Partial image encryption with automatic selection using YOLO

***A Thesis submitted to the Faculty of Engineering & Technology, Jadavpur University in partial fulfillment of the requirements for the Degree of Master of Engineering in Software Engineering****.*

***2020-21 ME(SWE) 2nd Year Thesis Paper***

***Master of Engineering Degree 2020-2022***

***in***

***Software Engineering***

***under***

***Jadavpur University***

*BY*

***SOUJANNYA ROY***

*(ROLL NO: 002011002022)*

*Examination Roll No:*

*Under the Guidance and Supervision of:*

***DR. BIBHAS CHANDRA DHARA***

*Professor*

*Department of Information Technology*

*Faculty of Engineering and Technology*

*Jadavpur University (Salt Lake Campus)*

*Kolkata- 700106*

**JADAVPUR UNIVERSITY**

**DEPARTMENT OF INFORMATION TECHNOLOGY**

**FACULTY OF ENGINEERING & TECHNOLOGY**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Certificate of Recommendation**

I hereby recommend the thesis, entitled, **“Partial Image Encryption”**, prepared under my guidance by **Soujannya Roy** (Roll Number:002011002022), be accepted in partial fulfillment of the requirements for the degree of **Master of Engineering** in **Software Engineering** from the **Department of Information Technology** of **Jadavpur University**.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**DR. BIBHAS CHANDRA DHARA**

Department of Information Technology

Jadavpur University, Kolkata

Countersigned by:

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

|  |  |
| --- | --- |
| **Head of the Department**  Department of Information Technology  Jadavpur University, Kolkata | **Dean**  Faculty of Engineering & Technology Jadavpur University, Kolkata |

**Jadavpur University**

**Faculty of Engineering & Technology**

**Department of Information Technology**

**Certificate of Approval**

***The thesis at this instance is hereby approved as a creditable study of an engineering subject carried out and presented in a manner satisfactory to warrant its acceptance as a prerequisite to the degree for which it has been submitted. It is understood that by this approval the undersigned does not necessarily endorse or approve any statement made, opinion expressed, or conclusion drawn therein, but approve this thesis for the purpose for which it is submitted.***

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Signature of Examiner Signature of Supervisors**

**Faculty of Engineering & Technology**

***Declaration of Originality and Compliance of Academic Ethics***

*I hereby declare that this thesis contains literature survey and original research work by the undersigned candidate, as a part of my Master of Software Engineering studies.*

*All information in this document has been obtained and presented in accordance with academic rules and ethical conduct.*

*I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Signature with date)

Soujannya Roy

Class Roll Number: 002011002022

ME in Software Engineering (6 Sems) JADAVPUR UNIVERSITY

# **Acknowledgements**

I would like to express my sincere gratitude to my supervisor PROF. BIBHAS CHANDRA DHARA for his continuous support and motivation in fueling the pursuance of carrying out this thesis project. Without his guidance and persistent encouragement, this work would not have been possible. He has been a tremendous mentor for us throughout this academic journey. Many of his academic advises about our career growth have been priceless.

I would like to convey sincere gratitude to him for providing us constant inspiration to stand firm against several setbacks throughout the course. Additionally, I would like to thank all the technical, non-technical and office staffs of our department for extending facilitating cooperation wherever required. We also express gratitude to all our friends in the department for providing the friendly environment to work on the project work.

Finally, I would like to thank everybody who has provided assistance, in whatever little form, towards successful realization of this project but with an apology that we could not mention everybody’s name individually.

Place: Jadavpur University, Salt Lake Campus

Date:

# LIST OF FIGURES

[Figure 1 : High Level Overview of Partial Image Encryption 1](#_Toc105093211)

[Figure 2: Image 3](#_Toc105093212)

[Figure 3: Zoomed in image showing pixels 3](#_Toc105093213)

[Figure 4: Image as 2D matrix 3](#_Toc105093214)

[Figure 5: Unsafe internet channel due to hackers 4](#_Toc105093215)

[Figure 6: Security needed in case of Military Image transaction 4](#_Toc105093216)

[Figure 7: Map images used for encryption 5](#_Toc105093217)

[Figure 8: Process of detection 6](#_Toc105093218)

[Figure 9: Different ways of operating on the images (automatic) 7](#_Toc105093219)

[Figure 10: Image Classification 8](#_Toc105093220)

[Figure 11: Object Detection 8](#_Toc105093221)

[Figure 12: Traditional versus DL workflow 9](#_Toc105093222)

[Figure 13: CNN network 10](#_Toc105093223)

[Figure 14: Steps in working of CNN 10](#_Toc105093224)

[Figure 15: Faster RCNN block diagram 11](#_Toc105093225)

[Figure 16: Output from Mask RCNN 12](#_Toc105093226)

[Figure 17: Breakdown of SSD 13](#_Toc105093227)

[Figure 18: SSD flow diagram 13](#_Toc105093228)

[Figure 19: Output with SSD 14](#_Toc105093229)

[Figure 20: YOLO breakdown 15](#_Toc105093230)

[Figure 21: YOLO native pytorch implementaion 15](#_Toc105093231)

[Figure 22: Output with YOLO 16](#_Toc105093232)

[Figure 23: Complete flowchart 18](#_Toc105093233)

[Figure 24: Object detection flowchart 19](#_Toc105093234)

[Figure 25: Encryption flowchart 20](#_Toc105093235)

[Figure 26: Encryption with RSA 21](#_Toc105093236)

[Figure 27: Sending flowchart 22](#_Toc105093237)

[Figure 28: Decryption using Substitution 23](#_Toc105093238)

[Figure 29: Decryption with RSA 24](#_Toc105093239)

[Figure 30: Input Image 25](#_Toc105093240)

[Figure 31: Object 26](#_Toc105093241)

[Figure 32: Object chosen 26](#_Toc105093242)

[Figure 33: (a) Encrypted with substitution (b) Encrypted with RSA 27](#_Toc105093243)

[Figure 34. (a) Dog Original Image and (b) Partially encrypted image 27](#_Toc105093244)

[Figure 35: Result analysis table using NPCR and UACI 28](#_Toc105093245)

# LIST OF ABBREVIATION

|  |  |
| --- | --- |
| YOLO | You Only Look Once |
| ROI | Region Of Interest |
| RSA | Rivest–Shamir–Adleman |
| DL | Deep Learning |
| SSD | Single Shot Multibox Detect |
| CNN | Convolutional Neural Network |
| RCNN | Region based Convolutional Neural Network |
| RPN | Region Proposal Network |

# TABLE OF CONTENTS

[**Acknowledgements** iv](#_Toc105889232)

[LIST OF FIGURES v](#_Toc105889233)

[LIST OF ABBREVIATION vi](#_Toc105889234)

[TABLE OF CONTENTS vii](#_Toc105889235)

[Abstract ix](#_Toc105889236)

[1.1 Objective of the work 1](#_Toc105889237)

[1.2 Scope of the thesis 2](#_Toc105889238)

[1.3 Motivation of the work 2](#_Toc105889239)

[1.4 Organization of the thesis 2](#_Toc105889240)

[2. Methods and process 3](#_Toc105889241)

[2.1 Introduction 3](#_Toc105889242)

[2.2 Requirements of partial image encryption 4](#_Toc105889243)

[2.3 Applications 4](#_Toc105889244)

[2.4 Overview of the process 5](#_Toc105889245)

[2.4.1 Selecting the significant data 5](#_Toc105889246)

[2.4.2 Encryption of selected data 5](#_Toc105889247)

[2.5 Auto selection of area of interest prior to partial image encryption 6](#_Toc105889248)

[2.5.1 Introduction 6](#_Toc105889249)

[2.5.2 Choosing method for auto selection 7](#_Toc105889250)

[2.5.3 Categories for neural networks for object detection 8](#_Toc105889251)

[3. Proposed method 14](#_Toc105889252)

[3.1 Overview of the proposed framework 14](#_Toc105889253)

[3.2 Technologies used 15](#_Toc105889254)

[3.3 Comparative study 15](#_Toc105889255)

[3.4 Flowchart 16](#_Toc105889256)

[4. Experimental results and discussion 20](#_Toc105889257)

[4.1 Experimental setup 20](#_Toc105889258)

[4.2 Implementation algorithm 20](#_Toc105889259)

[4.3 Results 20](#_Toc105889260)

[5. Conclusion 23](#_Toc105889261)

[6. References 24](#_Toc105889262)

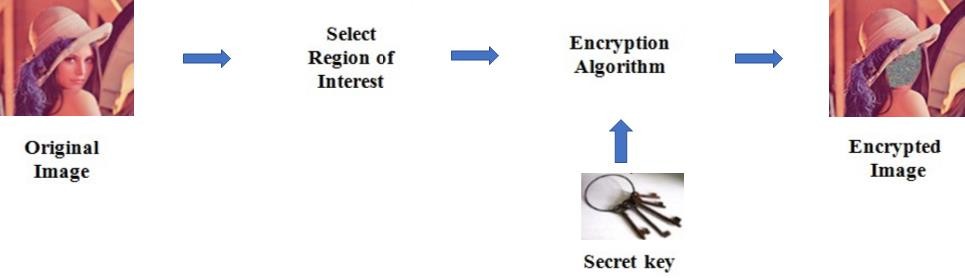
Partial image encryption with automatic selection using YOLO

## Abstract

In recent times, with the increase in multimedia applications, the need for secured transfer of data has increased too. Some examples can include, military image database, satellite images, telecommunication and confidential video conferencing, medicinal images, etc. The channel through which these data passes can be insecure, so the requirement for safe transfer of messages is very important at these times. Normal method can’t be used to encrypt images because of the image data having size which is a lot bigger than data in text form. That is where Partial Image Encryption or Selective Image Encryption comes into picture. When we think about medical and satellite application, even small quantity of encryption can secure the whole image, we don’t need to encrypt the whole image. In this paper we are going to talk about partial encryption after the automatic selection of area of interest using YOLO algorithm of object detection and have a comparative study between encrypting it using RSA and our proposed substitution method.

1. Introduction

From the name we understand that, not the entire data, but only a selected part of the data is being encrypted. This can, result in reduction in the time taken. This selection of the region of interest can be done in manual form or automatic form, but in this paper, we are going to have detailed discussion on how it can be done automatically because manually selecting the ROI for each image can be time as well as energy consuming.



*Figure 1 : High Level Overview of Partial Image Encryption*

The whole image data set is manipulated in case of image encryption algorithms that are commonly used. Transferring the data is expensive with respect to time as well as bandwidth, too. One way is we can use compression algorithms on the images, but this increases the processing time altogether because, once the encrypted data reaches the receiver, they need to reverse the process to get the data, as a result double the time is taken. So, encryption of a small part of data from the image that can make the whole data unusable seems a better solution. This process is called partial image encryption.

### Objective of the work

The objective of this paper depicted in this thesis, is to perform partial image encryption using automatic selection of ROI and then encrypting that part of the image. At first, the task is to analyze different methods of object detection, then to choose which method to use for the implementation, and finally encrypting the ROI. This thesis also gives a comparative study between RSA and proposed substitution method.

### Scope of the thesis

This thesis is an attempt to present a simple way to partially encrypting an image using deep learning models for automatic selection of the ROI. An exhaustive study has been made to understand the topic and implement a simple way. This article is focused on building a ground-level understanding of a few different ways of selecting the ROI and finally, achieving partial image encryption of an image; and implementation of a specific way. Our thesis will help the researcher and developer in understanding few ways of automatically selecting the ROI and partially encrypting an image. It gives a demo of two full implementations. It also provides a comparative study between RSA and our proposed method using substitution.

### Motivation of the work

Research have achieved many aspects in the past few years in this field. There is research that shows how to do it completely. There are various ways for manual selection of ROI and encrypting the ROI. The motivation of the work comes from wanting to implement partial image encryption in a very simple yet effective way, in a considerable time using deep learning algorithms to automatically select the ROI. Research and developments are still going on at a booming rate in this field for improving the scope of existing neural networks for the purpose of computer vision.

### Organization of the thesis

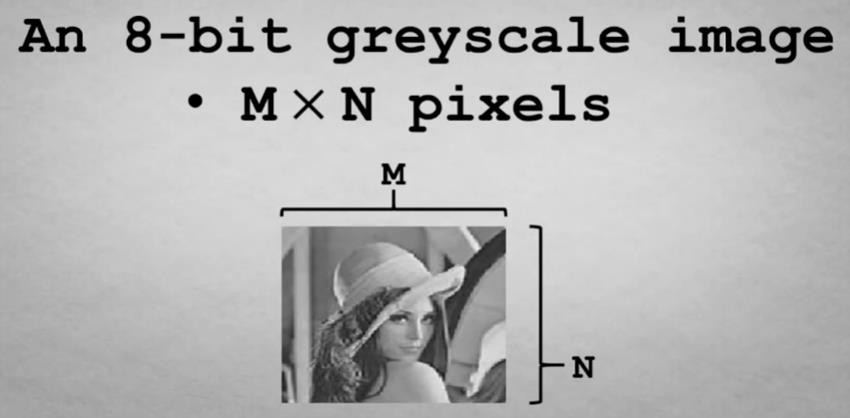
This thesis is organized in the following way: the first section named ‘Methods and process’ describes the methods and processes of partial image encryption in details; it consists of two ways of how we can select the part of the image containing the important data and then, we discuss in detail three most popular algorithms for object detection and compare the outputs on the same image for each algorithm. The second section is the proposed method. It is the method implemented and consists of the description of the implementation and comparative study between two methods implemented. In the next section, we analyze the results on different images and do a comparative time analysis. Finally, we conclude the thesis in the final section.

# Methods and process

### Introduction

|  |  |
| --- | --- |
| https://lh3.googleusercontent.com/oAJU0QUBxIywEn3ffYhHqOn53U0YkpDHcuW4fUUKjAtDX6f9L-VZSx5qLVHQZTqDbivxklGIzxzZ0TMRKBhwkHtMPXsMjVj0HSe4AGjxpWGOHUdvDrSNJfDnyrtb4c30jPh2pK0  *Figure 2: Image* | https://lh6.googleusercontent.com/yMjSXie8wzSRqAlQDThfVFgpz1zzHFp6tZ4G1Ut0CnZgSMQY2srRB8H0-26zxj2LAlg6g4HOzYjUcxCphDlbMmH2u7sqoKk2FAs7BXrUaO0oG5Jjky2Ph4-yZsSCVb94eE6cNIQ  *Figure 3: Zoomed in image showing pixels* |

An image basically consists of a two-dimensional matrix having values representing each pixel. Each pixel contains a value that is 8bit i.e., 256 shades per pixels. For a greyscale image, following is the shades with respect to bits. It can be similarly done for colored images.



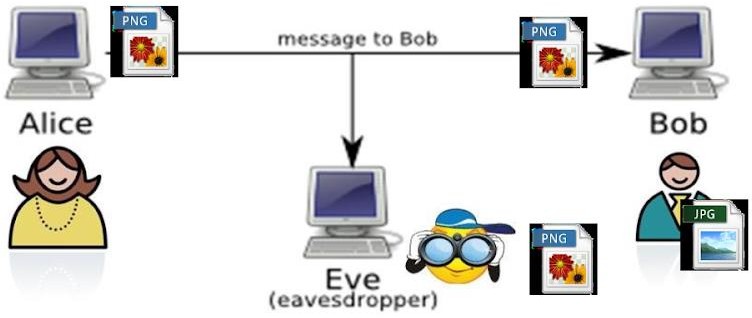
*Figure 4: Image as 2D matrix*

### Requirements of partial image encryption

The requirements are: Need to be able to access and work on the image pixels. Ability to create an encrypted image that cannot be hacked by the hackers easily. Encryption time should be fast enough. After decryption, the image should be equal to the input image.

### Applications

In the recent times, due to the pandemic and the travel bans imposed, many people had to resort to consulting doctors through video calls. As a result confidential medical data was transferred in voluminous amounts to people over the internet. Also, when medical personnel need some suggestion from doctors of different countries, personal medical data needs to be transferred over the network medium, and it should be fast as it involves the patient’s condition. Even in case of military data sharing, this is needed. This is when partial image encryption is needed and valued.



*Figure 5: Unsafe internet channel due to hackers*



*Figure 6: Security needed in case of Military Image transaction*

### Overview of the process

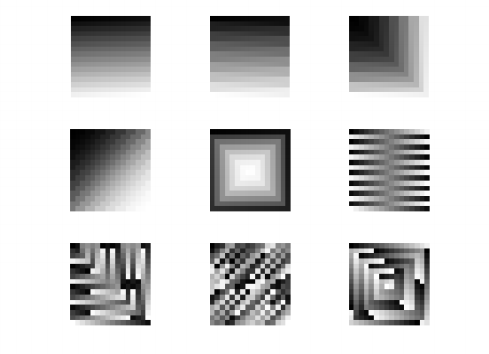
The main method to partially encrypt an image is hereby as follows: First is area selection prior to encryption. Then we need to encrypt that area.

#### 2.4.1 Selecting the significant data

This can be done in two ways: It can be done manually by diving the picture into blocks and then selecting the blocks that contains the significant data. It can be selected automatically using an algorithm to select most detailed part of the image as the sensitive part, removing which we can get the result. After selecting the sensitive area, we encrypt that specific area.

#### 2.4.2 Encryption of selected data

This is usually done in two steps: Creating an encryption key Encryption of the image ROI using the encryption key that was created in the previous step. Now, there is many ways to encrypt the image using various algorithms, here the first part of the thesis includes analysis of how it would work if we encrypted using mapping images. So, here the mapping images can be considered as encryption key which is mapped over the selected part of the image, thus encrypting the data of ROI. Following are some examples of mapping images:



*Figure 7: Map images used for encryption*

###### Manual

In this method first we can encrypt the input image into some sub blocks. It is then given as input to encryption process block. The encryption block contains two inputs: selected block i.e., the ROI and the other one is the map image i.e., the encryption key*.*

###### Automatic

In this way we can select the area of interest using some operations that we are going to discuss further in the other section. Then just the chosen part of the image is encrypted using the map images shown.

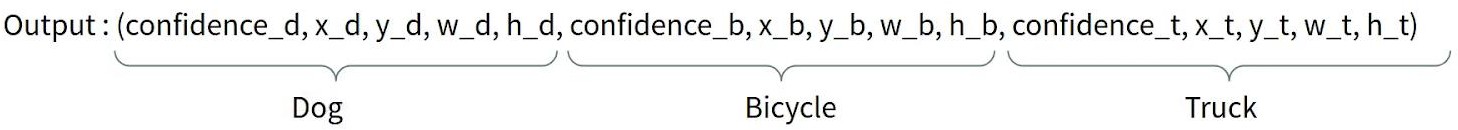
### Auto selection of area of interest prior to partial image encryption

#### 2.5.1 Introduction

From a computer vision point of view, the image is a scene consisting of objects of interest and a background represented by everything else in the image. The relation and interactions among them are the key factors for understanding the prospect. One of the finest works in computer vision includes image classification and object detection.

|  |  |
| --- | --- |
| https://lh4.googleusercontent.com/3N3WXX1tbNeKgD0AJjDz9wpiM621gS9edMpOxHeV3cviT6S_-M6J9mSKl5NR6b9rsimYg4xEjy_TfSCu0bdeST_dURqPxcN3HEbq5VR0mI5muwtOmPFZQxwGIdhLNF-tn7kU_krkkFU  *Figure 8: Image Classification*  Output:(confidence) | https://lh3.googleusercontent.com/2NowU_1K_OuaxW0N2_kSELXnQ4OMzhAkk9I0fF2Aa2Nkl72GHidGpHw9QdLJ-lXms8ws9aHxLXclgmcaXmiIeLFMsWgEXHUR4LkBJAHEmROJ8uUeJVaZGmmV05K05rD1TdZHx5QbaHM  *Figure 9: Object Detection*  Output: (confidence, x, y, w, h) |

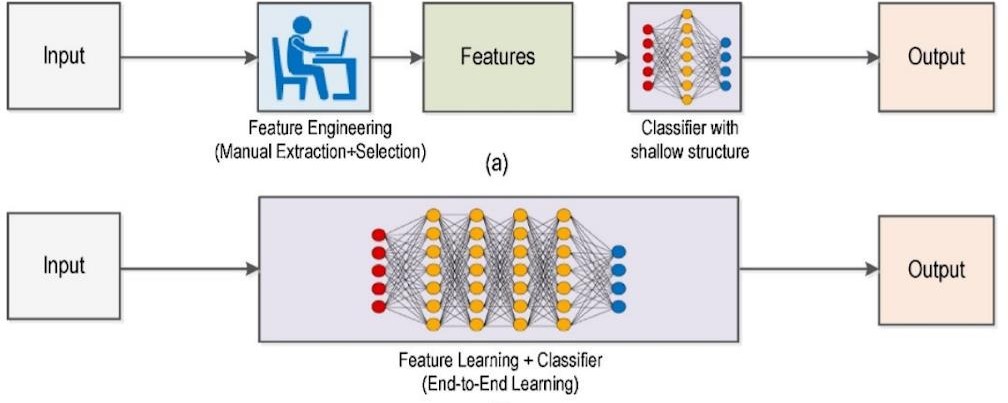
Detecting an image determines the presence of an object and/or its scope, and locations in the image that is the input. Object detection typically precedes object recognition. Here, we are mainly going to focus on object detection rather than recognition. This whole thing can be treated as a two-class object recognition, where one class represents the object class, and another class represents non-object class i.e., the background part. The output format should be as given below:



Object detection field is typically carried out by searching each part of an image to localize parts, whose properties match those of the target object in the training database.

#### 2.5.2 Choosing method for auto selection

Auto selection of ROI can be done either by traditional method or using deep learning. In this paper, we are going to talk about different Deep Learning methods to achieve this. There are a few reasons for that. One thing distinctive from traditional image processing is that when we use neural networks, we see the following advantages: "Learning" very distinguishing features which improves accuracy. Sharing computation when computing these features, which improves speed.

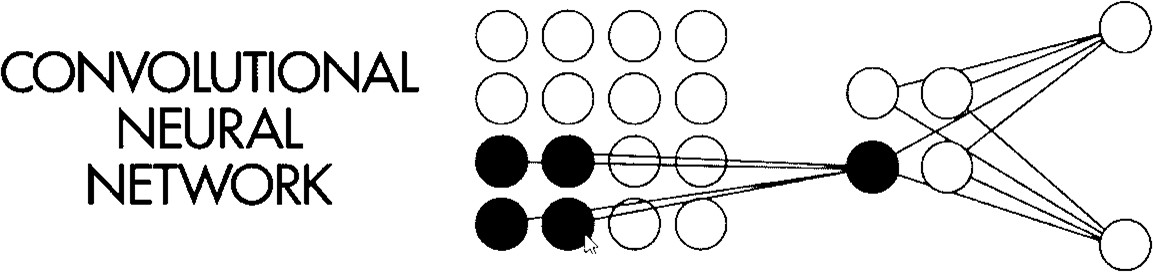


*Figure 10: Traditional versus DL workflow*

(b)

#### 2.5.3 Categories for neural networks for object detection

There are 2 types of neural networks that are deep that can be used for detecting an object: "One stage" object detectors (YOLO, SSD, Transformer based NN), and "Two stages" object detectors (RCNN). These are based on the CNN algorithm. The workflow is shown below:



*Figure 11: CNN network*

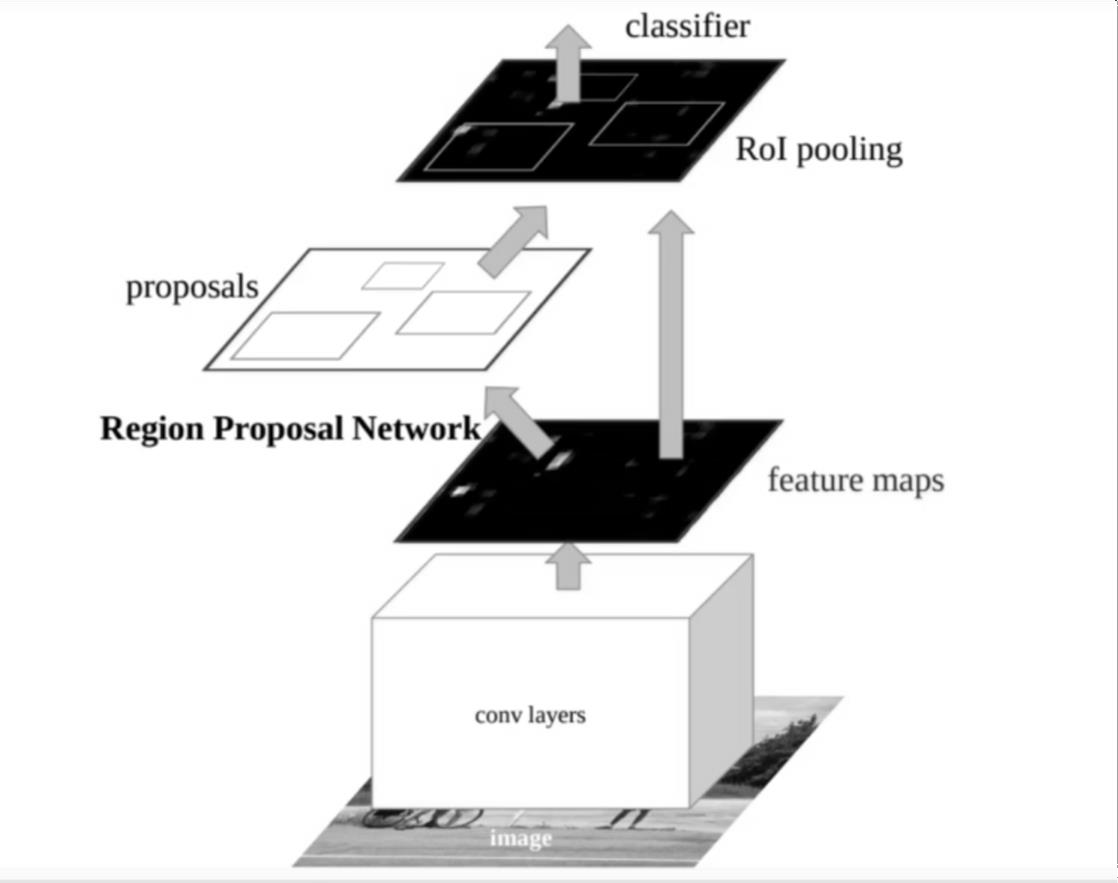


*Figure 12: Steps in working of CNN*

##### 2.5.3.1 Mask RCNN

They have this picture here of this image that shows the different steps that our CNN network takes in order to make predictions at the end for classes and for bounding boxes surrounding objects in those images. So, if we look at the image here, what we can see is that we start with an input image such as this one shown here. It is then passed to the convolutional layers here. Usually these are layers from a pre trained neural network that was used for classification mostly. So, for example, we would get or we would use Convolutional layers from Vision Network or Inception Network and what we get at the end or as an output is feature maps. So, use feature maps will

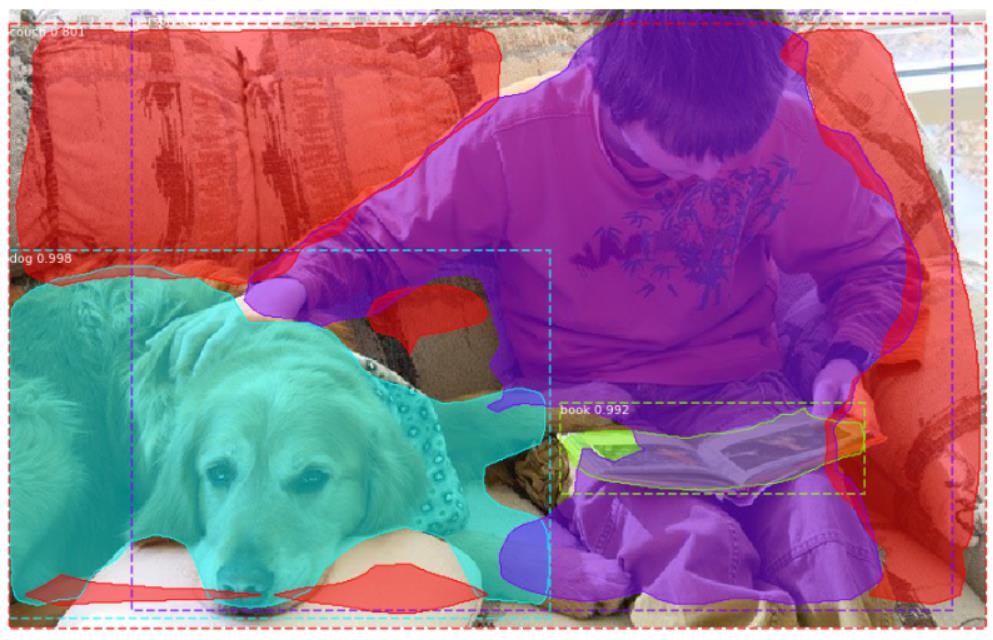
then go through a neural network, a small neural network called Region Proposal Network, or RPN, for short. And the goal of this RPN neural network is to propose regions that this network thinks that objects will exist in it, so it might think that this surface here or this area here will contain some objects, although it will not tell us which object it is just going to tell us that, for example, these three regions here, they have objects that are different than background. So, they could be like dog, bicycle, cat, whatever, but they are just different than background. So, the goal of the RPN neural network is this. And after that, what we have is a mother network, so all of these networks work together. So, when we finish this part here, we have finished the first stage. Our CNN network is in two stages i.e., a two-stage based object detector. And what happens next is that we best the output of the RPN neural network and the feature maps to another neural network. That is that that has the main task of Region Roi pooling, Roi calling is a region of interest. So, what happens is that in this new home that we get at the end, classes and bounding boxes surround the objects in the image.



*Figure 13: Faster RCNN block diagram*

We can also talk about another RCNN method called the Mask RCNN, R- CNN is basically the Region based Convolutional Neural Network. This was

originally published in <https://arxiv.org/abs/1703.06870>.This is a tensorflow model pre-trained on COCO dataset This method after execution returns: Bounding Box- Coordinates (Like in MobileNet SSD) Class Label- Label index with confidence (Like in MobileNet SSD) Mask- A pixel-wise mask for every object detected.



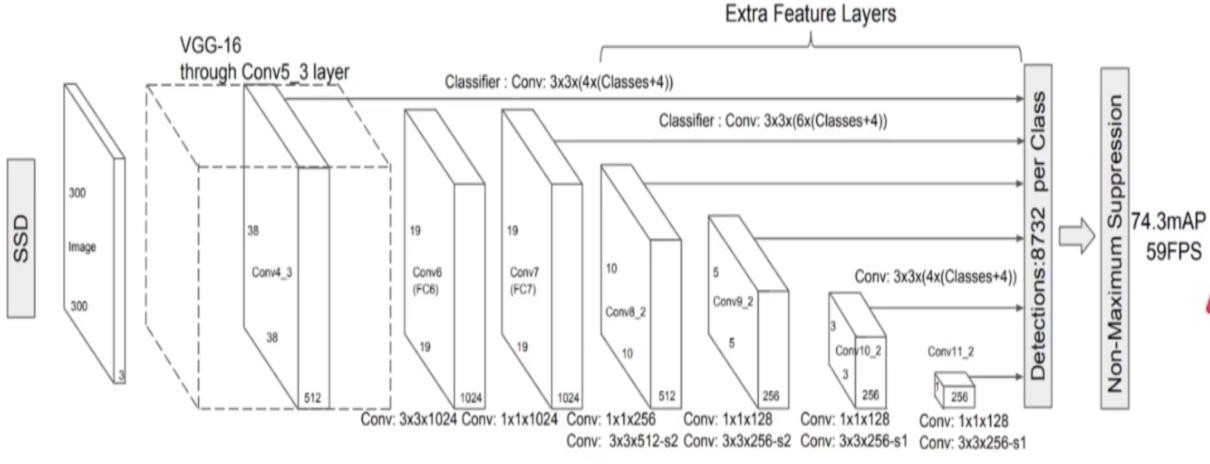
*Figure 14: Output from Mask RCNN*

This figure shows the output of the Mask RCNN algorithm. It applies a mask i.e.; it provides a segmentation of the objects that is why the name.

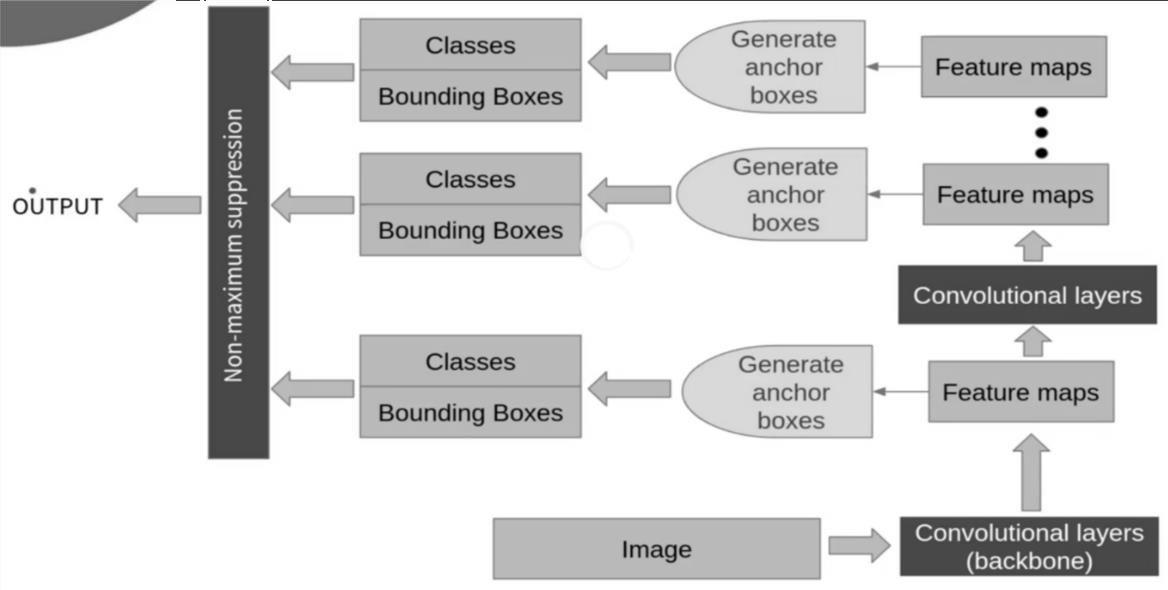
##### 2.5.3.2 SSD

The SSD basically works as follows, it starts by an image and an input, it passes it through a convolutional neural network or a backbone, just like CNN. We get some feature maps here and we can notice that. After this, we have multiple convolutional layers where we are making the volumes output's here, so the feature maps, we are making them smaller and smaller and smaller. And as you can see, each time, we are basically trying to make detection. So, we pass the image through the backbone. We get some feature maps. We try to make some detections. Using the first feature map, we take the feature map,

we pass it through another convolutional layer, and then we try to make detections on the output feature maps. Then we do that again. We passed it through some set of convolutional layers, we get new feature maps, and we make detections in those feature maps. We do this several times, as you can see here. And at the end, we have a set of detections, a big number of detections here. And then what we do is that we filter those detections, we do that by using a function which is a non-maximum suppression, here.

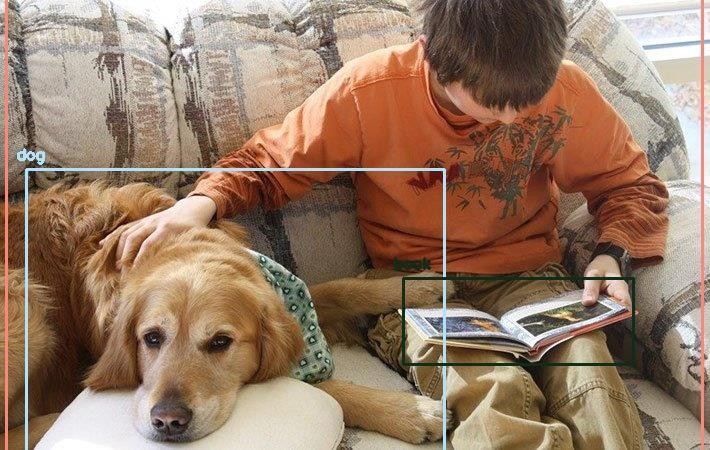


*Figure 15: Breakdown of SSD*



*Figure 16: SSD flow diagram*

One type of SSD is SSD MobileNet. It is a CNN architecture designed for low computing power devices like mobile devices. That is why it is named so. Single shot learning can classify objects from one, or only a few, training samples/images. This algorithm uses bounding box regression by Et al.



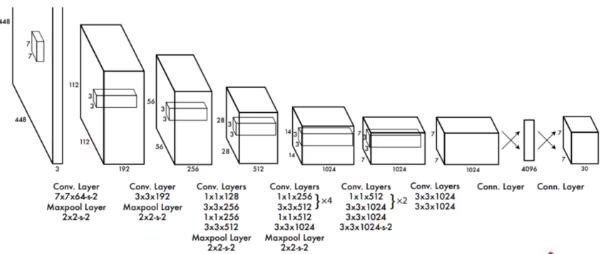
*Figure 17: Output with SSD*

The above figure shows how the output should be in MobileNet SSD.

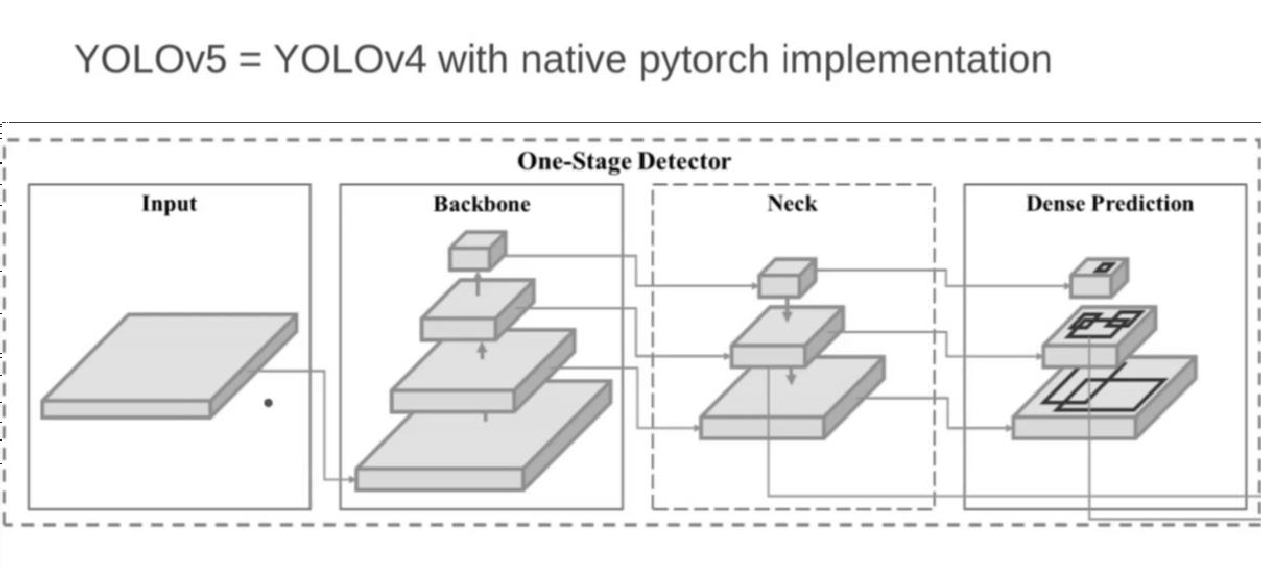
##### 2.5.3.3 YOLO

It looks very similar to a classification neural network and it's much simpler than CNN, for example. And here, the main things that you need to take from this network here is that the anchor boxes, because YOLO also uses anchor boxes just like CNN and SSD. So, your algorithm is actually like our CNN in terms of how the anchor boxes are or where they are constructed. So, in our CNN, we have the anchor boxes. Basically, constructed or defined, loosely defined is a better word are defined in the based on the input image, so based on the input image, we split the image into multiple cells and then we define our boxes there. So, in that sense, your algorithm is like CNN. But in fact, in terms of the architecture, your algorithm is much more like SSD because it's also having a bunch of convolutions. It's a one stage object detector. So, there is no there's no small neural network that does proposing regions like CNN. But it's very, very similar to SSD since we have. A bunch of convolutions and then we try to predict our bounding boxes at the end, but it's different than SSD in terms of if you looked at the network, then you realize that in SSD we assign a bunch of anchor boxes in each level of the feature map. So, for

example, we input the image, we get some feature map, we assign anchor boxes here, then we then that feature map goes to another convolutional layer, then the output we assign new anchor boxes, so on and so forth until the end. So, we get so many anchor boxes and various levels of the network. But in YOLO we define the anchor boxes in the input here. So, the algorithm there are five variations or the same five versions of it as of as of now.



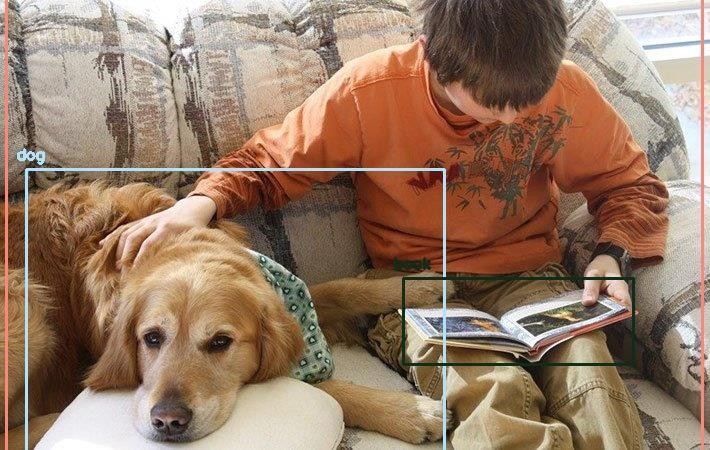
*Figure 18: YOLO breakdown*



*Figure 19: YOLO native pytorch implementation*

This was submitted in the paper <https://arxiv.org/abs/1506.02640>. In Pascal Titan X GPU, max speed achieved is 30 FPS. YOLO V3 with COCO dataset can detect 80 categories and no pixel segmentation or masking is available.

As we can see, YOLO is the perfect blend of speed and accuracy, this is what we are going to use in the proposed model.



*Figure 20: Output with YOLO*

# Proposed method

### Overview of the proposed framework

In the proposed framework, we are using YOLO method discussed earlier to detect the ROI and encrypting the selected part with RSA algorithm and a substitution method. We are using YOLO method because it is the most efficient among the discussed methods with respect to time and accuracy. The time taken to detect an object is very less using Mobilenet SSD and only one image is enough to train the model but as a result, the output is not too accurate. On the other hand, the mask RCNN model needs a little more time to work but the accuracy is very good, YOLO is a method that is on the middle ground between these two models, where the time taken is moderate and the

accuracy is moderate. So, in this method we are using YOLO model to detect the object from image. Next, we encrypt using RSA algorithm, because it being an asymmetric key algorithm is much secure and very difficult to hack the encrypted data. But the time taken by RSA algorithm is more so, we propose another method of substitution to increase the time efficiency. We are comparing the encryption processes using RSA and our substitution method. So, there is a comparative study along with the explanation and results using both methods and analysis of time taken and performance using each of the methods.

### Technologies used

* Language used: Python
* Kernel used: Python 3.6.5
* Platform used: VSCode / Jupyter / Google Colab
* Packages used: Numpy, Matplotlib, OpenCV, random (randrange, getrandbits)
* Object Detection model used: yolov3-spp.weights, yolov3-spp.config, yolov3.txt

### Comparative study

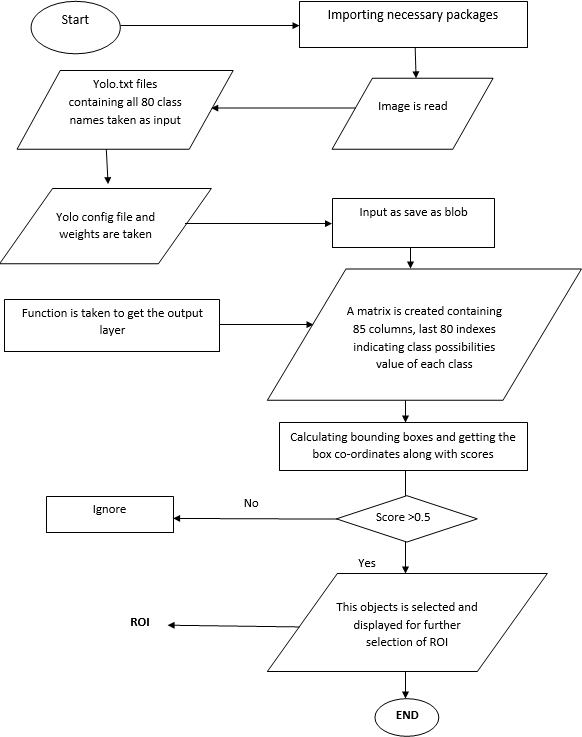
At first, we detect the object using YOLO algorithm, then we encrypt the method using two methods and we compare between them. We are comparing the encryption processes using RSA and our substitution method. For the RSA method, we generate the key and encrypt the ROI using the key. To decrypt, we use the reverse process. In the substitution method, we make three matrices for each of r, g, b components. First rows of matrices are populated using random permutations from range 0 to 255. Then, we right rotate each row with random values. Then we substitute the pixel values with value of the cell with row number of the pixel row and column number of the pixel value. Similarly, we reverse the process to decrypt the object using the encrypted image and the matrices we made.

### Flowchart

##### Complete flow

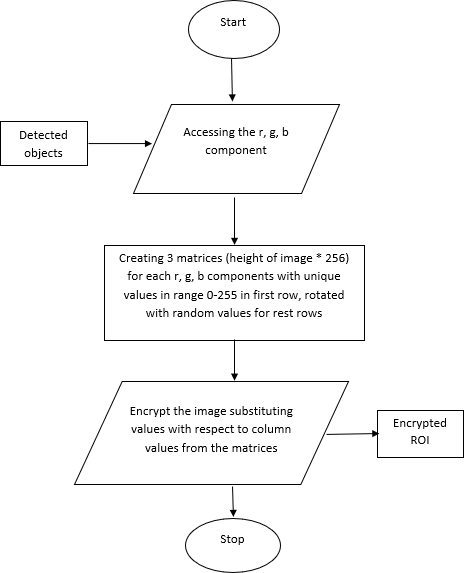
*Figure 21: Complete flowchart*

##### YOLO object detection flow



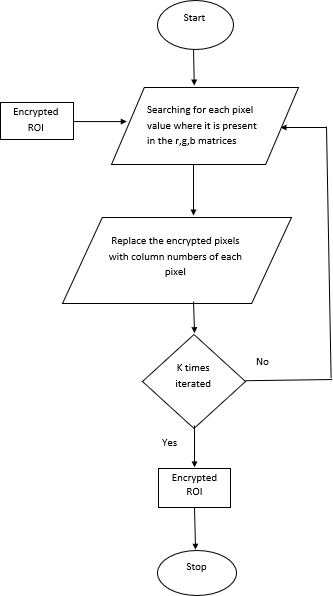
*Figure 22: Object detection flowchart*

##### Encryption flow with substitution



*Figure 23: Encryption flowchart*

##### Decryption using substitution



*Figure 26: Decryption using Substitution*

# Experimental results and discussion

### Experimental setup

The project implementation is conducted on the VS Code. It can also be conducted on Jupyter Notebook or Google Colab. The necessities to run this code is, having Python (latest version) installed in your device and the path is set as environment variable. The original experimental setup has python version 3.6.5. So, any version higher than that will work fine. It is written in ipnyb file, and it needs to stay connected to a python kernel.

### Implementation algorithm

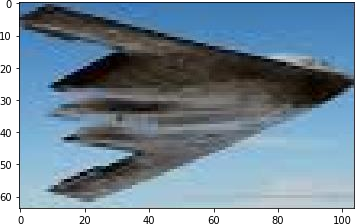
We use the YOLO algorithm to detect the object, it works on 80 classes and is efficient. This is a model that is a perfect blend of speed and accuracy that gives optimum results. Then, select the object of our choice and pass it out to the encryption algorithm. We encrypt by making an array of random integers, then putting it in the first row of a matrix of dimension height of the image \* 256 for each of the r, g, b color components. Then we, right shift each pixel value and fill the whole matrix. Finally, we substitute in the image the corresponding values form the matrices. And we compare the results to the output generated using RSA algorithm on the same images.

### Results

##### Input image

*Figure 28: Input Image*

##### Objects detected



*Figure 29: Object*

##### Partially encrypted image

|  |  |
| --- | --- |
| *(a)* | *(b)* |

*Figure 30: (a) Encrypted with substitution (b) Encrypted with RSA*

##### Results on other images

Here are some of the Partially Encrypted Images for some sample images:

|  |  |  |
| --- | --- | --- |
|  |  |  |
| *(a)* | *(b)* | *(c)* |

*Figure 31. (a) Original Image, (b) Partially encrypted image using substitution method and (c) Partially Encrypted Image using RSA algorithm*



##### Result analysis table

We check here, the NPCR and UACI values between the encrypted part and the original ROI, to analyze the encryption method and check the SSIM value between the input image and decrypted image for each of R,G,B components and get the average, to see how much difference is present between them. We also, compare the times taken by each method. We are checking all the parameters on the dog image as it contains multiple objects.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Method | NPCR | UACI | Time Taken | | | SSIM |
| Key Generation  Time(secs) | Encryption Time  (secs) | Decryption Time  (secs) |
| Substitution | 99.602 | 29.194 | 1.3 | 1.2 | 5.6 | 99.71 |
| RSA | 99.494 | 27.958 | 3.1 | 4.1 | 2.7 | 99.69 |

*Figure 32: Result Analysis Table*

# Conclusion

In this paper, we presented two simple easy frameworks for partial image encryption. We detect the object from an image using the YOLO framework. Using it, we can see in the results section that objects are detected in an accurate manner. With respect to the encryption part, as discussed earlier, the four requirements for a successful partial image encryptions are: Need to be able to access and work on the image pixels. Ability to create an encrypted image that cannot be hacked by the hackers easily. Encryption time should be fast enough. After decryption, the image should be equal to the input image. Using the RSA method, we can access the image pixels and have performed the operations. The encryption took 4.1s and the decryption took 2.7s for a RGB image of size (576,768). So, the speed is also fast enough. And as we can see from the results, the final decrypted image is exactly like the input image. It is a very simple approach, too. Similarly for the substitution method, all the four criteria for successful partial image encryption is fulfilled. Now to compare the two methods, substitution and RSA; the key generation time and encryption time of substitution method is much lesser than RSA, but the decryption time of RSA is lesser because for substitution method the time complexity for decryption is O(n3) as for each cell we need to traverse the matrices again. The encryption of using the substitution gives better results than the RSA algorithm as it is difficult to predict the ROI, as seen from the image results. So, considering the results from the two methods, we can say that substitution method is a better way than RSA because we are doing partial image encryption instead of total image encryption so that the time taken is decreased. So, considering the total time of the two methods, the proposed substitution method is the more efficient and preferrable approach.

# References

* Fares Jalled, ´ Moscow Institute of Physics & Technology, Department of Radio Engineering & Cybernetics Ilia Voronkov, Moscow Institute of Physics & Technology, Department of Radio Engineering & Cybernetics, “Object Detection Using Image Processing”, 23 Nov, 2016.
* Niall O’ Mahony, Sean Campbell, Anderson Carvalho, Suman Harapanahalli, Gustavo Velasco Hernandez, Lenka Krpalkova, Daniel Riordan, Joseph Walsh IMaR Technology Gateway, Institute of Technology Tralee, Tralee, Ireland [niall.omahony@research.ittralee.ie](mailto:niall.omahony@research.ittralee.ie), “Deep Learning vs. Traditional Computer Vision”.
* Krizhevsky A, Sutskever I, Hinton GE (2012) ImageNet Classification with Deep Convolutional Neural Networks. NIPS’12 Proc 25th Int Conf Neural Inf Process Syst 1:1097–1105
* Nash W, Drummond T, Birbilis N (2018) A Review of Deep Learning in the Study of Materials Degradation. npj Mater Degrad 2:37. https://doi.org/10.1038/s41529-018- 0058-x
* C.P. Papageorgiou, M. Oren, T. Poggio, A general framework for object detection, in: ICCV ’98: Proceedings of the International Conference on Computer Vision, Washington, DC, USA, 1998, pp. 555-562.
* S.Z. Li, L. Zhu, Z. Zhang, A. Blake, H. Zhang, H. Shum, Statistical learning of multiview face detection, in: ECCV ’02: Proceedings of the European Conference on Computer Vision, Lecture Notes in Computer Sciences, vol. 2353, London, UK, 2002, pp. 67-81.
* Gaurav Bhatnagar , Q.M. Jonathan Wu, Selective image encryption based on pixels of interest and singular value decomposition, Digital Signal Processing 22 (2012) 648–663.
* Rohith S, K N Hari Bhar, A Nandini Sharma “Image Encryption and Decryption using Chaotic Key Sequence Generated by Sequence of Logistic Map and Sequence of States of Linear Feedback Shift Register”, ICAECC, 10th-11th October 2014
* Komal D Patel, S.B., "Image Encryption Using Different Techniques": A Review International Journal of Emerging Technology and Advanced Engineering, 2011. 1(1): p. 30-34.
* H. El-din. H. Ahmed, H.M.K., O. S. Farag Allah, "Encryption quality analysis of the RC5 block cipher algorithm for digital images". Optical Engineering, 2006. 45( 10).
* Mohammad Ali Bani Younes, A.J., "Image Encryption Using Block-Based Transformation Algorithm ", IAENG International Journal of Computer Science,, February 2008. 35 , IJCS\_35\_1\_03(1): p. 15-23.
* Belmeguenaï Aïssa, D.N., Redjimi Mohamed, "Image Encryption Using Stream Cipher Algorithm withNonlinear Filtering Function", in IEEE High Performance Computing and Simulation (HPCS), 2011 International Conference. 2011, IEEE: Istanbul. p. 830 - 835
* M. Van Droogenbroeck , R.B., "Techniques for a selective encryption of uncompressed and compressed images". In ACIVS’02, Ghent, Belgium. Proceedings of Advanced Concepts for Intelligent Vision Systems, 2002(2002).
* Mohammad Ali Bani Younes, A.J., "An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption". IJCSNS International Journal of Computer Science and Network Security, 2008. 8(april 2008): p. 191-197.
* S. P. Nana'Vati, K.P.P., "Wavelets: Applications to Image Compression-I". Scientific and Engineering Computing, 2004. 9 No 3: p. 7.
* B.Acharya, S.K.P., G.Panda, "Image Encryption Using Advanced Hill Cipher Algorithm", 2009 Journal of Recent Trends in Engineering (IJRTE), 2009. 1: p. 663- 667