American Journal of Interdisciplinary Research and Development
ISSN Online: 2771-8948
Website: www.ajird.journalspark.org
Volume 11, Dec., 2022

A NOVEL METHOD FOR HIDING INFORMATION DEPENDING ON FAST CONVOLUTION NEURAL NETWORK RESULTS

Asst. Prof. Dr. Ali Abdulazeez Mohammedbaqer Qazzaz,
Dr. Zeina Hassan Razzaq Elaf J. Al Taee
University of Kufa / Faculty of education / computer science department
alia.qazzaz@uokufa.edu.iq, zienah.alhadad@uokufa.edu.iq,
elafj.altaee@uokufa.edu.iq

ABSTRACT

Hiding important information into suitable cover is crucial task in keeping security information from any edit, replace and change for the purpose of protecting special communication from unwanted effects from the third parity. Hiding information can be defined as a science or art for hiding important information in digital format such as text, audio, video and image (message) into a suitable digital file (cover) into deterministic sequence to prevent the detection of the hidden information from other unwanted parts. The proposed method consist of many steps that integrates for the purpose of producing compact result, the first step in the proposed system related to encryption process of the important text that prepare to be transformed to the suitable distention by extracting suitable key from a guide image in deterministic way and then ciphering text, the second step related to the constructing fast convolution neural network and used this network in detecting decided objects like cars, persons, animals,….. and then determined the coordinates of the points of the bounding box that cover the object after that in the third step a suitable algorithm proposed for hiding encrypted text into the image out of the bounding box in calculated position which is depend on the suitable metrics (edge strong) to decide the accepted position for hiding the bits of the message. The results of hiding text into suitable cover image have good values from the accepted range of the peak signal to noise ratio as well as any person cannot be recognized any difference between input and output images.

Keywords: steganography, convolution neural network, key exchange, edge detection, stream cipher.

I. Introduction

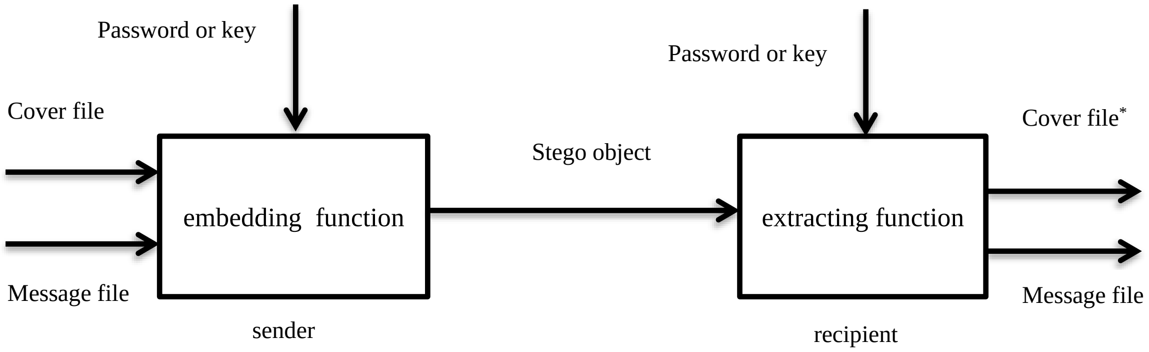
A. Steganography

Information hiding is the process of producing protected information into suitable cover for the purpose of security, many algorithms will be suggested for ensuring the security of the important and crucial information, these algorithms can be divided into[1]

1- watermarking algorithm.
2- steganography algorithm.

Steganography algorithms suggest suitable and calculated path for hiding information so this path can be converted in the other side for the purpose of extracting the hidden information by applying the same and opposite direction so, the goal of Steganography process is hiding secret messages inside other suitable covers in a special way that does not permit any person to even decide that there is a secret information present in this cover [2]. Hiding information into a media requires following elements [3]

- ✓ The cover file that will contain the message.
- ✓ The important and secret message (text(plain or cipher), audio, video and image).
- ✓ The embedding function.
- ✓ The extracting function which is the inverse of the embedding function [5].
- ✓ A suitable password or key used in arranging embedding and extracting operation[4] as illustrated in figure (1).



Figure(1) General steganography system

There are many usage of steganography process

- ✓ Send secret information to its destination.
- ✓ Steganography process used in constructing watermarking process.
- ✓ storing information on a general location[3].
- ✓ E-commerce depend on using protected users by password and username embedded into suitable images by using steganography[5].
- ✓ Simplify Key exchange process.

✓ Steganography simplify the process of transforming sensitive data with the existence of eavesdroppers without knowing data has been passed [4].

Steganography techniques can be classified by many factors as follow

1- Depending on the password or key:- the type of the key classify steganography algorithms into

✓ Pure steganography:- in this method of steganography the embedding process start by first position of the cover file and stopped when the message file is finished without taking in account any limitations or features to select some places rather than other places [6].

✓ Secret key steganography:- in this method of steganography the embedding process depend on secret key that is known for the two parts of hiding information. This secret key can be words or features discovered from the cover and does not change after hiding information for the purpose of never effecting the extracting process after exchanging these features. The secret key can be used for deciding the position for hiding information or for deciding the amount of message bits that will be hidden in the specific position. In this methods the same key used in hiding information in the cover file and in extracting the same information from the stego object file[7].

✓ Public key steganography:- in this method the embedding and extracting processes depend on two related keys (private and public) [8], each party of steganography has public and private keys where the public key is known and spread through the networks and private key is secret so the sender use the public key of the recipient in embedding process of the message bits into the selected cover and send them to the second party which used its private key for extracting information[9].

2- Depending on the types of the cover file:- the type of the cover file can be used in classifying steganography algorithms into

✓ Text steganography:- in this method the cover file is text file (.txt, .docx, .pdf,…) and the massage file can be in any format. The capacity of hiding information here in limited and the change in the cover file is noticeable and the embedding algorithm rely on some features like font size, spaces between letters, spaces between words, spaces between lines, spaces between paragraphs, errors in writing specific letters,…….[10].

✓ Audio steganography:- in this method of steganography the cover file is audio file in any formats and the message file can be in any format, in this type of steganography the capacity for hiding wanted messages is greater than text steganography but the audio file is too sensitive to noise so the embedding steganography is limited because of this factor [11].

✓ Image steganography:- in this method of steganography the cover file is image in any format so this type is much popular than other types because of the popularity of the image files as well as this type has good capacity in hiding large files without any visual effects in the stego object [12], there are many suggested algorithms to implement image steganography each one of them has its special methodology in hiding bits in random places with random number of bits from different pixels [13].

✓ Video steganography:- in this type of steganography the cover file is video file (image file +audio file) the capacity for hiding information here is too great and have advantages of images file as well as audio file in one file [14].

3- Depending on the approach of hiding information:- there are many types for hiding information like

✓ Insertion steganography:- in this type of steganography the secret information (message) hidden in some places in the cover file not readable by the known programs for reading file in specific formats like after of EOF, some places of the header, ……. , so the cover file not exchange and the size of the stego file comparing to its type and content represent a negative index for existence hiding information in the stego file[15].

✓ Substitution steganography:- in this type of steganography the secret information (message) hidden by substitute bits of message instead of bits of cover file so the contents of cover file will be changed but in accepted range that does not noticeable by the viewer of the stego file even if the examiner see the source cover file, there are some metrics for deciding the efficiency of steganography algorithms like peak signal noise ratio[10].

✓ Generation steganography:- in this type of steganography the sender create file in any type consist of some decided features arranged in deterministic fashion so each feature represent specific bits [15].

4- Depending on the domain of hiding information:- according to this feature, steganography methods can be classified into

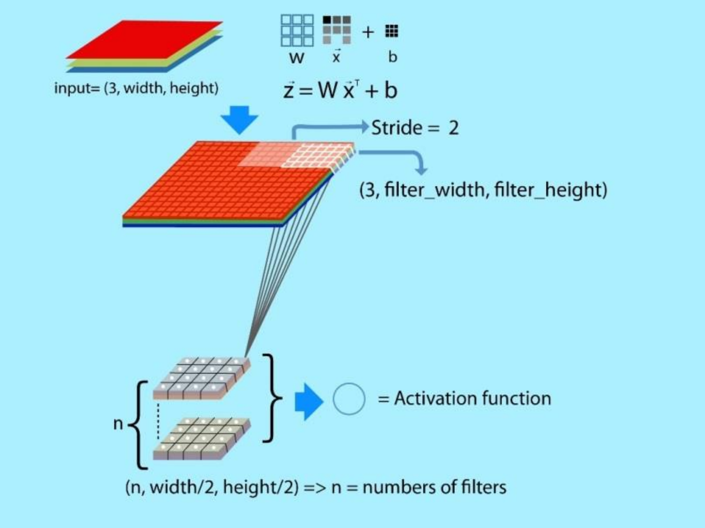
✓ Special domain steganography:- in this type of steganography the process of hiding message in the cover done in special domain, and applying hiding algorithm on the source cover file [7].

✓ DCT domain steganography:- in this type of steganography the process of hiding information in the cover done after applying Discrete Cosine Transform, and hiding message bits in the coefficients of DCT [16].

✓ Wavelet domain Steganography:- in this type of steganography the process of hiding information in the cover done after applying Wavelet Transform, and hiding message bits in the coefficients of regions (LL, LH, HL, HH) [17].

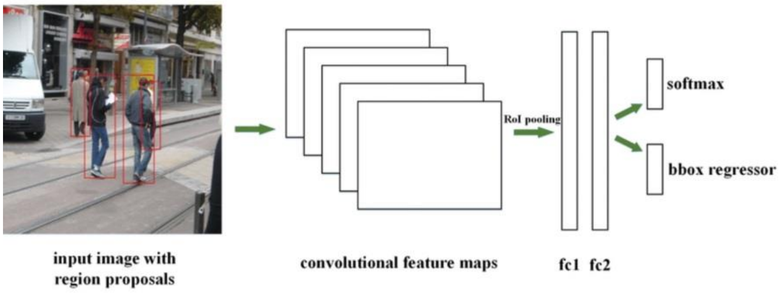
B. Convolution Neural Network

The main goal of machine learning is to finding suitable technique for detecting recognizing wanted objects in a picture. In the past the researchers in recognizing objects having the selection of effective object characteristics on the basis of human knowledge the detection of items depending on their features of that objects, such as convolution neural network as illustrated in figure (2) [18].


input= (3, width, height)
W
x
+
b
$\vec{z} = W\,\vec{x}^{T} + b$
Stride = 2
(3, filter_width, filter_height)
n
= Activation function
(n, width/2, height/2) => n = numbers of filters

Figure(2) convolutional neural network

many of models will be suggested some of them with accepted performance. Many techniques of deep learning for the purpose of identification and recognition objects are available, such as (Region, fast region and faster region) convolution neural network, versions (1 to 6) YOLO, and the versions of SSD [19], two important steps summarize the R-CNN for detecting objects, first step uses uniform Search (Selective) for the purpose of locating specific number of boxes that related to the wanted object in the input images. Then, the second step perform classifying process for each bounding boxes by using convolutional neural network as illustrated in figure (3) [19].



Figure(3) region convolution neural network

The YOLO network is simple identification algorithm speedy by adding some additional layers into pre-trained convolution-NN for the purpose of detecting wanted object in the input images, as well as YOLO network is very suitable for solving identification problem since it is more accurate as illustrated in figure (4).

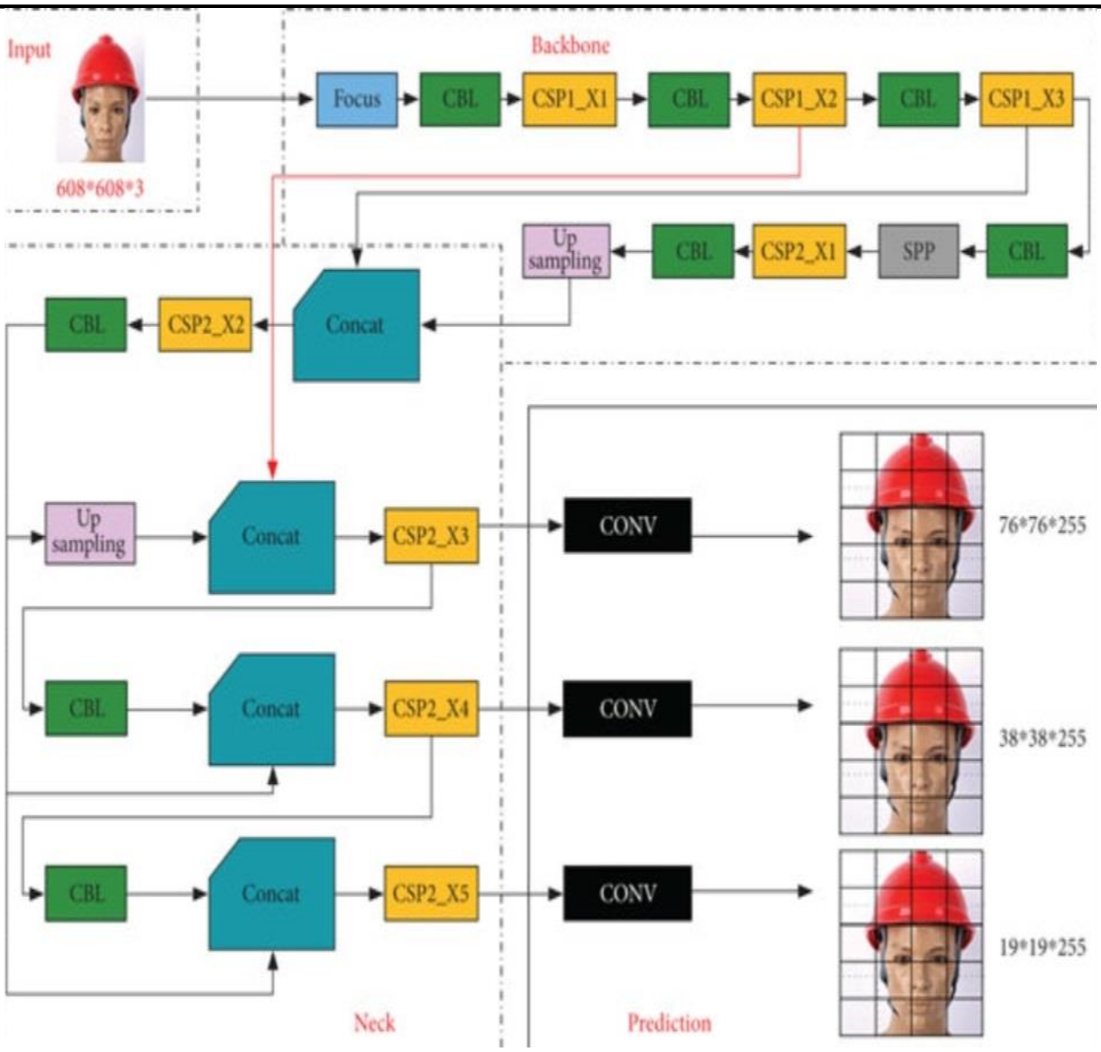


Figure (4) Yolo V5 architecture

C. Stream Cipher and key exchange

stream cipher (SC) traditionally use binary key with long equal or greater than text because of security goals, stream key must be as long enough to improve the wanted requirements of the security. The general idea of SC was similar to the One-time Pad. The SC method based on applying XOR (⊕) gate between bits of the message and related key bits [21], So stream cipher equation can be written as

$$E :\{ 0, 1\} \times \{0, 1\} \rightarrow \{0, 1\}, (m, k) \rightarrow m \oplus k \qquad \dots (1)$$

Where m is the message.
K is the key.
plaintext, key stream and ciphertext bits are in the space {0, 1}.

Generally one of the most crucial step in SC security is the process of providing the key to the parties of communication and the succeeding of any SC method related to the strength of the key. The general structure of stream ciphers can be illustrated in figure (1)[22].

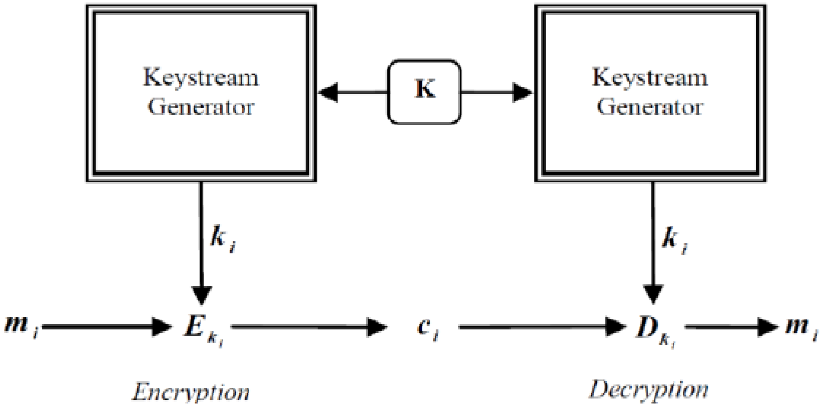


Figure (5) SC structure

One of the most important state in the cryptography system is key exchange problem so many searches try to solve this problem by suggest some algorithms or managing this process in secure but simple fashion [23].

II. Related work

1- **Pin Wu et.al. (2018) in [24]** combines perfect deep convolutional NN strategies with steganography method for embedding image in image. The proposed method hiding images with the same number of pixels with a hiding rate of 98.2% (bits for each pixel) of 23.57 by changing only 0.76% of the file of the cover image on average. The proposed method simply learns by applying end-to-end process of mappings between the selected image as a cover and the embedded image in party one and between pixels of the stego object image and of the hidden image. The proposed system as well as show that the message image with specific payload capacity, is still robust to some stego analysis methods like statistical method.

2- **Eman S. Harba et.al. (2021) in [25]** proposed a model of hiding video or still image within cover video file by applying training and essentially using convolutional neural networks (CNN). In the proposed system, two essential goals can be performed for any hiding methods which are:

i- raising security, this state will be achieved in the proposed system by randomized weights and network architecture. so, the way used by the network for hiding the information is protected and unknown by person does not have the exact weights.

ii- increasing the capacity of the cover, and this process will be achieved by making decisions to discover better position in the cover that produce more size in hiding process.

Search used specific square images (45000) from the dataset "ImageNet" with width equal to255 for the purpose of training.

3- **Aarsh Bararia(2021) in [26]** proposed and implement a technique for data securing process by using Steganography and Cryptography methods for giving sound security method consist of multiple layers of security and helping to carrying important information securely. the message encrypted by using AES technique then the encrypted text embedding within the decided image pixels after that the stego object image encrypted within another cover using process of multi-image steganography in merging with Deep NN. The system using cover image from specific dataset and then training the network for the purpose of hiding first stego image into the second cover image.

4- **Fariha Aiman et.al. (2019) in [27]** focused on video steganography By hiding message Video within suitable and selected cover video. Firstly the residual of the message video and the cover video is determined because embedding the residual file is very easy than embedding source video. The system exploit the advantages of deep convolutional NN strategies. The suggested model is efficient if it is compared with other method as all results of the proposed system shown.

5- **Anupama A Kori (2021) in [28]** In this search, the message is a secret image that will be embedded by suitable cover image which consist of embedding process of the message and the stego image is separated from the cover file image which involves the process of recovery suitable information. many deep learning models like

i- Preparation Network,

ii- Hiding Network and

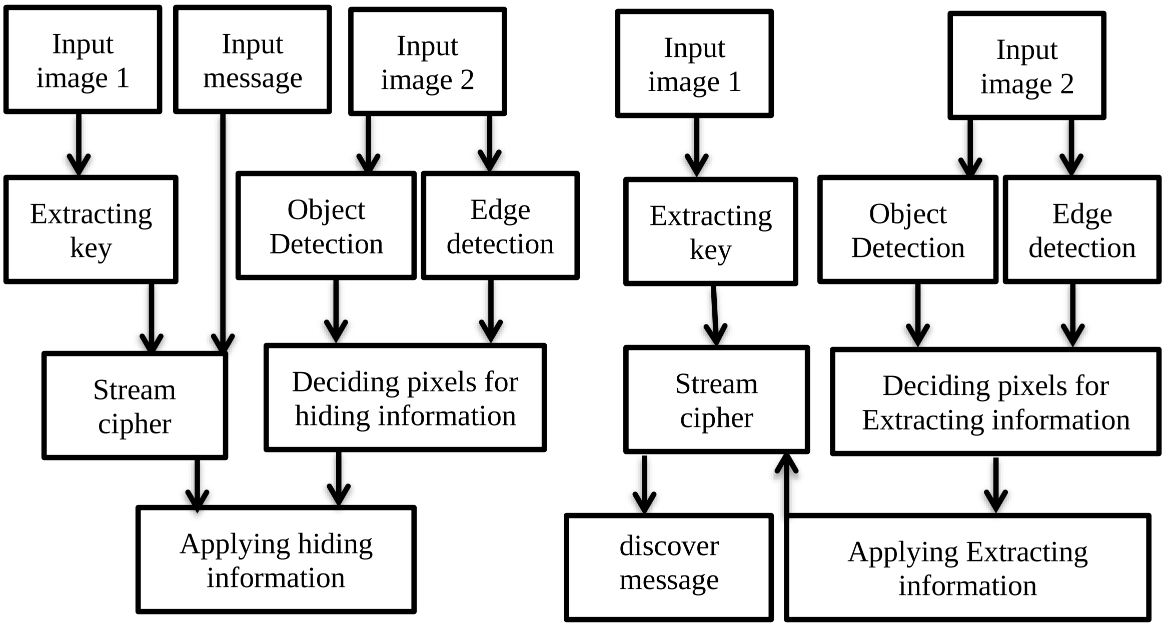
iii- Reveal Network

Will be designed to perform as a dual and trained simultaneously on random images that selected from proposed Database and the system efficiency is good on natural images from different sources. The system embedding message image-into-cover image by exploiting advantages of deep convolutional NN techniques**.**

6- **Digvijay Pandey et.al. (2021) in [29]** a covert communication and extracting special data techniques depend on hiding process and the process of compressing image is built by using suitable deep NN. the input to the proposed system is textual image and the cover image pre-processed firstly, then the covert images are performed and hidden into the least significant bit of the pixel of the cover image. After that, stego object will be compressed for the purpose of saving storage capacity at the embedding end. finally, the extracting end will receive this stego object. So, the process of steganography as well as compression process converted in reverse fashion at the extracting end. The proposed system has many problems that make it an efficient one compared to others. choosing perfect hiding method and effective compression method is the most effective part in constructing the proposed system which integrates methods of hiding image achieves best efficacy related to peak signal-to-noise ratio as a metric.

III. The proposed system

The proposed system can be divided into two stages one for hiding information and the other for extracting information each stage contain three main steps each one of these step contain many processes inside it as illustrated in figure(6)



a-hiding stage b-extracting stage

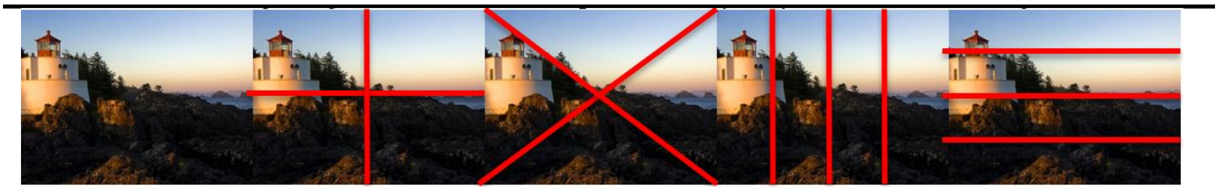
Figure(6) block diagram of the proposed system

A- Hiding stage:- this stage start by entering two images one for extracting key and the other for hiding input message by applying the following steps

1- Key extracting step:- this step consist of the following process

a- Input suitable image and secret message.

b- Dividing image into four different parts in many ways as illustrated in figure (7)



a-input image b-first way c-second way d-third way e-fourth way

Figure (7) dividing image into four parts

c- calculate number of pixel for each color value:- this process repeated for each way of the four ways as well as for each band(red, green and blue) as illustrated in table (1) for red band and the same process repeated for green and blue band.

Table (1) key constructing for red band

Way no.	Way 1					Way2					Way3					Way4				
Pixel val.	0	1	2	..	255	0	1	2	..	255	0	1	2	..	255	0	1	2	..	255
No. of pixel	5	100	0		1	7	2	11		22	1	7	9		101	5	8	3		26
Binary	101	1100100	0	..	1	111	10	1011	..	10110	1	111	1001	..	1100101	101	1000	11	..	11010
Key	10111001000............1111101011...........1011011111001............1100101101100011............11010																			

Then the key will be constructed by merging keys for red band by taking all four ways then red band then blue band.

d- Ciphering secret message by converting it to binary representation and applying Xor gate between message bits and key bits to produce encrypted message that will be used in the next steps for hiding into suitable cover.

2- Object detect and identified by Yolo network and deciding region of Interest step:- this step consist of many processes for the purpose of finding ROI as follow

a- Input suitable image to pre trained Yolo network for detecting and identifying the existence of cars in the image as illustrated in figure (8).

Figure (8) Detecting car in the input image b- The bounding box that will be drown by the network can be taken as region 1 and the rest of images consider as region 2 as illustrated in figure (9)

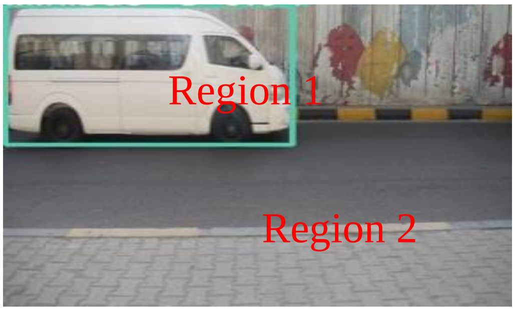


Figure (9) dividing image into regions

c- Applying Sobel horizontal and vertical edge detection then calculate total edge in each pixel

-1	-1	-1
0	0	0
1	1	1

a-Vertical

-1	0	1
-1	0	1
-1	0	1

b-Horizontal

Figure (10) Sobel edge detector

The result of applying Sobel edge detector can be Explained in figure (11)

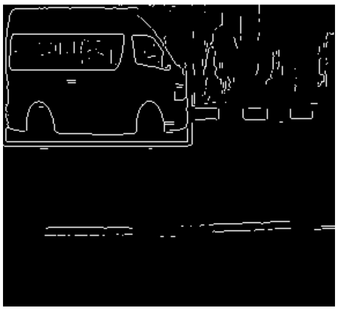


Figure (11) Sobel edge detection (red band)

d- Calculate mean value for edge values in region 1 and in region 2

e- If mean edge in region 1 greater than mean edge in region 2 then region 1 consider ROI otherwise region 2 consider ROI

3- Discovering pixels for hiding encrypted message and hiding information step. In this process the ROI will be scanned from top to bottom and from left to right to arrange edge pixel from high to low value and deciding number of bits to be hidden in each edge pixel as follow

$$X = MAX_{\text{edgevalue}} - MIN_{\text{edgevalue}} \qquad \ldots(2)$$

$$\begin{array}{lll} & PIXEL_{\text{edgevalue}} \geq \frac{X}{2} & \textit{Hide in 3 bits} \\ if & \frac{X}{2} > PIXEL_{\text{edgevalue}} \geq \frac{X}{4} & \textit{Hide in 2 bits} \qquad \ldots(3) \\ & PIXEL_{\text{edgevalue}} < \frac{X}{4} & \textit{Hide in 1 bit} \end{array}$$

The message bits are embedding in image pixel according to decided number of bits for each pixel and by scanning pixels according to the consider feature (the strength of edge in each pixel in the input image)

B- Extracting stage:- in this stage the same steps and processes will be implemented on input image 1 for extracting the same key as in hiding stage as well as stego object to discover ROI in inverse fashion applied in the first stage as illustrated in figure (6).

Here essential problem must be mentioned where all calculations in ROI must avoid first three bits because these bits will be changed in hiding algorithm and all calculation become wrong if three LSB will be consider.

IV. Results

When the proposed system will be applied on many images and messages the final stego image will not be recognized that has any effect or any distortion in any pixel compared with its neighbor as improved by efficiency metric peak signal to noise ratio (PSNR)

$$PSNR = 10\,log_{10}\frac{(l-1)^2}{\frac{1}{N^2}\sum_{r=0}^{n-1}\sum_{c=0}^{n-1}[g(r,c)-I(r,c)]^2} \qquad ...(4)$$

Where

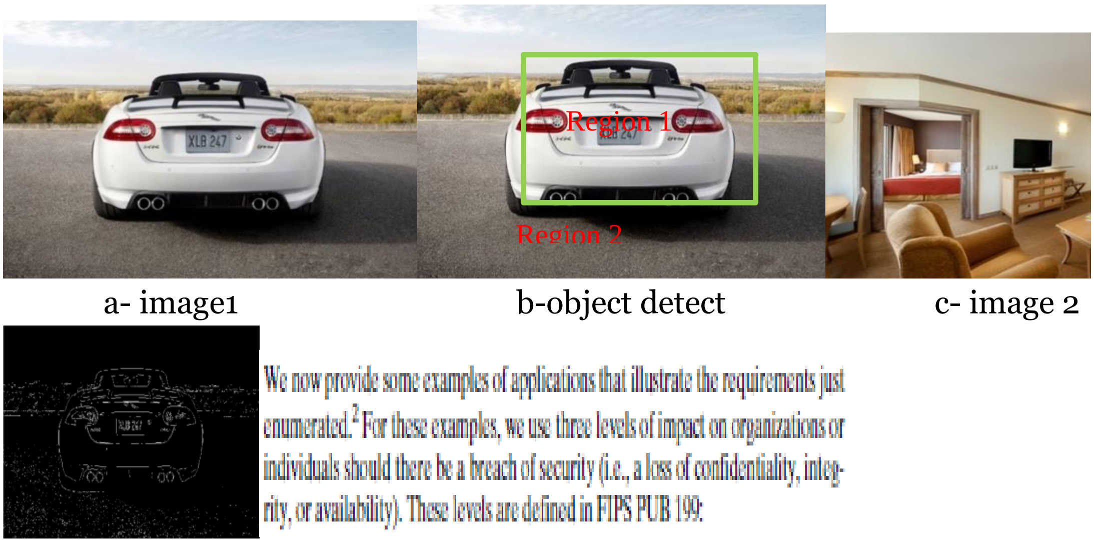
N= number of columns or rows in the image.

L= number of colors in the image.

G(r,c) is stego image.

I(r,c) is original image.

Test 1



We now provide some examples of applications that illustrate the requirements just enumerated.[2] For these examples, we use three levels of impact on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability). These levels are defined in FIPS PUB 199:

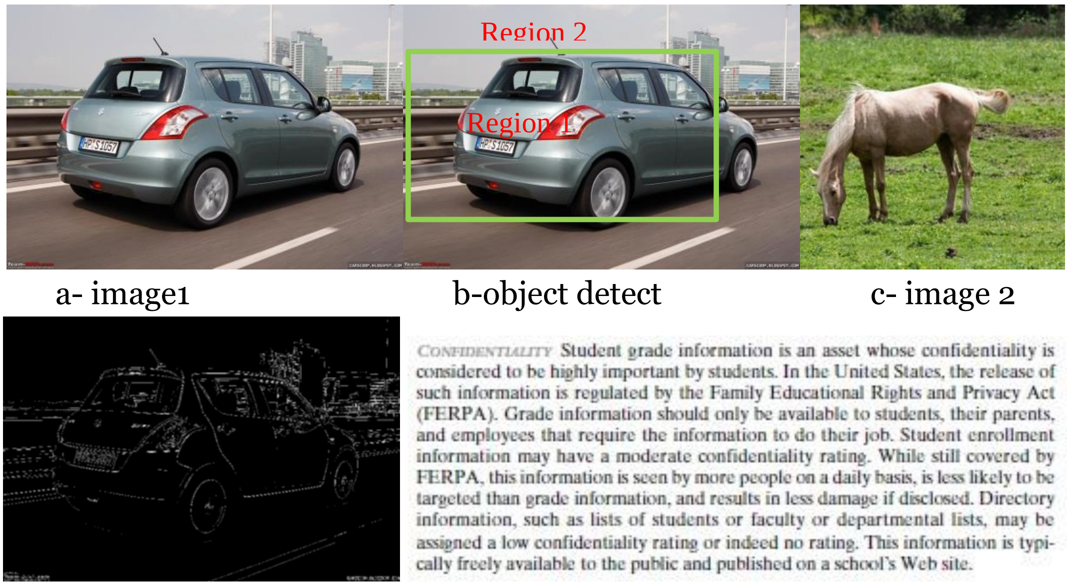
a- image1 b-object detect c- image 2

d- edge image e-message

Figure (12) test 1 results

In test1 image 1 used for hiding information after finding edge image and decide region 2 for hiding information according to suggested metric and image 2 used for extracting secret key for encryption message. The PSNR for test 1 between stego-image and input image is **95.35**

Test 2



CONFIDENTIALITY Student grade information is an asset whose confidentiality is considered to be highly important by students. In the United States, the release of such information is regulated by the Family Educational Rights and Privacy Act (FERPA). Grade information should only be available to students, their parents, and employees that require the information to do their job. Student enrollment information may have a moderate confidentiality rating. While still covered by FERPA, this information is seen by more people on a daily basis, is less likely to be targeted than grade information, and results in less damage if disclosed. Directory information, such as lists of students or faculty or departmental lists, may be assigned a low confidentiality rating or indeed no rating. This information is typically freely available to the public and published on a school's Web site.

a- image1 b-object detect c- image 2

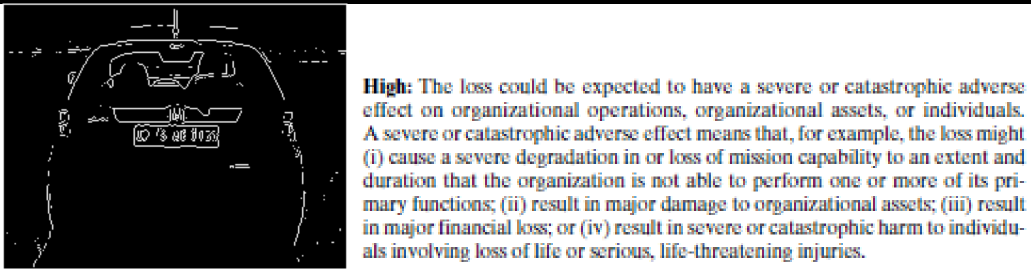
d- edge image e-message

Figure (13) test 2 results

In test 2 image 1 used for hiding information after finding edge image and decide region 1 for hiding information according to suggested metric and image 2 used for extracting secret key for encryption message. The PSNR for test 2 between stego-image and input image is **84.9**

Test 3

a- image1 b-object detect c- image 2



High: The loss could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. A severe or catastrophic adverse effect means that, for example, the loss might (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious, life-threatening injuries.

d- edge image e-message

Figure (13) test 3 results

In test3 image 1 used for hiding information after finding edge image and decide region 1 for hiding information according to suggested metric and image 2 used for extracting secret key for encryption message. The PSNR for test 3 between stego-image and input image is **96.6**

V. Conclusions

Steganography methods depend on many factors for the purpose of deciding the efficiency of the each algorithm, the proposed system work by deciding pixels for hiding bits depending on the value of edge in this pixel and as known that the pixel with high edge value is the place differ from its neighbors so this pixel is suitable for hiding more bits compared with pixel has low edge value that reflects small differ from its neighbors so this pixel is not suitable for hiding message bits. The discovering the place of hiding information in the cover image is crucial step in any hiding system, so discovering information related to the places of the image that will be used for hiding information depend on the bounding boxes that will be drown by Yolo network, this mean that the secret key that will be used by hiding information algorithm depending on the input image and this key change if the input image changed and the key change for each hiding process. ciphering secret text by using stream cipher method after discovering secret key from the input image make the process of key exchange simple for cryptographic system parties as well as very difficult or impossible for any other unwanted person. The results of the proposed system reflect the simplicity in ciphering and hiding information but very difficult in analysis the stego-image that transform from the sender station to the recipient station via network media.

References

[1] Sadoon Hussein Abdullah, " Steganography Methods and some application (The hidden Secret data in Image)", Biology Depart , Science Collage , University of Mosul , Mosul , Iraq,2009.

[2] Ghadeer Fahad Alfuhaid, " STEGANOGRAPHY USING IMAGES", Kingdom of Saudi Arabia, Majmaah University,2018.

[3] Nidhal El Abbadi, Elaf J Al Taee, and Zainalabideen Abdulsamad,"Improve image deblurring", 2018 International Conference on Innovative Trends in Computer Engineering (ITCE), 25–30 (2018).

[4] Arvind Kumar and Km. Pooja, " Steganography- A Data Hiding Technique", International Journal of Computer Applications (0975 – 8887), Volume 9– No.7, November 2010.

[5] Darko Trifunović, " Digital steganography in terrorist networks", XLII International Symposium on Operations Research,2015,Vol.V(1).

[6] Stuti Goel, Arun Rana & Manpreet Kaur, " A Review of Comparison Techniques of Image Steganography", Global Journal of Computer Science and Technology Graphics & Vision, Volume 13 Issue 4 Version 1.0 Year 2013.

[7] Baneen Qasem et.al., " A Review and Comparison for Audio Steganography Techniques Based on Voice over Internet Protocol", Kerbala Journal for Engineering Science Vol. 01, No. 02 (2021) ISSN: 2709-6718.

[8] Nesir Rasool Mahmood, Ali Abdul Azeez and Zahraa Nesir Rasool, " Public Key Steganography", International Journal of Computer Applications (0975 – 8887) Volume 100– No.8, August 2014.

[9] Alexis Camacho et.al., " Public Key Neural Linguistic Steganography", 2020.

[10] Suhad Malallah Kadhem, " Text Steganography Method Based On Modified Run Length Encoding", Iraqi Journal of Science, 2016, Vol. 57, No.3C, pp:2338-2347.

[11] Megha and Mahesh singh, " Methods of Audio Steganography", International Journal of Engineering and Management Research, Volume-4, Issue-3, June-2014, ISSN No.: 2250-0758.

[12] Sura I. Mohammed Ali, " A Review of Image Steganography Techniques", Journal of University of Babylon for Pure and Applied Sciences, Vol. (28), No. (3): 2020. Online ISSN: 2312-8135.

[13] Gandharba Swain, " Digital image steganography using variable length group of bits substitution", International Conference on Computational Modeling and Security (CMS 2016).

[14] Nidhal El Abbadi, and Elaf J Al Taee,"An efficient storage format for large sparse matrices based on quadtree", International Journal of Computer Applications, 2014, 105, 25–30.

[15] Dr.Manjula G R and Sushma R B, " Video Steganography: A Survey of techniques and methodologies", International Conference on Smart Data Intelligence (ICSMDI 2021).

[16] Adel Almohammad, " Steganography-Based Secret and Reliable Communications: Improving Steganographic Capacity and Imperceptibility", Brunel University, August, 2010.

[17] Devadath C Prabhu, et.al., "Multiple Image Steganography using LSB-DCT Technique", International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Published by, www.ijert.org ICACT – 2016.

[18] Enas Muzaffer Jamel, " Image Steganography Based on Wavelet Transform and Histogram Modification", Ibn Al-Haitham Jour. for Pure & Appl. Sci. 33 (1) 2020.

[19] Asst. Prof. Dr. Ali Abdulazeez Mohammedbaqer Qazzaz and MSc. student Ahmed Younus Abdulkadhim, " Comparison study about Car Detection and Type Recognition Techniques", International Journal of Mechanical Engineering, ISSN: 0974-5823 Vol. 7 No. 2 February, 2022.

[20] Asst. Prof. Dr. Ali Abdulazeez Mohammedbaqer Qazzaz and MSc. student Ahmed Younus Abdulkadhim, " Car Detection and Features Identification Based on YOLOV5", International Journal of Mechanical Engineering, ISSN: 0974-5823 Vol. 7 No. 2 February, 2022.

[21] Shakir Mahmood Abas, " A YOLO and Convolutional Neural Network for the Detection and Classification of Leukocytes in Leukemia", Duhok Polytechnic University , Kurdistan Region – Iraq, 2021.

[22] Heri Nurdiyanto, Robbi Rahim and Nur Wulan, " Symmetric Stream Cipher using Triple Transposition Key Method and Base64 Algorithm for Security Improvement", International Conference on Information and Communication Technology (IconICT), IOP Conf. Series: Journal of Physics: Conf. Series 930 (2017) 012005.

[23] Zainalabideen Abdullasamd Rasheed and Ali Abdul Azeez Mohammad Baker, " A Novel Method of Generating (Stream Cipher) Keys for Secure Communication", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 1, Ver. I (Jan – Feb. 2015).

[24] Dakshita Khurana, " Stream Cipher Examples, Block Cipher Introduction", University of Illinois, Urbana Champaign, September 1, 2020.

[25] Pin Wu, Yang Yang and Xiaoqiang Li, " StegNet: Mega Image Steganography Capacity with Deep Convolutional Network", arXiv:1806.06357v1 [cs.MM] 17 Jun 2018.

[26] Eman S. Harba, Hind S. Harba, Inas Ali Abdulmunem, " Advanced Intelligent Data Hiding Using Video Stego and Convolutional Neural Networks", Baghdad Science Journal P-ISSN: 2078-8665 Published Online First: April 2021.

[27] Aarsh Bararia, " Image Steganography on Cryptographic text using Neural Networks", School of Computing National College of Ireland, 2021.

[28] Fariha Aiman and G. R. Manjula, " Video Steganography using Convolutional Neural Network and Temporal Residual Method", International Journal of Computer Applications (0975 – 8887) Volume 178 – No. 46, September 2019.

[29] Anupama A Kori, P. I. Basarkod and Veena. K. N, "Deep Learning Technique In Steganography With Multimedia Network Security For Health Care", International

Journal of Creative Research Thoughts (IJCRT), 2021 IJCRT | Volume 9, Issue 7 July 2021 | ISSN: 2320-2882.

[30] Digvijay Pandey et.al., " Secret data transmission using advance steganography and image compression", Int. J. Nonlinear Anal. Appl. Volume 12, Special Issue, Winter and Spring 2021, 1243-1257.

[31] Elaf J. Al Taee and Zainalabideen Abdulsamad,"A New Approach for Fingerprint Authentication in Biometric Systems Using BRISK Algorithm" ,Int. J. Adv. Sci. Eng. Inf. Technol., vol. 8, no. 5, pp. 1941–1947, 2018.