Multimedia Tools and Applications (2023) 82:7529–7552
https://doi.org/10.1007/s11042-022-13677-3

Development of secrete images in image transferring system

Hemanta Kumar Bhuyan[1] · A. Vijayaraj[1] · Vinayakumar Ravi[2]

Received: 19 June 2021 / Revised: 6 March 2022 / Accepted: 11 August 2022 /
Published online: 24 August 2022

Abstract

This paper addresses a model to secrete the information of one image under another without losing quality of image. Different approaches have been utilized for image hiding as needed, but multiple images maintain secrecy with information under another image is a challenging task. Thus, the framework is proposed to sustain the secrecy of an original image from another image. The proposed system collects random images through ImageNet and uses them as per the requirements of secrete images. The framework is used the deep neural networks method to build secrete information of multiple images under a single image. The enormous transfer of images is used to select standard image modifications using advanced deep learning approaches. It develops the significance of the critical framework that alleviates the choice of finding the hidden image information. Two vital methods such as Peak Signal to Noise Ratio (PSNR) and the Structural Similarity Index (SSIM) are used to find out difference between host and secret image by their corresponding evaluation scores. It produces the confidentiality of the image with the help of the host image. Therefore, data from several images are protected under a single image. The different image data are experimented with good performance. For comparative analysis, the accuracy is better in retrieving two secrete images on all experiments, like approximate accuracy is 100%. Still, when we considered PSNR and SSIM scores on the same two secrete images, accuracy became less than 50%.

Keywords Information hiding · Image verification · Steganography · Hiding images · Image trust

✉ Vinayakumar Ravi
vravi@pmu.edu.sa

Hemanta Kumar Bhuyan
hmb.bhuyan@gmail.com

A. Vijayaraj
satturvijay@gmail.com

[1] Department of Information Technology, Vignan's Foundation for Science, Technology & Research (Deemed to be University), Guntur, Andhra Pradesh, India

[2] Center for Artificial Intelligence, Prince Mohammad Bin Fahd University, Khobar 34754, Saudi Arabia

Notations explanations DID-ANetDefocus Picture Deblurring Auxiliary Learning Net.
LSBLeast significant bits.
FMDFeature Map Distillation.
FDDFeature Decoder Distillation.
FMCFeature Map Consistency-enforcement.
DNNDeep neural networks.
GANGenerative-adversarial-networks.
CNNConvolutional neural network.
OOriginal Secrete Image.
HHost image.
O′Receiver Secrete Image.
H′Receiver Host image.
||H-H′||Error in Host image.
||O-O′||Error in original image.
αWeight Parameter to adjust error.
minMinimum.
RGBRed, Green, Blue.
PSNRPeak Signal to Noise Ratio.

1 Introduction

In immoral practices, confidential data have been maintained for the public with a secret strategy by concealing messages in images. The existing approaches involved with learning techniques for an inverse mapping on a cycle-consistency requirement to monitor the image processing. It is not possible to learn the inverse mapping for all domains, because it introduces additional trainable parameters. Consequently, they are useless in situations involving multiple visual picture domains, texture alterations, or semantic consistency preservation [50]. Sometimes defocus blur as opposed to object motion blur which is brought by the depth of field limitations of cameras. The parameter of the point spread function can be used to determine the amount of defocus, resulting in a defocus map [37]. The Defocus Picture Deblurring Auxiliary Learning Net (DID-ANet) had developed for new network architecture intended exclusively for deblurring a single image with the help of mapping evaluation.

Several meta-information of images, such as pixel information, colour quality, the boundary of image, image sequence, etc., can be maintained without modifying any appearance in each image. Different methods are used to monitor or find out replica images available on fake sites or social media. The subtle variations can be simply seen by investigating the symbols' reform on secrete imperceptible indications for the whole image. It is the entire exclusive of cooperation the visual integrity of the observed image [26].

In above cases, secrete information of different images does not apply steganography techniques on single image with single location. Thus, it is challenging task to maintain the secret information with high-quality sequence confidentiality because the statistical quality of the image can change the image information by setting it in a post. The gap of approaches is involved in few research works such as the hidden ability determination of grayscale images is alluded in [36], the secrete techniques affect the least significant bits (LSB) of images [19], the image model's dimensionality is performed for steganography, either matching models [46] or deep learning [51].

From the above steganography approaches, we found the limitations from existing approaches as follows:

(a) There are few differences in [28] on secret image information, such as secret information is not required for encoding to match the reformation of secret images.
(b) Fewer image variations can lead to a significant error in secret images.
(c) The quantity of information for secrecy maintains a 1:1 ratio between secrecy and host information.

Thus, we proposed a model to maintain secret information of different images under a single image to avoid the above limitations. Thus, the proposed work aims to create a distinguished container network to preserve a hidden image under another image using DNN techniques.

As per DNN techniques, the model is considered for sharing information from original images to modified images in this paper. In this model, local modification of the original image provides a local modification of the secrete image. It creates the confidentiality of image information for the secrete post. Thus, it makes obscure the information of the secrete message. Further, we try to encode the image based on some BPP (bits per pixel) as per the required image. Our proposed work and steganography are most significant during the processing of image. Due to the amount of secret information, there is no certainty of secret image for concealed image detection. Yet, in the proposed solution, the techniques of steganography are used.

In Fig. 1, multiple images are concealed in a host image-based container, and the original image is retrieved from the corresponding host image. It is a secret system of images where the container retains both the original and the host image. The original images are considered as secret images in the container under the host image. The original image is hidden under the host image so that only the host image faces outward. Few authors have also used encoded additional image transmission information in [17]. For example, colour information is concealed in the same image. But in our proposed model holds full images secret. Based on deep learning techniques, the secret information is extracted by the receiver from the color images. The quantity of modification is elaborated based on the quantity of secrete information and maintained secrecy in a smaller number of bits. In contrast, it distorts the image. On the image itself, the amount of search adjustment is taken into account. Based on the secrecy of details, the smooth regions of the image can be preserved by strident with high frequency, which is hard to identify the origin of the image. The steganography and dimensionality approaches are considered for better analysis before developing our proposed model. Although we analyse several aspects of the secret image information model with different components and approaches in different sections of this paper, still we explained the major contributions of this proposed model as follows

(a) We designed the model where multiple images are concealed in a host image-based container
(b) We developed a transferring image system through three components: secret image preparation, secret image under host, and uncovered secret image under Divulge network.
(c) We designed Transferring images by grounding networks.
(d) We designed a solitary network based on Grounding Network, Concealed Network, and Divulge Network. Designed the structure of the image for three parts of Networks.

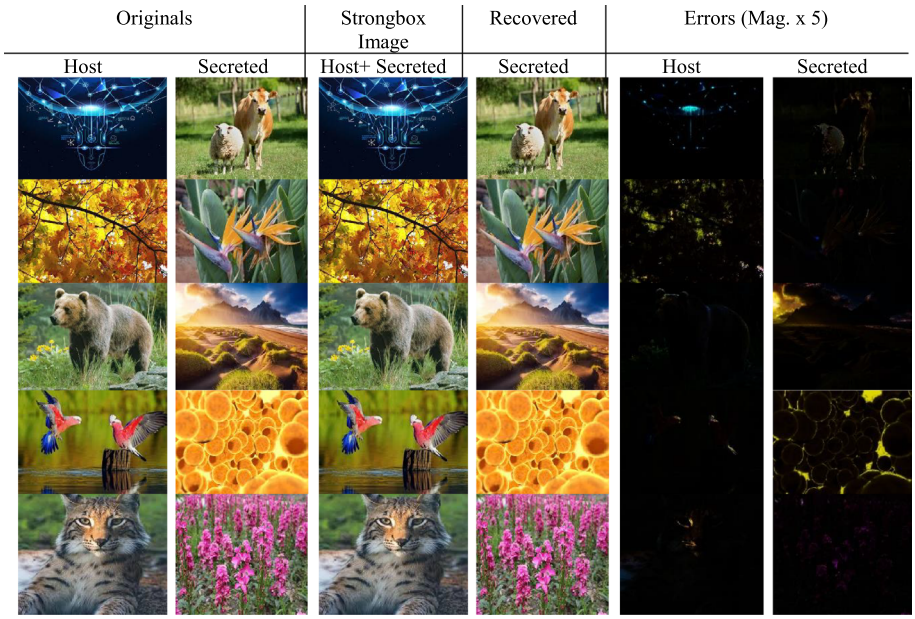


Fig. 1 Secret the original image through the container

(e) Positive and negative test images through the trained networks by making three kinds of images (Host, secrete, strongbox)
(f) The experimental performance is developed using the proposed model.
(g) We also used 2D convolutional networks for the above network model.

For the flow of this model with different sections of this paper, the following consecutive sections are elaborated. In Section 2, the description of the related works with the different existing models are mentioned. The framework for the complete original image hidden under the host image across three network components is explained in Section 3. This section mentioned different approaches as per the model of secret images using various techniques to find out the secret details. In Section 4, experimental results explain the concealed multiple images and the recovery of those images with corresponding information. It is concluded in Section 5 that future works are listed.

2 Related works

The image processing with various approaches have been developed as per requirement of image quality, transparency and transfer from one medium to another. Sometime, two approaches generate good performance compare to single approach. Example: The quaternion matrix-based colour image processing model was inspired by the two methodologies (a) low-rank decomposition and (b) nuclear norm minimization [38]. Their bonding approach is designed normal to complex domain based on optimal methods. Sometimes, segmentation method is used to detect the image as per edge pixels. In a recursive Bayesian approach, the

edge-based segmentation method iteratively scans the picture for edge pixels using a Gaussian process regression model of an edge of interest. Image gradients are used with global structural information to improve grouping of edge pixels sequentially [15].

It is difficult to accurately identify surveillance targets since they are often low-resolution and noisy. Although knowledge distillation is an efficient way for dealing with it, previous work has focused on reducing the number of channels in student networks, rather than feature map size. The Feature Map Distillation (FMD) approach suggested by Huang et al. [25] allows for a distinct feature map size for teacher and student networks. Feature Decoder Distillation (FDD) and Feature Map Consistency-enforcement (FMC) for low-resolution object recognition are the two primary components of FMD's high-resolution object recognition which directly lead the learning of shallow features of student networks.

Although different steganography models have been developed to maintain hiding of image information as demand of research work, it still requires developing more secrecy of image information differently. Despite the recent exciting results obtained by incorporating deep neural networks (DNNs), steganalysis [38, 39] is used for secret messages and still preserves the secret mechanism itself. It can be considered privacy preservation of image data in container using [6, 7]. Few authors have used DNNs for the binary representation of a text message instead of images. Additional DNN is used to assess the essential details received from the image box. A procedural model is proposed to render hidden small messages in images [27]. Few techniques help insert the required image information through the communicated networks with fairly general alterations for bearing such as rotation, inversion etc. DNNs have used hidden images for the adversary's message [24]. In [22], Goodfellow et al. have found a generative-adversarial-networks (GANs) approach to yield noise signals to discover a hidden message. The above techniques concentrate on encoding small messages, steganographic model studies, and image detection.

As per Auto-encoding networks [3, 23], authors developed the nearby image density. The system has trained to condense the image and put the secret image under the assigned host image. The transformed images are performed on compressed images, such as image boundaries and orthogonal components [44]. Kingma and Ba have developed the model that trained for three networks with stochastic optimization [29] and initiated with various parameters. But Abadi et al. used default parameters for the experiments based on machine learning techniques [1].

Various methods are used for obtaining secret knowledge via LSBs, such as steganalysis tool kits and others like multi-objective-based feature selection [2, 10, 11]. As in [4, 12, 49], various authors have developed their methods for the secretion and compression of sensing image data and fuzzy-based data selection. Using steganalysis methods consisting of sampling, statistical analysis [42], and StegExposeis is highly efficient for previous pixels. The image quality is developed using deep learning based on the convolutional neural network (CNN) model [13]. The software quality of data for biometrics has been developed in [16, 30], whereas data privacy is designed in [8, 9, 14] during distributed data sharing in a computational network. Liao et al. have developed the model to separate the data hiding from the encrypted image [33], partition Strategy in Color Image Steganography [34]. They have used resourceful steganography for inserting a group of secret information into multiple images adaptively. They distributed these images in a cloud storage with the receiver, using existing single image steganography [35].

From above study, we found various image steganography algorithms could hide only within one cover. Local image steganography does not allow scaling and location adaptive

image steganography which refer to multi-secret steganography within single cover. This makes the literature gap from existing work. Thus, we aim to make image steganography that hide a full-sized multi-image with secrecy into single termed cover. This is achieved as per proposed model which is mentioned in next section.

3 Framework for secret image

Although different authors have developed their own model for Image Steganography, they have not developed the secrecy for different image information in a single location. Thus, we proposed the model for maintaining the secret information of multiple images into one image. Here, the model and its components are explained in subsequent sections in this paper. Initially, we considered the transferring image system with three essential components to hide and transfer images as required in Fig. 2. It prepares the image adequately in the first part (i.e., image information with size) and holds it in the grounding network. This Network collects the original images, and the details are analysed in the correct format. Such images recognize the next step or next part of the system as a hidden image. The central part of the system is referred to as the concealing network in the second part, which gathers hidden images from the system's first part. This section organizes both the host and hidden images to keep the secret information under the host image for the strongbox image to be looked at and kept. From a strongbox, no one can see the secret image. In the third section, it is considered that the disclosure network gathers the confidential image information and discloses the original image to the recipient.

The Network of both encoders and decoders has been trained to reveal a hidden image. The DNN determines the position of secret information in the proposed work, places the hidden information, and squeezes the image as necessary. The neighbouring pixels of entire color channels disperse the hidden image. For host and secret images, both work as a couple or pair.

The complete structure comprises three networks: Original, Hiding, Network Reveal (Fig. 2). For preceding the image transformation, these networks are considered. The first Network initiates the image work in two parts, such as (a) the original image (b) the host image (another

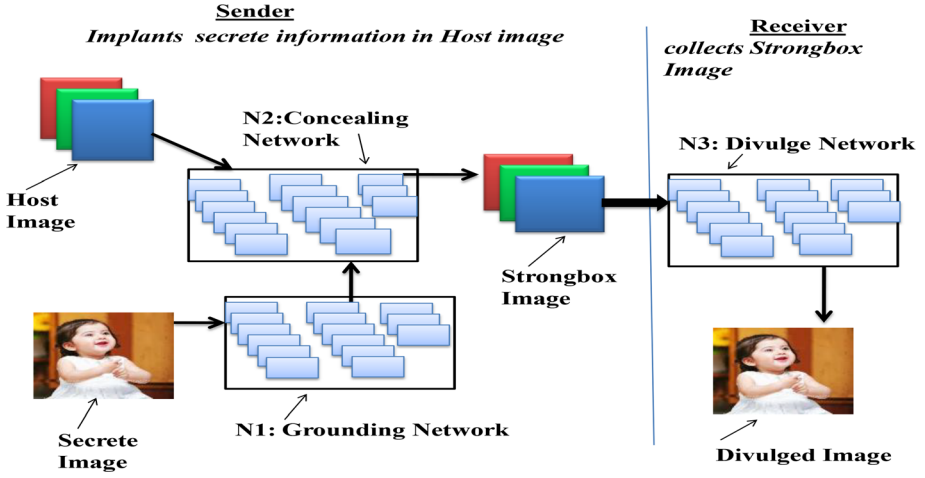


Fig. 2 Components for transferring image system

image), trying to hold the original image within itself, i.e., the hidden image under the host image. The first Network's essential job is to build the color pixels (Red, Green, and Blue (RGB)) of the original image (secret image) to be transformed with image features into a hiding network. The deep learning approaches are used to process these works. The concept of Fig. 2 is collected from [4].

The concealed image is embedded under the host image by the Concealing Network in the second part of the Network (N2). The output image of the initial Network enters the Concealing Network input image and operates with its host image. The pixel field consists of an NxN pixel for the input image and a hidden RGB channel-based host image. The performance of the second Network generates the image of the container cantered on (N x N, RGB pixels). The outcome of this work depends on the image of the strongbox, which is a design by (N x N, RGB pixels). The strongbox image is shown in Fig. 2 as a host with enough details to recreate the hidden image.

The Divulge Network is built in the third part of the framework, mining the concealed image from the strongbox. The image of the sender and receiver is communicated through the proposed method with container confidentiality. The basic approach is used for auto-encoding networks from [23] and renders a reduced image [3]. Here, the combination of the two images is shown in the container as the host image. The proposed system is intended to reduce errors between the propagated images.

The secret image is processed through the ground network, as shown in Fig. 3. All transformed images will evaluate the number of compressed images, such as image boundaries and orthogonal components [44]. In Fig. 3, the original images are transferred by the grounding network. Here, the N1 Network collects original color images. It considers three channels in this Network to take out the image information and reach the concealed Network. The edge of each image is defined from this channel by zooming. The middle channel produces vital image frequency areas described in the right zoom image in Fig. 3.

Three parts of the network function as a solitary network are shown in Fig. 4. For operating them, the primary cryptic method is used. Two terms error are generated in the system such as (a) the term 1 is identified by the error = ||H-H′|| through Grounding and concealing networks and (b) the term 2 is influenced by the error = || O-O′||. Two network components, such as the Grounding and concealing network components, are used to determine the error with O and H's help (where O is the secret image and H is the host image).

Further, the error propagation is determined as follows. Let the original image (O), receiver image O, host image (H), and receiver host image (H) are used to determine the error propagation as follows using weight (α).

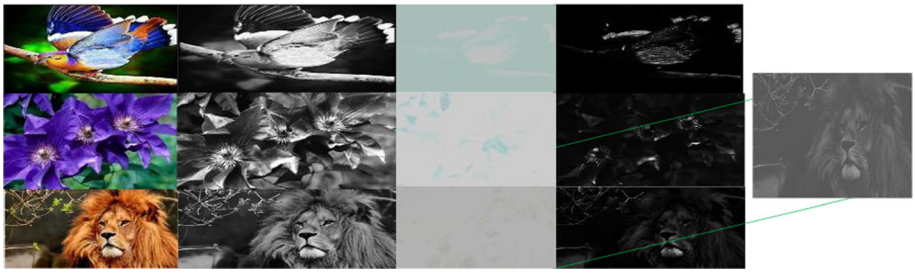


Fig. 3 Transferring image by grounding network

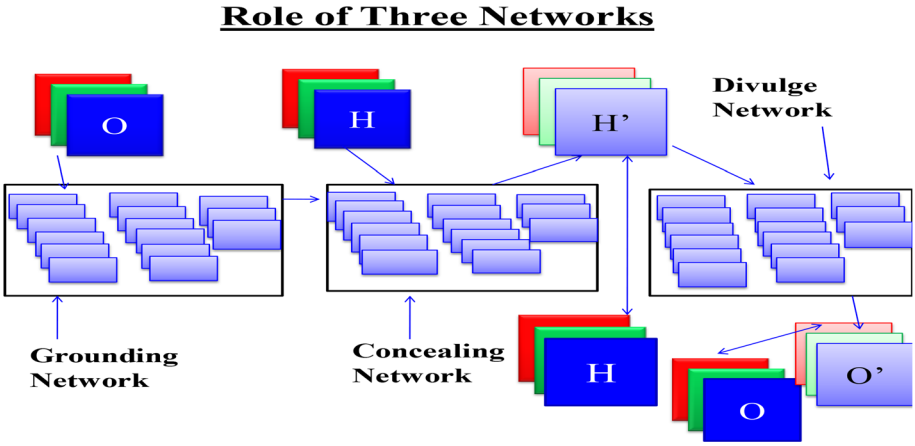


Fig. 4 Three parts of Network worked as solitary Network

$$L\left(H, H^{'}\ O, O^{'}\right) = \left\|H{-}H^{'}\right\| + \alpha\left\|O{-}O^{'}\right\| \tag{1}$$

Equation (1) determines the breeding error as per model shown in Fig. 4. Here, the host image error is modified with the weights because this Network does not rebuild the host image. It is only capable of retrieving the hidden image from the strongbox. It is also trained to relay hidden image information to all networks with $\alpha\|O\text{-}O'\|$ signals. Equation (1) is used for both revealing and hiding networks that help to encode hidden image information. The neural architectures and training hyper-parameter are utilized for getting excellent networks for the needed task. The network architecture for the image is listed in Table 1. The model revealed the efficiency of various networks with image dissimilarity. Pixel-wise and channels with RGB depth are defined by the input and output of all images.

The framework is trained for three networks with stochastic optimization [29], and the parameters are started with a variation. The experiments are developed using machine learning techniques [1] with default parameters. The ten networks of excellence with results are shown in Fig. 1. The value of α is set for quantitative gain; otherwise, $\alpha = 0.75$ for less quantitative benefit in the networks. Alpha (α) can be tried here as two settings for indistinguishable performance, such as 1.0 and 1.25. For both the host and secret picture, the mean error per

Table 1 Design the structure of image for three parts of Networks

Network	Input	Results	Performance remarks
Grounding	100×100×3 → (Image to secrete)	→100×100×5 (Transmitted secrete image)	The diversity performance-based dimensions are attempted, but it creates similarity from 5 channels.
Concealing	100×100×3+100×100×7 → (Host Image & Transformed Hide Image)	→100×100×3 (strongbox Image)	The results come into view as the original host image.
Divulge	100×100×3 → (Strongbox Image)	→100×100×3 (rebuilt secret image)	This part is in divulge Network with receiver. Here, the decoded result should become visible like a secret image.

network channel is evaluated. The consequence of the error is 2.4 for the host image, 3.4 for the hidden image. The evaluation is calculated against the obstacle of ImageNet.

The secret part of the architecture is built for each Network with the same size, phase, and activation utilizing {size, step, depth, activation}. Still, the depth is modified depending on the Network. It is distributed between inputs and outcomes. It has been constructed as 2D-Conv by a 2D convolutionary network with a standard format (size, stride, depth, activation). For example: 2D-Conv (2 × 2, 1× 1, 5, tanh) is used for Grounding with depth 5, but depth 3 is used with other parameters (size, stride, activation) for both Concealing and Divulge Network. In both grounding and concealing network, the network architecture preserves secrete image as {→ 2D-Conv (4 × 4, 1 × 1, 25, relu), → 2D-Conv (2 ×2, 1 ×1, 25, relu)} in both grounding and concealing network whereas {→2D-Conv (4 × 4, 1 × 1, 50, relu), →2D-Conv (4 × 4, 1 × 1, 25, relu)} in divulge network.

3.1 Discovering secret information from image

Let the sender select the available image from the host image in the proposed scheme, and the opponent gets another available image without a hidden image. By design, the secret image is revealed from the container, as shown in Fig. 5. The secret image is not so mysterious that the secret image's safe and recognizable features are observable.

In Fig. 5, the hidden image is available in a strongbox under the host image with enormous transparent color regions. The question arises: how many secret images can retain by the sender for higher-entropy images? To collect the hidden images from the sender, the opponent will create its plan. In this case, to avoid the image's originality, the image can be changed as required before sending it to the container. The outline of this idea is as follows.

Since we aim to develop a distinguished container network to preserve a hidden image under another image while transferring images, the encoding-decoding network method is considered for our proposed model. Thus, we used ten different networks with corresponding architectures and broadcasting with valid parameters. It has also been trained on three types of image-based networks, such as (a) host image, (b) hidden image, (c) strongbox image. These images are regarded as a cluster/set of "+ve." The "-ve" set is created by replacing a secret image with a randomly selected image. For avoiding the disturbance of the revealing image, this collection does not include a strongbox. As described in Fig. 6, the secret images implanted inside the strongbox are considered +ve sets.

The deep neural networks (DNNs) are trained to discern a collection of positive and negative hidden image samples in containers. As per the proposed Network, the initial and host images are transferred. The training samples are evaluated by networks that are instructed.

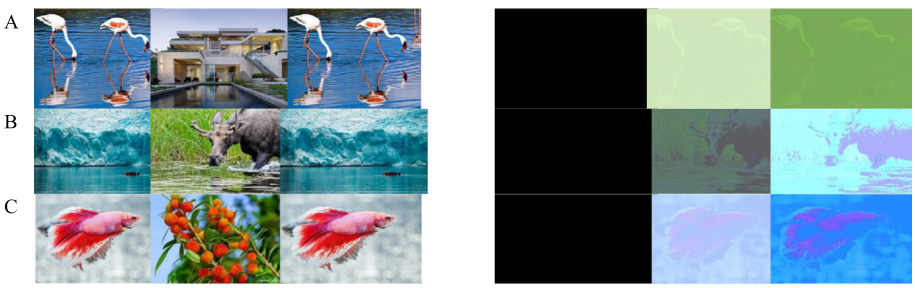


Fig. 5 Implanted of secrete and host images

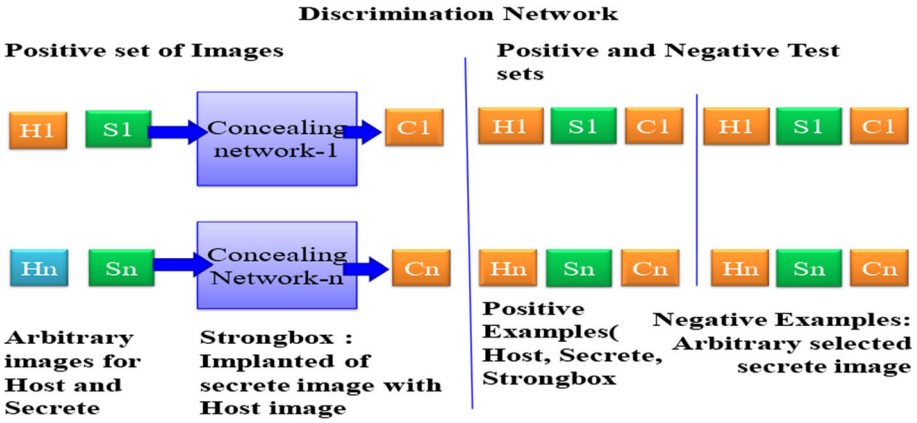


Fig. 6 Positive and negative test images through trained Network by making three kinds of images (Host, secrete, strongbox)

Thus, three networks have been considered, which are already clarified. Both networks are actively contributing their findings to image processing. On proposed triplets, more than 95% of accuracy is obtained. For a known secret image, extracting the original image from the container without decoding the image is simple. The model does not retain an unaltered host. Detection sensitivity is therefore improved.

The high accuracy rates are generated without revealing confidential information based on an embedded image in a strongbox. For strongbox image transformation, it uses a sequence of blur operations. The discrepancy between the original and the container image can be obtained via the RGB channel with revealing results. The technique revealed is measured as: Revealed result = min(255| Strongbox–strongbox$_{blur}$| x V) and $5 \leq V \leq 20$. As shown in Fig. 7, the usual transformation provides smaller elements of the embedded image.

Moreover, the outcome and the blurred result cannot be compared exclusively to the unchanged host image. When it collects and compares the result and blurred result images, as shown in Fig. 7, there will be no difference between them. It retains the same quality of color. This is a probable susceptibility to the original host image but exclusive of the right to use it.

In general, removing the blurred container image makes it difficult to discover the data from the hidden image. Despite this, the study provides details about the secret

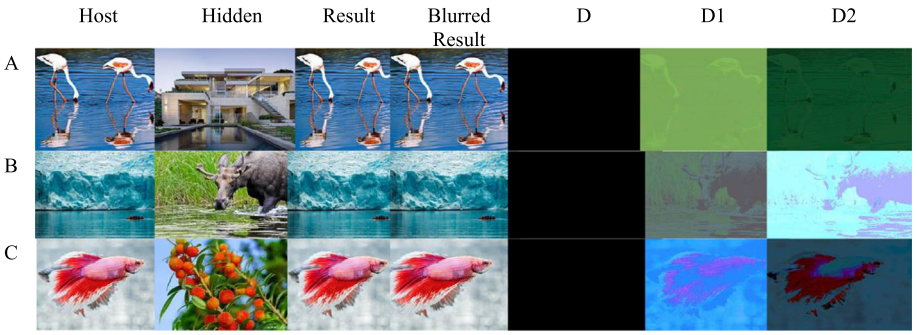


Fig. 7 Unchanged host image and Blurred Result

image process that is quite clearly implanted in the absence of areas of the host image. It has previously alluded to a hidden picture that does not reduce the efficacy of this process for unique detection such as watermarking. Nevertheless, by removing the replicating portion of the secret image after image modification, the known secret image would produce a significant problem. The techniques are used in the next section to generate hidden data with less perceptible details.

3.2 Blurring the secret image

We have considered the last segment in the strongbox image where leftovers of the hidden image are discovered. The position of DNN in the unaffected host image is essential. But it is clarified that two methods are concealed with the hidden image. The expectation of the hidden approaches is concerned with (1) when the host image is identified without image quality disruption, the specifics of the hidden image are very difficult to ascertain, (2) the hidden approach involves local error without error transmission. It is difficult for a huge quantity of secret information to encode both host and secret images accurately. Each mistake affects each pixel. Therefore, it affects the reconstruction of pixels based on a hypothetical hidden image obtained.

The simple approach designed for concealing the hidden image is to process the modification of the pixels prior to forward the image to the concealing Network [43]. The cryptic Network reveals a jumbled secret image, the images are acquired from the strongbox image. This process has significant characteristics for each pixel without disturbance of other pixels, the neighbouring inaccuracy can be harshly reconstructed. Thus, the countable image is unidentifiable, lacking any rebuilding defect.

After using blurring approaches, the secrete images maintain permutations on the pixels before use in concealing network and the result is shown in Fig. 8a based on blurring images. This model sends the secrete image with the host image with shuffled shown in the left column in this figure. The secrete image transfers pixels permutations with a performed image. The receiver recovers the decoded secrete image from the right half column and the original secrete image. The remaining error images of both host and secrete images are shown in error columns. As comparing to Figs. 5 and 7, the error doesn't involve both secrete and host images.

It utilized exciting networks in the earlier sector with or without permutation stages enclosed approximately the remote system. Sometimes, it did not work for stock-up images as pixels through neural networks (NN) [23, 31]. The NN briefly signifies the information in an image by making use of space coherency. Sometimes, the rearrangement images are deficient in space formation. So, the Network is needed to commit to memory pixel strengths. The system is not always trained to execute well only standard images on pixel rearrangement images. But it reiterates the whole exercises for secret images to conceal images exclusive of the spatial coherence of usual images. More than ten networks are considered to retrain the identical structural designs with additional rearrangement steps.

Figure 8b explains the performance of the largest Network in an experimental self-determining test collection (a). Here, the absence of colour exchange of the primary concealed in occupying space construction is perceptible ("Shuffled-1" in 3rd column). Similarly, if the inaccuracy of the host image reconstruction is exaggerated, it is challenging to locate the hidden image mark (Fig. 8a, Column 7). Figure 8b shows the

mean error per channel of both the host and the hidden image Fig. 8b. The host and secret image are represented by a pair of data values in this figure. In this figure, four pair bars are available as (1) one-time combination rearrangement, (2) multi-combination rearrangement, (3) qualified rearrangement network, and (4) permutation-free baseline. The midway rearrangement images are also listed.

In general, networks are trained to encode rearrangement images that are substantially slow compared to the training's simple hiding networks. Different hiding networks are taking diverse time for preparation. Encoding images of rearrangement is an imperatively significant problem. Ultimately, for necessary processing, it is essential to investigate the rearrangement of images. Tracing the actual location of the pixels [32] is created by rearranging images with space coherence. On the other hand, alternate mappings can be alleviated on the basis of a large number of established aspects [20].

3.3 Concealing numerous images

The proposed model effectively implants an additional full-colour M×Mimage of the same size as the hidden image arrangement or rearrangement, as shown in Fig. 1. It generates various aspects of the pixels compared to the encoding of non-pixel rearrangement images with M x M, which does not trust the nearby space construction in standard images. It encoded more than a single image in the concealment of multiple images as its capability without using the network capacity for pixel rearrangement. If it secretes the different images, each image is

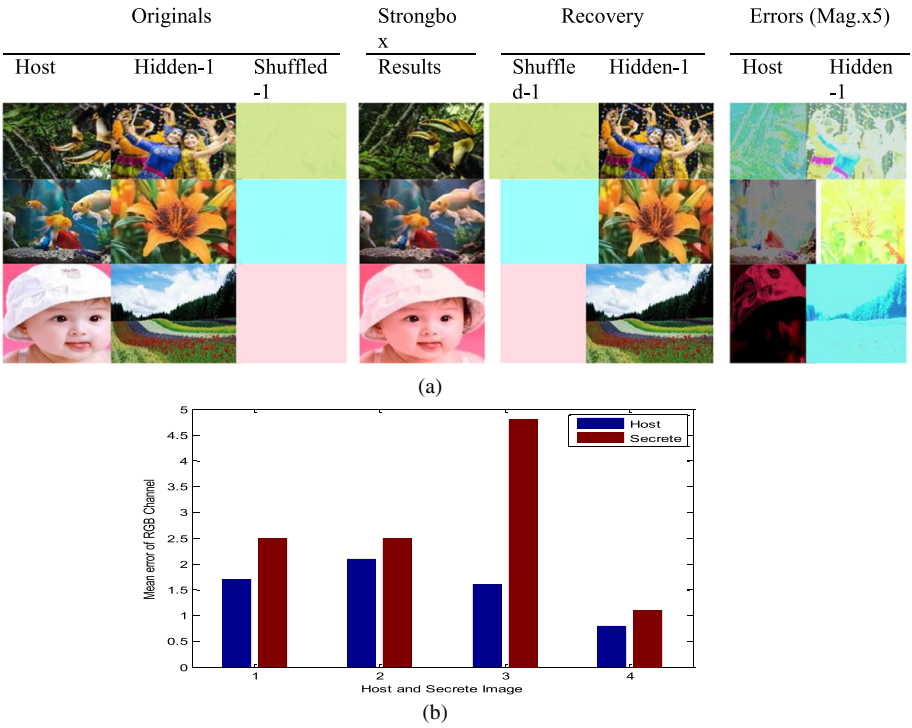


Fig. 8 **a** Cryptic approaches for host and secrete images. **b** Mean error in RGB channels for host and secrete image

complicated to restore when encoded exclusively for any disturbances. The ability to hide the excess of a solo image in addition to secrecy also enables us to hide multiple, autonomous, pixel-wise sources of complementary details, such as image quality, image movement, number of images, image depth, etc.

In reality, it attempts to hide two full-size M×*M*images based on 2 × the amount of information in the host, as shown in Fig. 9. At last, for whole process, the permutation approaches are taken on secret images where two images are permuted and secret within one host image.

4 Experiments

4.1 Data sets

We have considered the data set of various images from the ImageNet images. We randomly selected images from ImageNet dataset. We collected the available images from the Corel Database [41]. We considered almost 2,000,000 images in the system for experiments.

4.2 Experimental set up

We have used different experimental setting components for our proposed model such as software tools, languages, and packages. We considered python language with NumPy. Different experiments are demonstrated on a personal computer (PC) with software and hardware specifications such as 1) an Intel Core i7 CPU with 16 GB of RAM, 1 TB Hard disk and 2) Python 3.0.7 on a Windows 10 OS for implementation. MATLAB tool is also used to evaluate the dataset and graphical representation of data. We used Python library i.e., TensorFlow for deep learning approaches as our model.

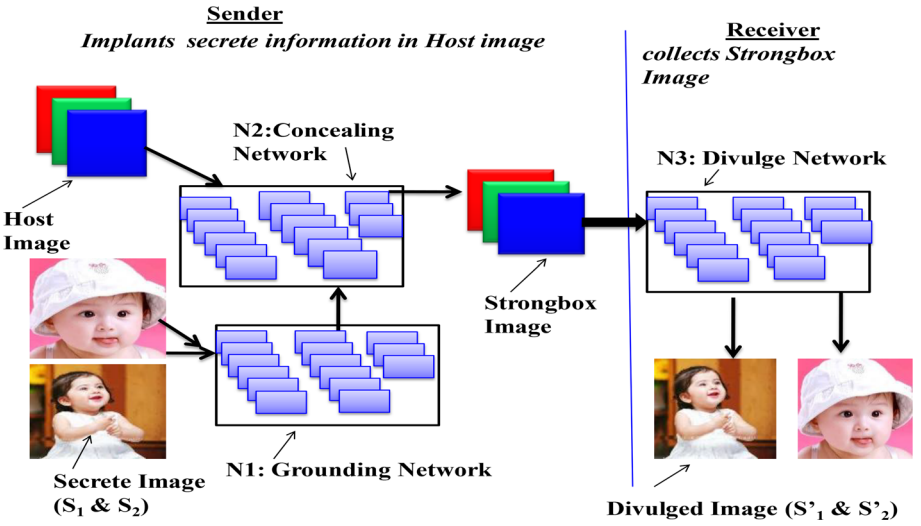


Fig. 9 To secrete two complete M×*M* images inside a host image with equal size and compare with Fig. 2

4.3 Rebuild the strongbox image

The system focuses on encoding enormous image details with a visually appearance. There is no apparent attempt made to secrete the information from the revealing computer. The image information is a part of the hidden message, which is challenging to find out and cannot be abstracted to be secret. But it can evaluate the confidential image data that resides in it.

Many methods are available for obtaining secret information via (least significant bits) LSBs, such as steganalysis tool kits and others like multi-objective-based feature selection [2, 10, 11]. As in [4, 12, 49], various authors have developed their methods for the secretion and compression of sensing image data and fuzzy-based data selection. Using steganalysis methods consisting of sampling, RS analysis, statistical analysis [42], StegExpose is a highly efficient method for previous pixels. In addition, for large series, the threshold is set as needed. The ROC curve is then shaped accordingly, which, as seen in Fig. 10, differs from random guessing. Figure 10 is developed based on true positive and false positive rates during detection of an embedded image via DNNs.

StegExpose tries to get information from merely placed in the LSB bits. The images are arranged as 24 bits (8 x (R, G, B)) with some pixel bits. The R channel for all pixels of the host image in the container can determine the effect on the rebuild of the container image, as shown in Fig. 11A, B. The Red, Green control the container's image, and Blue Channels with bits of magnitude and impact proportion. In rebuilding the secret image, bit flip is essential for the bit position of all colour channels. The error doesn't affect the bit position of the secret image. Thus, the information of the secret image is transferred in colour channels without disturbance in LSB.

The hidden image transformation is pushed with confidential data. The dissimilarity measurement between the original and its secret image is called a pixel distance procedure to find the error as follows. Let a secret image O, host image H, be available as a proposed system in container image C with both concatenations.

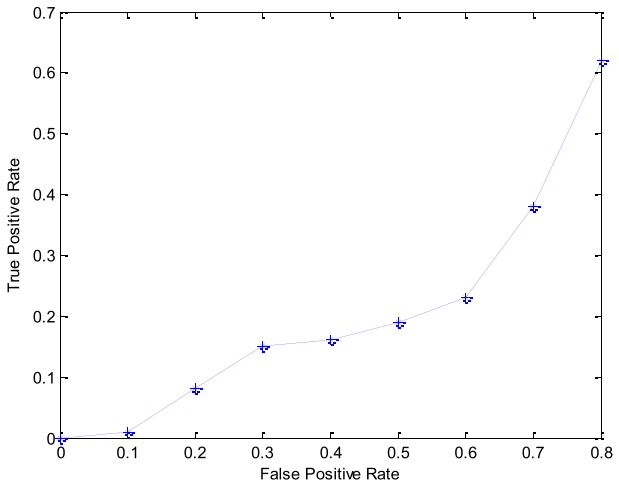


Fig. 10 ROC curves: True Positive Rate vs. False Positive Rate

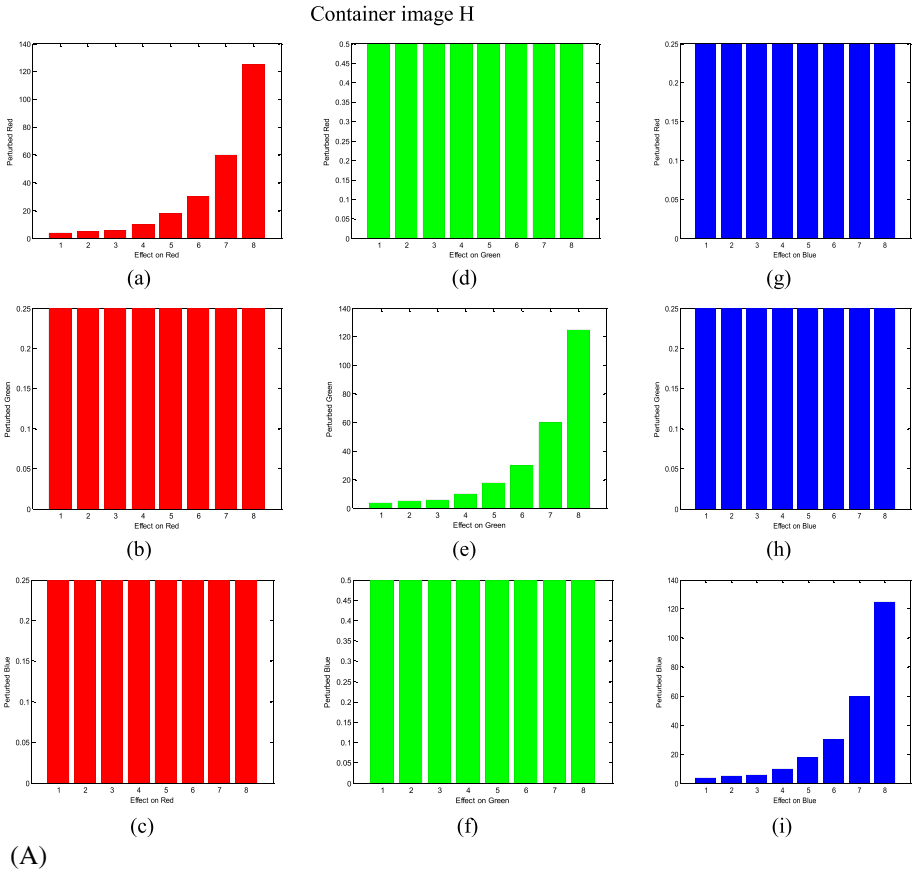


Fig. 11 **A** Sensitive Bits in the Container Image without effect on other bits. **B** Same bit flip in the container image has effects across all colour bands in the recovered secret image

The image in C passes to the Reveal network to disclose O'. For spatial distribution, both images represent the change. Let the modification is taken in C as C_n on a single pixel and pass to Reveal Network provide $O_0^{'}$. It determines pixel-distance from the perturbed pixel as $\|O'\text{-}O_0^{'}\|$ on each pixel, as shown in Fig. 12. It is remarked on this pixel-distance as follows. The secret image is shared with boundary pixels and colour bits. Secret image pixel encoding is shared in containers. With the help of CNN, the sum of spatial distribution is taken into account. Atrous convolution layers [18] can be taken for this system, but they do not consider this system.

Based on (a) collected ImageNet images as -ve samples and (b) proposed strongbox images as +ve samples, the detection networks were considered binary classifiers. The tested input image and architectures found that the detection networks carry out excellent on the image with 24 x (N x N) heaped binary input layers. Each input image retains the above input layers based on the qualified networks.

The secrete image is implanted contained by the host image in Fig. 3. The output at the strongbox image is listed in the third column as 'result.' Based on the distinguished image, the opponent can try to get both original and host images by amplifying these images. Via three

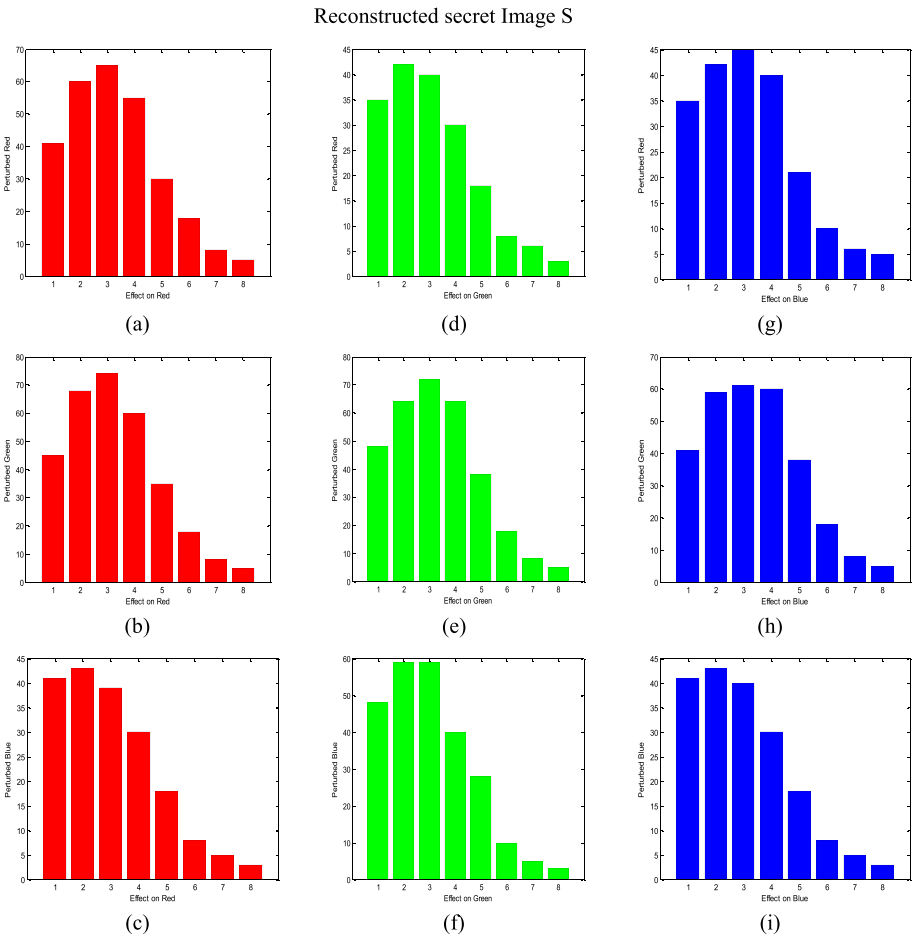


Fig. 11 continued.

columns with differences, few tested images are listed for amplifying visible secret or host image. Here, D, D1, and D2 define the variations. Such variations are not fixed; they can vary according to amplification.

The uncovering networks obtained some ranges of combined classification rates. The Least-Significant-Bit (LSB) is obtained using a color channel and a hidden image from detection networks. The least L is checked on to hit more than 99% of the combined rates (1, 2, 3, 4). The detection rate remained as before for extra bits inserted randomly at 4-bit locations. Therefore, based on adjustment with extra bits, there is no such number of detection rates.

The detection rates do not impact confidential information, image alteration, orbit positions of image. Thus, it focuses on the location of the secret image rather than the ability to notice the quality of the secret image.

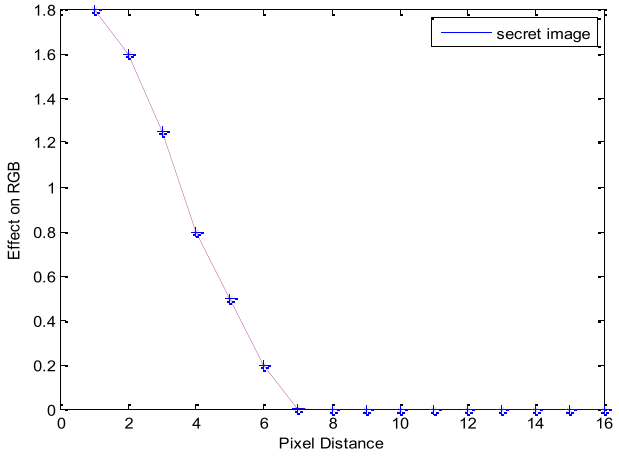


Fig. 12 The average effect on perturbing pixel for reconstruction of secret image based on pixel distance

4.4 Image error analysis

The images are experimented as per proposed model as shown in Fig. 9. As per experiments, the second essential bits' loss on all images with weighted uniformly. Each transmission channel part needs to be retrained by the system. The test's success is shown in Fig. 13a, b lists the measurement of many errors in the hidden image of the experiment. Here, the error occurs, but the reforms remain, indicating good consistency.

When concealing two images within a solo host image, there are three outcomes created with distinctive rebuilding. In the smooth area of the host image, less saturated colors emerge, and differential noise is available.

It experimented with the two-image concealing method in equal networks. It trained inequality networks from Section 3 to discover a precise secret image that was implanted in a container image. The revealing networks had approximately 95% accuracy for the solo picture concealing mission. The accuracy decreases to approximately 73% for the encoding of various network images. The practice of concealing data further conceals the hidden picture based on necessary assumptions.

At last, we used the perturbation and the various images concealed in the same system. Basically, inside a solo host image, two images are permuted with secrets. On a secret solo image and the non-permuted two-secret image systems, the reconstruction errors increase significantly. Despite the long training times allowed for considered networks, the growth of errors is visible. The mean error of the RGB channels for the host and two secret images is shown in Fig. 13b. The mean error differential is shown in Fig. 13c. There are some examples of the secret and restored images available in Fig. 14a. The accurate quantity of the images is included with the statistical production for identification, despite the increase in disruption and rebuilding errors.

4.5 Image quality loss on recovery

It obtained the images for visual evaluation with statistical measurements of both host and strongbox image reconstruction errors and reforming the hidden image from the container image. It is claimed that the strongbox image became recognizable as a host image based on the success of the proposed system. The rebuilt images are simply identifiable according to

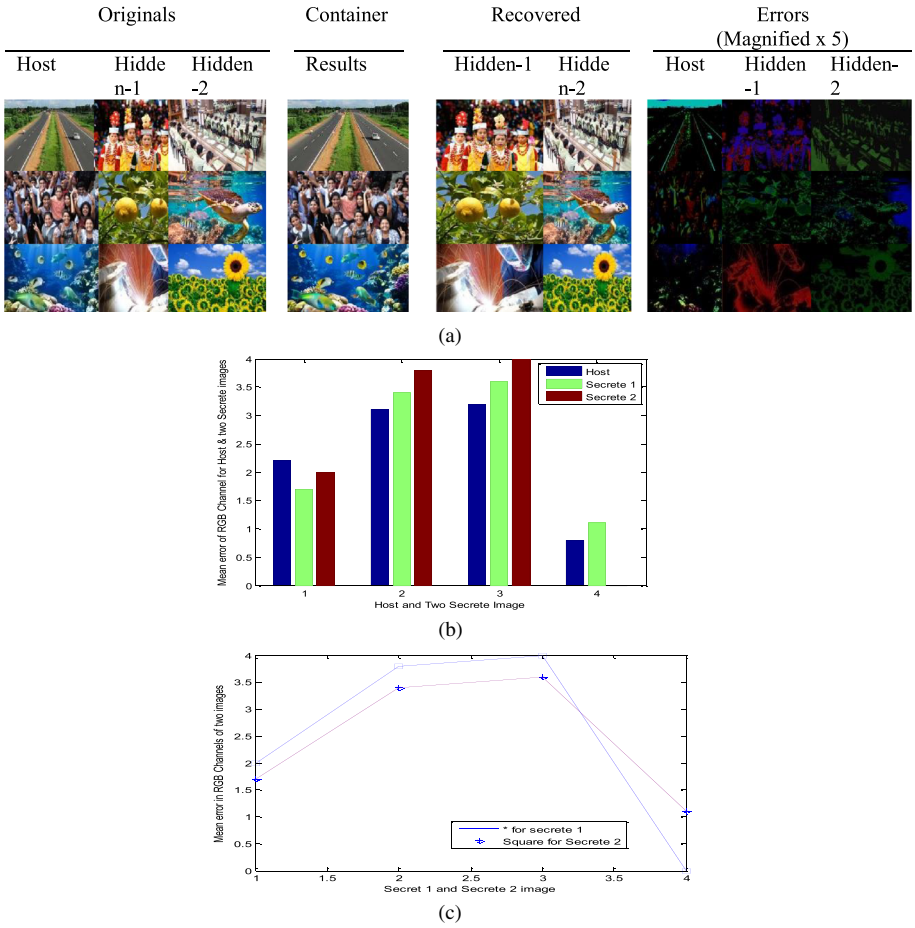


Fig. 13 **a** Two images under single host. **b** Mean error in R,G,B Channels for host and two secrete Images. **c** Mean error in RGB Channels for secrete 1 and secrete 2 Images

secret images. Thus, the images are identifiably defined based on an image recovery system [5, 21, 40, 48]. Many techniques are used to generate similar images from many images, as in [5, 42, 45], without any modification.

The recovery task was based on a built or reconstructed image in multiple formats, such as a container image, a reconstructed hidden image, and a two-fold reconstruction image (i.e., intimate two images in the system). The goal is to recover the images of the novel host, secrete-1 and secrete-2, correspondingly on the entire identical match. The complete image record is initially collected from the ImageNet, Site, and Corel Database [41].

When concealing two images within-host images and eliminating space continuity, it generates distinctive image reconstruction. The performance demonstrates severe deprivation of noise volume and ability deficiency. The particulars of the images, such as size and statistical data, are simply recognizable and integral.

It determined the accuracy based on the recovery of the exact image as the single top match from total images. The 500 look-ups are tested for the experiment. The scores are mentioned in majority of the tests as in Fig. 14b. This is happened on the largely violent of the concealing

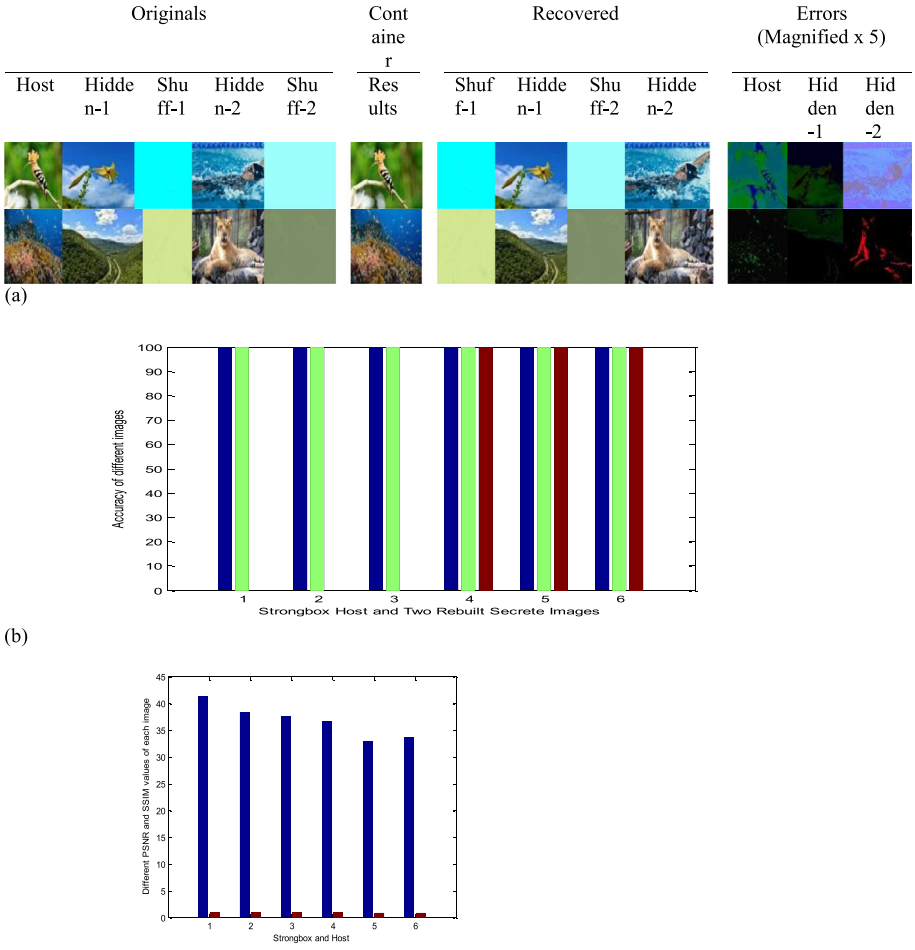
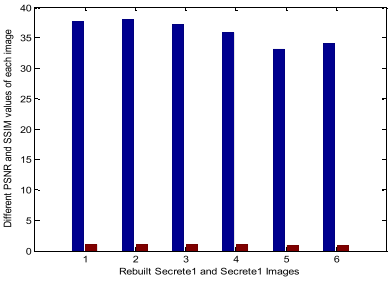


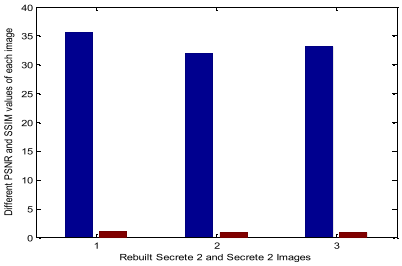
Fig. 14 **a** Distinctive rebuilding of images. **b** Recovery performance of several testing of total images. Five hundred trials for the experiment, Accuracy result. **c** PSNR and SSIM scores between strongbox and host. **d** PSNR and SSIM scores between Rebuilt secret 1 and secret1. **e** PSNR and SSIM scores between Rebuilt secret 2 and secret 2. **f** PSNR scores between Strongbox and Rebuilt secrete 1. **g** SSIM scores between Host and Secrete 1

process explained in this paper. It has also considered two images for concealing in a solo network with arrangement through permutations.

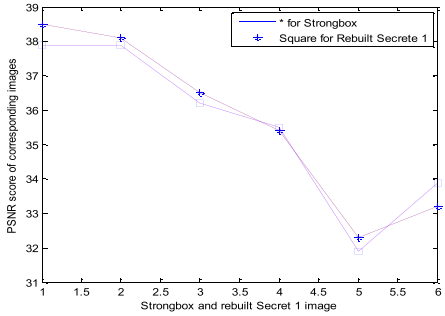
For strong and secret images with precision, several resulting values are produced in Fig. 14b. Due to good precision, the figure demonstrates good output on strong and restored secret images. In this figure, six parameters are taken into account, and the accuracy of three pair images, such as (strongbox, host), (rebuilt secrete1, secrete 1), and (rebuilt secrete2, secrete 2) are evaluated. Six parameters are (a) secret-1 without permutation image, (b) secret-1 with single permutation image, (c) secret-1 with multiple permutation image, (d) secret-2 without permutation image, (e) secret-2 with single permutation image, (f) secret-2 with multiple permutation image. The above parameters are used for evaluation on the above pair of images. In Fig. 14b, column 1, 2, 3 are secret 1 image with no, single and multiple permutation whereas (strongbox, host), (rebuilt secrete1, secrete 1), and (rebuilt secrete2,



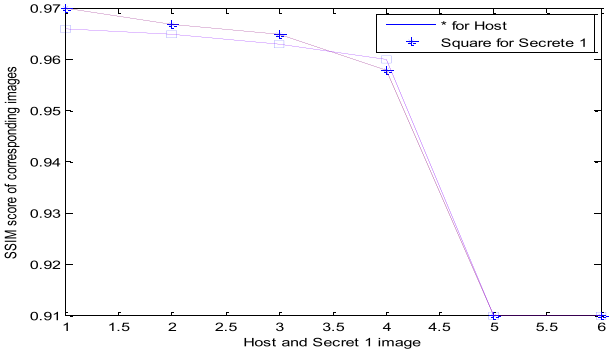
(d)



(e)



(f)



(g)

Fig. 14 continued.

secrete 2) are identified as three colours such as Navy blue, Lime, Brown respectively. In column 1, 2, 3, brown colour is not available means (rebuilt secrete2, secrete 2) is not applicable due to secret 1 image maintain own information. But in column 4,5,6, (rebuilt secrete2, secrete 2) is evaluated and shown in brown colour in Fig. 14b. Similarly, in Fig. 14c-e, PSNR and SSIM contain Navy blue and brown colour respectively.

Finally, for the proposed method of experimental evaluation, two typical methods, such as the Peak Signal to Noise Ratio (PSNR) and the Structural Similarity Index (SSIM) as per [47], are taken into account, as shown in Fig. 14c-e. The distinct PSNR score is in Fig. 14f between Strongbox and Reconstructed Secret 1 and the SSIM score is in Fig. 14g between Host and Secret 1, respectively. The PSNR and SSIM scores are similar to the corresponding pictures as shown in Fig. 14f, g, respectively. These figures provide perceptual data evaluated to assess the fluctuation in image quality between unique, host, and rebuilt image. Several resulting values are generated using PSNR and SSIM methods based on the same parameters as in Fig. 14b with the same pair of images. The results of the above methods are shown in Fig. 14c-e.

4.6 Comparative analysis

Although, our proposed work is very rarely used and we couldn't find such kind of work which can compare with existing work on different model. Different author may be developed own methodology or model for hiding or maintaining secrete information in a single image, but we considered information of multiple images hide in a single image with maintaining secrete information of original image which was a challenging task for us. Thus, we don't compare with any existing model which related to our work, but we considered comparative analysis within our proposed model with different approaches.

The following comparison have been taken within our proposed model.

(a) The mean error is different in RGB channels for host and single secrete image as shown in Fig. 8b, but if we compared with host and two secrete images, its mean error is changing with little changing values as shown in Fig. 13b. Further, mean error in RGB Channels for secrete 1 and secrete 2 Images are different in Fig. 13c.
(b) The colour channel for all pixels of the host image in the container can regulate the effect on the reconstruct of the container image, as shown in Fig. 11A, B. Sensitive Bits in the Container Image does not affect on other bits as shown in Fig. 11A whereas same bit flip is considered in the container image that effects across all colour bands in the recovered secret image as shown in Fig. 11B
(c) When we considered accuracy result analysis, we got two different kinds of output which is clearly shown in Fig. 14b. In this figure, first three columns are showing secrete 1 image with different permutations whereas last three columns are showing secrete 2 images with different permutations based on solo networks.
(d) Different PSNR and SSIM score among strong box, host, secret 1 and secret 2 have been compared with different manner of approaches.

5 Conclusions

In this paper, we have proposed DNN self-possessed system which is built to secret images under other images. Implanting a full original image into a new image of the same size is

considered many bits to be devoted to the hidden image. Three categories of image processing networks are considered for developing our proposed model. Additionally, the deep neural network techniques are taken to conceal twice for more information per host medium. The detection networks are trained after creating encoding system. Thus, based on the determinability of the secret information, the opponent is used to supply a complementary error signal and minimize reconstruction errors. During permutation of the secret image, the host and both secret images are simply recognized with comparable error rates. Finally, we have concentrated on hiding information to resolve opponent intent such as stealing or altering images that generates secret information. For all standard platforms and web browsers, the output of this static content (i.e., host image) is observable. Two important typical methods such as Peak Signal to Noise Ratio (PSNR) and the Structural Similarity Index (SSIM) are used to find out difference between host and secret image by their corresponding evaluation scores. The 500 look-ups are tested for the experiment. The scores are generated as per the permutations of the tests. This is happened on the largely violent of the concealing process explained in this paper. The deep neural networks will be trained directly with the motion vectors based on image density for future work.

Data availability The data that support the findings of this study are available from the first author upon reasonable request.

Code availability The code is available from the first author upon reasonable request.

Declarations

Conflicts of interest/competing interests The authors declare no conflict of interest.

References

1. Abadi M, Barham P, Chen J, Chen Z, Davis A, Dean J, Devin M,Ghemawat S, Irving G, Isard M et al. (2016) Tensorflow: a system forlarge-scale machine learning. In OSDI, vol. 16, pp. 265–283
2. Aslam MA, Azam MRF, Abbas M, Rasheed Y, Alotaibi SS, Anwar MW (2022) Image Steganography using Least Significant Bit (LSB) - A Systematic Literature Review. 2022 2nd international conference on computing and information technology (ICCIT), Tabuk, Saudi Arabia, pp. 32–38
3. Baldi P, Hornik K (1989) Neural networks and principal component analysis. Neural Netw 2(1):53–58
4. Baluja S (2020) Hiding images within images. IEEE Trans Pattern Anal Mach Intell 42(7):1685–1697
5. Baluja S, Covell M (2008) Wave print: efficient wavelet-based audio finger printing. Pattern Recogn 41(11):3467–3480
6. Bhuyan HK, Kamila NK (2014) Privacy preserving sub-feature selection based on fuzzy probabilities. Cluster Computing Springer 17(4):1383–1399
7. Bhuyan HK, Kamila NK (2015) Privacy preserving sub-feature selection in distributed data mining. Applied Soft Computing Elsevier 36:552–569
8. Bhuyan HK, Kamila NK, Dash SK (2011) An approach for privacy preservation of distributed data in peer-to-peer network using multiparty computation. Int Journal Comput Sci Issues (IJCSI) 3(8):424–429
9. Bhuyan HK, Dash SK, Roy S, Swain DK (2012) Privacy Preservation with Penalty in Decentralized Network using Multiparty Computation. Int J Advanc Comput Technol (IJACT) 4(1):297–303
10. Bhuyan HK, Kamila NK, Jena LD (2016) Pareto-based multi-objective optimization for classification in data mining. Cluster Computing (Springer) 19(4):1723–1745
11. Bhuyan HK, Kumar LR, Reddy RK (2019) Optimization model for Sub-feature selection in data mining, 2nd International Conference on Smart Systems and Inventive Technology (ICSSIT 2019), IEEE Explore, pp 1212–1216

12. Bhuyan HK, Chakraborty C, Pani SK, Ravi VK (2021) Feature and sub-feature selection for classification using correlation coefficient and fuzzy model. IEEE Trans Eng Manag:1–15
13. Bhuyan HK, Chakraborty C, Shelke Y, Pani SK (2021) COVID-19 diagnosis system by deep learning approaches. Expert Syst 39(3):1–18
14. Bhuyan HK, Kamila NK, Pani SK (2021) Individual privacy in data mining using fuzzy optimization, engineering optimization. Pp. 1-19 (early published)
15. Burke J, King S (2022) Edge tracing using Gaussian process regression. IEEE Trans Image Process 31:138–148
16. Chandra K, Kapoor G, Kohli R, Archana G. (2016) Improving software quality using machine learning. In: 2016 international conference on innovation and challenges in cyber security (ICICCS-INBUSH). Pp. 115-118
17. Chaumont M, Puech W, Lahanier C (2013) Securing color information of an image by concealing the color palette. J Syst Softw 86(3):809–825
18. Chen L-C, Papandreou G, Kokkinos I, Murphy K, Yuille AL (2018) Deep lab: semantic image segmentation with deep convolutional nets, atrous convolution, and fully connected crfs. IEEE Trans Pattern Anal Mach Intell 40(4):834–848
19. Fridrich J, Goljan M, Du R (2001) Detecting LSB steganography in color, and gray-scale images. IEEE Multimed 8(4):22–28
20. Fridrich J, Goljan M, Soukal D (2004) Searching for the stego-key. In Proceedings of SPIE, vol. 5306, pp. 70–82
21. Gong Y, Lazebnik S, Gordo A, Perronnin F (2013) Iterative quantization: a procrustean approach to learning binary codes forlarge-scale image retrieval. IEEE Trans Pattern Anal Mach Intell 35(12):2916–2929
22. Goodfellow I, Pouget-Abadie J, Mirza M, Xu B, Warde-Farley D,Ozair S, Courville A, Bengio Y (2014) Generative adversarial nets. In Adv. in Neural Information Processing Systems, pp 2672–2680. https://papers.nips.cc/paper/2014/hash/5ca3e9b122f61f8f06494c97b1afccf3-Abstract.html
23. Hinton GE, Salakhutdinov RR (2006) Reducing the dimensionality of data with neural networks. Science 313(5786):504–507
24. Hu D, Wang L, Jiang W, Zheng S, Li B (2018) A novel image steganography method via deep convolutional generative adversarial networks. IEEE Access 6:38303–38314
25. Huang Z, Yang S, Zhou MC, Li Z, Zheng G, Chen Y (2022) Feature map distillation of thin nets for low-resolution object recognition. IEEE Trans Image Process 31:1364–1379
26. Jain AK, Uludag U (2003) Hiding biometric data. IEEE Trans Pattern Anal Mach Intell 25(11):1494–1498
27. Jarusek R, Volna E, Kotyrba M (2018) Robust steganographic method based on unconventional approach of neural networks. Appl Soft Comput 67:505–518
28. Kessler GC (2014) An overview of steganography for the computer forensics examiner. Forensic Sci Commun 6(3):1–29
29. Kingma D, Adam JB (2015) A method for stochastic optimization. in ICLR, pp 1–15
30. Korshunov P, Marcel S (2017) Impact of score fusion on voice biometrics and presentation attack detection in cross-database evaluations. IEEE J Select Top Signal Process 11(4):695–705
31. Larsen ABL, Sønderby SK, Winther O (2015) Autoencoding beyond pixels using a learned similarity metric. Pp 1–8, arXiv:1512.09300
32. Li S, Li C, Lo K-T, Chen G (2008) Cryptanalysis of an image scrambling scheme without bandwidth expansion. IEEE Trans Circuits Syst Vid Technol 18(3):338–349
33. Liao X, Li K, Yin J (2017) Separable data hiding in encrypted image based on compressive sensing and discrete fourier transform. Multim Tools Appl 76:20739–20753
34. Liao X, Yu Y, Li B, Li Z, Zheng Q (2020) A new payload partition strategy in color image steganography. IEEE Transact Circuits Syst Vid Technol 30(3):685–696
35. Liao X, Yin J, Chen M, Zheng Q (2020) Adaptive payload distribution in multiple images steganography based on image texture features, IEEE transactions on dependable and secure computing. Pp. 1-14
36. Liu Q, Sung AH (2008) Image complexity and feature mining for steganalysis of least significant bit matching steganography. Inf Sci 178(1):21–36
37. Ma H, Liu S, Liao Q, Zhang J, Xue J-H (2022) Defocus image Deblurring network with defocus map estimation as auxiliary task. IEEE Trans Image Process 31:216–226
38. Miao J, Kou KI (2022) Color image recovery using low-rank quaternion matrix completion algorithm. IEEE Trans Image Process 31:190–201
39. Pibre L, Pasquet J, Ienco D, Chaumont M (2016) Deep learning is a good steganalysis tool when embedding key is reused for different images, even if there is a cover source mismatch. Electron Imaging 2016(8):1–11
40. Qamra A, Meng Y, Chang EY (2005) Enhanced perceptual distance functions and indexing for image replica recognition. IEEE Trans Pattern Anal Mach Intell 27(3):379–391

41. Tao D, Tang X, Li X, Wu X (2006) Asymmetric bagging and random subspace for support vector machines-based relevance feedback in image retrieval. IEEE Trans Pattern Anal Mach Intell 28(7):1088–1099
42. Trung V, Lai P, Raich R, Pham A, Fern XZ, Arvind Rao UK (2020) A Novel Attribute-Based Symmetric Multiple Instance Learning for Histopathological Image Analysis. IEEE Trans Med Imaging 39(10):3125–3136
43. Van De Ville D, Philips W, Van de Walle R, Lemahieu I (2004) Image scrambling without bandwidth expansion. IEEE Trans On Circuits and Sys Vid Technol 14(6):892–897
44. Vincent P, Larochelle H, Lajoie I, Bengio Y, Manzagol P (2010) Stacked denoising autoencoders: Learning useful representations in a deep network with a local denoising criterion. JMLR 11(Dec):3371–3408
45. Vu MH, Löfstedt T, TufveNyholm RS (2020) A question-centric model for visual question answering in medical imaging. IEEE transactions on medical imaging, volume: 39. Issue 9:2856–2868
46. Wang Y, Moulin P (2008) Perfectly secure steganography: capacity, error exponents, and code constructions. IEEE Trans Inform Theory Special Issue Security 55(6):2706–2722
47. Wang Z, Bovik AC, Sheikh HR, Simoncelli EP (2004) Image quality assessment: from error visibility to structural similarity. IEEE Trans Image Process 13(4):600–612
48. Wang G, Hoiem D, Forsyth D (2012) Learning image similarity from flickr groups using fast kernel machines. IEEE Trans Pattern Anal Mach Intell 34(11):2177–2188
49. Wang WZX, You W, Chen J, Dai P, Zhang P (2019) RESLS: region and edge synergetic level set framework for image segmentation. IEEE Trans Image Process 29:57–71
50. Xu W, Wang G (2022) A domain gap aware generative adversarial network for multi-domain image translation. IEEE Trans Image Process 31:72–84
51. Yedroudj M, Comby F, Chaumont M, Yedrouj-net (2018) An efficient CNN for spatial steganalysis. In IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP'2018, pp 2092–2096