Locating Algorithm	Steganographic Algorithm			
	HILL	HUGO BD	S-UNIWARD	WOW
[20]	0.1265	–	0.1059	0.1249
[27]	0.2770	–	0.1918	0.3076
[31]	0.2812	–	0.1983	0.3184
Proposed	0.2898	0.2902	0.2001	0.3198

Table 8
F1-score comparison between the proposed method and the existing method with payload capacity of 0.5*bpp*.

Locating Algorithm	Steganographic Algorithm			
	HILL	HUGO BD	S-UNIWARD	WOW
[20]	0.1953	–	0.1672	0.1937
[27]	0.3471	0.2989	0.2554	0.3725
[31]	0.3487	–	0.2587	0.3753
Proposed	0.3502	0.3212	0.2621	0.3796

ing that the results of the strategy proposed in this study show a significant outperformance over the considered existing methods for the HILL and WOW algorithms and show a slight superiority over the existing methods for the S-UNIWARD. The best improvement of the F1-score achieved with the proposed method over the existing methods is 0.2829 for the prediction of HILL.

Moreover, Table 8 presents the F1-scores, which show that the algorithms [20,27,31] achieve F1-scores with a minimum of 0.1672 and a maximum of 0.3725 while the F1-score of the proposed algorithm ranges between 0.2621 and 0.3796. Based on these results, the proposed method achieves the highest F1-score of 0.3796 when used to locate steganographic payloads hidden with the WOW algorithm, indicating a significant performance over all existing algorithms when used with the same steganographic algorithm. Overall, the table shows that the proposed algorithm is generally effective in locating steganographic payloads, outperforming all the existing methods in F1-score across the four adaptive steganographic algorithms and payload capacities tested.

6. Conclusion

In this study, the proposed steganalysis scheme involves using image modification maps generated by an adaptive steganographic method to create fuzzy correlation maps that can be used to locate modified pixels in an image. The study uses STC to generate modification maps by re-embedding a random message, and those maps are crucial features to obtain the best fuzzy correlation maps of an image. The experimental results show outperformance over the recently proposed algorithms for two considered scenarios (payload location with known payload and payload location with unknown payload). Our strategy has proved effective for detecting hidden bits produced by adaptive steganography in the spatial domain. The implications of this study are that it offers a potential solution for detecting adaptive steganography, which can be particularly challenging due to its difficult ability to modify image pixels. This method can help improve the accuracy of steganalysis by using modification maps and fuzzy correlation maps to locate the modified pixels. However, the dependency of the effectiveness on the quality of the modification map generated by the steganographic method may be a limitation to our strategy because the performance can be affected by the types of accuracy in modification map generation.

Future research could focus on applying this method for detecting steganography in the frequency domain, which could further improve the accuracy of steganalysis in the JPEG domain. Additionally, the proposed method could be extended to detect steganography in other media types, such as audio and video files.

Funding

This research was supported by the Ministry of Education, Culture, Research and Technology, The Republic of Indonesia, and Institut Teknologi Sepuluh Nopember.

All authors read and approved the final manuscript.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Abboud R, Tekli J. Integration of nonparametric fuzzy classification with an evolutionary-developmental framework to perform music sentiment-based analysis and composition. Soft Comput 2020;24(13):9875–925. doi: https://doi.org/10.1007/s00500-019-04503-4.

[2] Ahmad T, Fatman AN. Improving the performance of histogram-based data hiding method in the video environment. J King Saud Univ – Comput Inform Sci 2022;34(4):1362–72. doi: https://doi.org/10.1016/j.jksuci.2020.04.013.

[3] Arivazhagan S, Amrutha E, Jebarani WSL. Universal steganalysis of spatial content-independent and content-adaptive steganographic algorithms using normalized feature derived from empirical mode decomposed components. Signal Process Image Commun 2022;101. doi: https://doi.org/10.1016/j.image.2021.116567. 116567.

[4] Bas, P., Filler, T., & Pevný, T. (2011). "*Break Our Steganographic System*": *The Ins and Outs of Organizing BOSS* (pp. 59–70). https://doi.org/10.1007/978-3-642-24178-9_5.

[5] Chen Mo, Boroumand M, Fridrich J. Deep learning regressors for quantitative steganalysis. IS and T International Symposium on Electronic Imaging Science and Technology, 2018. https://doi.org/10.2352/ISSN.2470-1173.2018.07.MWSF-160.

[6] De La Croix NJ, Ahmad T. Toward hidden data detection via local features optimization in spatial domain images. In: 2023 Conference on Information Communications Technology and Society (ICTAS). p. 1–6. 10.1109/ICTAS56421.2023.10082736.

[7] De La Croix NJ, Didacienne M, Louis S. Fuzzy logic-based shiitake mushroom farm control for harvest enhancement. In: 2022 10th International Symposium on Digital Forensics and Security (ISDFS). p. 1–6. https://doi.org/10.1109/ISDFS55398.2022.9800832.

[8] De La Croix NJ, Didacienne M, Louis S, Philander JT, Ahmad T. Internet of things based controlled environment for the production of shiitake mushroom. In: IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS). p. 1–6. 10.1109/ICBDS53701.2022.9936039.

[9] De La Croix NJ, Islamy CC, Ahmad T. Secret message protection using fuzzy logic and difference expansion in digital images. Proceedings of the 2022 IEEE Nigeria 4th International Conference on Disruptive Technologies for Sustainable Development, NIGERCON 2022, 2022. https://doi.org/10.1109/NIGERCON54645.2022.9803151.

[10] De La Croix, N. J., Islamy, C. C., & Ahmad, T. (2022). Reversible Data Hiding using Pixel-Value-Ordering and Difference Expansion in Digital Images. *2022 IEEE International Conference on Communication, Networks and Satellite (COMNETSAT)*, 33–38. https://doi.org/10.1109/COMNETSAT56033.2022.9994516.

[11] Denemark T, Boroumand M, Fridrich J. Steganalysis features for content-adaptive JPEG steganography. IEEE TransInformForensic Secur 2016;11(8):1736–46.

[12] Deveci M, Pamucar D, Gokasar I, Koppen M, Gupta BB. Personal mobility in metaverse with autonomous vehicles using Q-rung orthopair fuzzy sets based OPA-RAFSI Model. IEEE Trans Intell Transp Syst 2022. doi: https://doi.org/10.1109/TITS.2022.3186294.

[13] Filler T, Fridrich J. Gibbs construction in steganography. IEEE Trans Inf Forensics Secur 2010;5(4):705–20. doi: https://doi.org/10.1109/TIFS.2010.2077629.

[14] Filler T, Judas J, Fridrich J. Minimizing additive distortion in steganography using syndrome-trellis codes. IEEE Trans Inf Forensics Secur 2011;6(3):920–35. doi: https://doi.org/10.1109/TIFS.2011.2134094.

[15] Gao D, Wang GG, Pedrycz W. Solving fuzzy job-shop scheduling problem using de algorithm improved by a selection mechanism. IEEE Trans Fuzzy Syst 2020;28(12):3265–75. doi: https://doi.org/10.1109/TFUZZ.2020.3003506.

[16] Guo L, Ni J, Su W, Tang C, Shi Y-Q. Using statistical image model for JPEG steganography: uniform embedding revisited. IEEE Trans Inf Forensics Secur 2015;10(12):2669–80. doi: https://doi.org/10.1109/TIFS.2015.2473815.

[17] Holub V, Fridrich J. Designing steganographic distortion using directional filters. In: 2012 IEEE International Workshop on Information Forensics and Security (WIFS). p. 234–9. doi: https://doi.org/10.1109/WIFS.2012.6412655.

[18] Holub V, Fridrich J, Denemark T. Universal distortion function for steganography in an arbitrary domain. EURASIP J Inform Secur 2014. , http://jis.eurasipjournals.com/content/2014/1/1.

[19] Hossen, Md. S., Ahmad, T., & Croix, N. J. D. La. (2023). Data Hiding Scheme using Difference Expansion and Modulus Function. *2023 2nd International Conference for Innovation in Technology (INOCON)*, 1–6. https://doi.org/10.1109/INOCON57975.2023.10100991.

[20] Hu D, Shen Q, Zhou S, Liu X, Fan Y, Wang L. Adaptive steganalysis based on selection region and combined convolutional neural networks. Security Commun Networks 2017;2017:1–9.

[21] Karampidis K, Kavallieratou E, Papadourakis G. A review of image steganalysis techniques for digital forensics. J Inform Secur Appl 2018;40:217–35. doi: https://doi.org/10.1016/j.jisa.2018.04.005.

[22] Ker, A. D. (2008). Locating steganographic payload via ws residuals. *Proceedings of the 10th ACM Workshop on Multimedia and Security*, 27–32. https://doi.org/10.1145/1411328.1411335.

[23] Ker, A. D., & Lubenko, I. (n.d.). *Feature Reduction and Payload Location with WAM Steganalysis*.

[24] Li B, Wang M, Huang J, Li X. A new cost function for spatial image steganography. In: 2014 IEEE International Conference on Image Processing (ICIP). p. 4206–10. doi: https://doi.org/10.1109/ICIP.2014.7025854.

[25] Li M, Wang GG, Yu H. Sorting-based discrete artificial bee colony algorithm for solving fuzzy hybrid flow shop green scheduling problem. Mathematics 2021;9(18). doi: https://doi.org/10.3390/math9182250.

[26] Guo L, Ni J, Shi YQ. Uniform Embedding for Efficient JPEG Steganography. IEEE Trans Inf Forensics Secur 2014;9(5):814–25. doi: https://doi.org/10.1109/TIFS.2014.2312817.
[27] Liu Q, Qiao T, Xu M, Zheng N. Fuzzy Localization of Steganographic Flipped Bits via Modification Map. IEEE Access 2019;7:74157–67. doi: https://doi.org/10.1109/ACCESS.2019.2920304.
[28] Ntivuguruzwa, J.D.L. C. (2021). Fuzzy inference-based prediction model for an IoT based water and pasture localization for pastoralists. In *International Journal of Research in Engineering and Applied Sciences (IJREAS)euroasiapub.org* (Vol. 11).
[29] Pevný T, Fridrich J, Ker AD. From blind to quantitative steganalysis. IEEE Trans Inf Forensics Secur 2012;7(2):445–54. doi: https://doi.org/10.1109/TIFS.2011.2175918.
[30] Prayogi, I. B., Ahmad, T., De La Croix, N. J., & Maniriho, P. (2021). Hiding Messages in Audio using Modulus Operation and Simple Partition. *Proceedings of 2021 13th International Conference on Information and Communication Technology and System, ICTS 2021*, 51–55. https://doi.org/10.1109/ICTS52701.2021.9609028.
[31] Qiao T, Luo X, Pan B, Chen Y, Wu X, Chen B. Toward steganographic payload location via neighboring weight algorithm. Secur Commun Networks 2022;2022:1–17.
[32] Quach T-T. Cover estimation and payload location using Markov random fields. Media Watermark Secur Forensics 2014;2014(9028):90280H. doi: https://doi.org/10.1117/12.2032711.
[33] Reinel TS, Brayan AAH, Alejandro BOM, Alejandro MR, Daniel AG, Alejandro AGJ, et al. GBRAS-Net: A convolutional neural network architecture for spatial image steganalysis. IEEE Access 2021;9:14340–50. doi: https://doi.org/10.1109/ACCESS.2021.3052494.
[34] Salloum G, Tekli J. Automated and personalized nutrition health assessment, recommendation, and progress evaluation using fuzzy reasoning. Int J Hum Comput Stud 2021;151:102610.
[35] Tabares-Soto R, Arteaga-Arteaga HB, Mora-Rubio A, Bravo-Ortíz MA, Arias-Garzón D, Alzate-Grisales JA, et al. Sensitivity of deep learning applied to spatial image steganalysis. PeerJ Comput Sci 2021;7:1–27. doi: https://doi.org/10.7717/peerj-cs.616.
[36] Veena ST, Arivazhagan S. Quantitative steganalysis of spatial LSB based stego images using reduced instances and features. Pattern Recogn Lett 2018;105:39–49. doi: https://doi.org/10.1016/j.patrec.2017.08.016.
[37] Wang GG, Gao D, Pedrycz W. Solving Multiobjective Fuzzy Job-Shop Scheduling Problem by a Hybrid Adaptive Differential Evolution Algorithm. IEEE Trans Ind Inf 2022;18(12):8519–28. doi: https://doi.org/10.1109/TII.2022.3165636.
[38] Wang J, Yang C, Zhu M, Song X, Liu Y, Lian Y. JPEG image steganography payload location based on optimal estimation of cover co-frequency sub-image. Eurasip Journal on Image and Video Processing 2021;2021(1). doi: https://doi.org/10.1186/s13640-020-00542-2.
[39] Xu G, Wu HZ, Shi YQ. Structural design of convolutional neural networks for steganalysis. IEEE Signal Process Lett 2016;23(5):708–12. doi: https://doi.org/10.1109/LSP.2016.2548421.
[40] Yalcinkaya F, Erbas A. Convolutional neural network and fuzzy logic-based hybrid melanoma diagnosis system. Elektronika Ir Elektrotechnika 2021;27(2):69–77. doi: https://doi.org/10.5755/j02.eie.28843.
[41] Yang C, Liu F, Ge S, Lu J, Huang J. Locating secret messages based on quantitative steganalysis. Math Biosci Eng 2019;16(5):4908–22. doi: https://doi.org/10.3934/mbe.2019247.
[42] Yang C, Luo X, Lu J, Liu F. Extracting hidden messages of MLSB steganography based on optimal stego subset. Science China Information Sciences. Science in China Press; 2018. Vol. 61, Issue 11. https://doi.org/10.1007/s11432-017-9328-2.
[43] Yang H, He H, Zhang W, Cao X. FedSteg: A federated transfer learning framework for secure image steganalysis. IEEE Trans Network Sci Eng 2021;8(2):1084–94. doi: https://doi.org/10.1109/TNSE.2020.2996612.
[44] Ye J, Ni J, Yi Y. Deep Learning Hierarchical Representations for Image Steganalysis. IEEE Trans Inf Forensics Secur 2017;12(11):2545–57. doi: https://doi.org/10.1109/TIFS.2017.2710946.
[45] Yedroudj, M., Comby, F., & Chaumont, M. (2018). *Yedrouj-Net: An efficient CNN for spatial steganalysis*. http://arxiv.org/abs/1803.00407.
[46] Zakaria, A., Chaumont, M., & Subsol, G. (2018). *Quantitative and Binary Steganalysis in JPEG: A Comparative Study*.
[47] Zhang R, Zhu F, Liu J, Liu G. Depth-wise separable convolutions and multi-level pooling for an efficient spatial CNN-based steganalysis. IEEE Trans Inf Forensics Secur 2020;15:1138–50. doi: https://doi.org/10.1109/TIFS.2019.2936913.

Ntivuguruzwa Jean De La Croix received a B.Sc. degree in computer science and systems from the National University of Rwanda, Rwanda, in 2013, a master's degree in information technology from the University of Madras, India, in 2016, a post-graduate diploma in education from University of Kigali, Rwanda in 2018, a master's degree in internet of things-embedded computing systems from the University of Rwanda, Rwanda in 2020, and he is currently pursuing a Ph.D. degree in computer science in Institut Teknologi Sepuluh Nopember (ITS), Indonesia. He has published several conference papers and journal articles on data hiding and the internet of things. He served as a teaching staff in the Christian University of Rwanda since 2019 and moved to the University of Rwanda in 2021. His current research interests include steganography, steganalysis, and deep learning for data security in the public network.

Tohari Ahmad received the Bachelor degree in computer science from Institut Teknologi Sepuluh Nopember (ITS), Indonesia, the master degree in information technology from Monash University, Australia, and the Ph.D degree in computer science from RMIT University, Australia. He was a consultant for some international companies. In 2003, he moved to ITS, where he is now a professor. His research interests include network security, information security, data hiding and computer network. He is a reviewer of a number of journals. Prof. Ahmad's awards and honors include the Hitachi Research Fellowship, and JICA Research Program to conduct research in Japan. His research is available at https://www.scopus.com/authid/detail.uri?authorId=35241970700.