# Secure Deep Learning Based Object Detection in Medical Images

**Blessa Binolin Pepsi[1*,] Jeyashree[2], Subitcha[3], Meenalochini[4]**
*[1,2,3,4]Department of Information Technology ,*
*Mepco Schlenk Engineering College, Sivakasi, Tamil Nadu, India.*
**Corresponding Author*

**Abstract**: In this paper, we propose a lightweight privacy preserving framework, which encrypts the medical images through secure algorithms and object detection using Faster RCNN on the encrypted images. Faster R-CNN is one of the most outstanding deep learning models for object detection. Using our proposed system, healthcare centers can efficiently complete privacy preserving computations of Faster R-CNN via the additive secret sharing technique and edge computing. The object detection of Faster R-CNN contains three stages namely feature map extraction, region proposal and regression and classification. To improve the efficiency of the proposed system, we improve the existing secure computation sub-protocols involved which includes division, exponentiation and logarithm. The newly proposed sub-protocols can dramatically reduce the number of messages exchanged during the iterative approximation process based on the coordinate rotation digital computer algorithm. In this project, the medical images are divided into two random shares and each random share is encrypted separately using the proposed algorithm. The random shares are joined by using the secret additive protocols and the object detection is done using the Secure Faster R-CNN on the encrypted images. The encrypted random shares are stored in the edge servers instead of cloud servers. The edge computing provides low robustness and high communication latency. Hence large amounts of data can be stored. Using proposed system, the healthcare centers can fearlessly share the patient's medical images without worrying about leaking of patient's information.

**Index Terms:** Secure–preserving, Faster R-CNN, secure medical images, addictive secret sharing, and secure sharing protocol

## I. Introduction

The deep learning has been developed day by day and many problems have been solved from day by day. We were inspired to preserve the medical images in a timely response and to get a steady communication between medical care centres .So to provide a good privacy preserving technique we have used Faster Secure RCNN to handle and safeguard medical images and data in a timely consumption manner. The main idea of our project is to establish a secure transfer of medical dates between health care centres and detect the object detection using Faster RCNN. But for a MRI or a CT scan, the amount of images taken is quite large. For a single patient, the time taken to process the image can be more than ten minutes [1]. The amount of medical images taken during a MRI or CT scan is huge. Hence local servers are not used since the time to process and store large amounts of data are difficult. So the cloud servers are used to store large amounts of data. The problem with the cloud server is that it has high robustness and low communication latency. Hence edge computing [2] is used which acts as a bridge between the user and the cloud server.

The efficiency of the Faster RCNN depends on the amount of training data. A single health care centre data is not sufficient for the efficient object detection. Hence multiple healthcare centres come into agreement to share the images between them. During sharing of images by the health care centres, there may be a chance of leaking of medical images. A patient's medical data is confined only to the particular health care centre. At the same time, medical images are valuable commercial resources for the healthcare center. Consequently, for patient privacy and smooth cooperation between healthcare centers, it is necessary to build an efficient privacy-preserving framework for Faster R-CNN based object detection of medical images. It is considered to be an ideal approach to assist medical diagnosis [3]. Doctors can utilize this to detect the tumors in medical images. No patients want to reveal their medical data and images to be known by others except the health care centers were the patients are treated. There are many Privacy preserving techniques to enhance the images allowing multiple input parties to train ML models without releasing their private data in its original form .Hence privacy preserving of medical images is a must and a important role. Here we use the proposed system for patient privacy and smooth co operation among the health care centers. Currently researches are based on data storage privacy and calculations in encrypted format [4].

To overcome this problem, schemes like homomorphic encryption (HE) [5] and garbled circuit (GC) [6] has been proposed. Homomorphic encryption is computation over encrypted data without access to the secret key. The result of such online computations remains encrypted. Here data processing is outsourced to a third party without the need to trust the third party to secure the data. Garbled circuit is a protocol that enables two party secure computations in which two mistrusting parties can jointly evaluate a function over the private inputs without the presence of trusted third party. For most real world applications, these methods are also intolerable and not computation intensive and memory intensive.

Differential Privacy is also a popular technique for privacy preserving of deep learning models. Differential privacy is a system for publicly sharing information about a dataset by describing the patterns of the group within the dataset while withholding information about individuals in the dataset. Here Differential Privacy requires few computations to generate few random perturbations [7].To address the above problem, we have proposed an additive secret sharing based Faster RCNN framework for privacy preserving object detection of medical images.

In summary the main contributions of this work are listed as follow:

- The first privacy preserving Faster R-CNN framework allows multiple health care centres to securely share medical image data and to build high performance Faster R-CNN model [8].
- Several addictive secret sharing based sub-protocols are designed to realise the corresponding functions safely and accurately.
- For secure computations of the feature work extractions network, the region proposal network and the classification and bounding box regression of Faster RCNN without revealing their original data.
- Next, a performance comprehensive analysis is done to prove the correctness and security of the proposed system.

In Section II, we describe the works related to the project. In Section III, the system architecture is described. Then the proposed system is explained in Section IV, followed by the results and experimentation results of system in Section V. The conclusion, future work and references are presented in Sections VI and VII respectively.

## II. Related Work

Faster R-CNN is one of the most successful convolution networks evolved from R-CNN which is the first type of deep learning network applied to the domain of object detection. The other works related to this project are as follows.

In recent years, the model has been widely deployed in the fields of autonomous driving. Faster R-CNN achieves state-of-the-art performance on generic object detection. However, a simple application of this method to a large vehicle dataset performs unimpressively. In this paper, take a closer look at this approach as it applies to vehicle detection and conducted a wide range of experiments and provide a comprehensive analysis of the underlying structure of this model. In the related work, it is also shown that through suitable parameter tuning and algorithmic modification, we can significantly improve the performance of Faster R-CNN on vehicle detection and achieve competitive results on the KITTI vehicle dataset. We believe our studies are instructive for other researchers investigating the application of Faster R-CNN to their problems and datasets.

Zhang et al. [9] succeeded in identifying and detecting the adhesion cancer cells in phase-contrast microscopy with limited samples, which was essential to help people against cancer. In this research paper it is said that in biology and medicine research, detection and identification of cancer cells plays an essential role to further analysis of cell properties and developing new drugs experiments. However, owing to the adhesion among cells and great changes in morphology, it is a very challenging task to detect and locate the cells accurately, especially for the cells adhesion area. In this work, a deep detector for cells based on the framework of Faster R-CNN is proposed, and based on this; a Circle Scanning Algorithm (CSA) is presented for the redetection of adhesion cells. And then a series of experiments are achieved. The results show that the proposed deep detector can detect and identify all separate individual cells in an image, and that the hybrid method by combining Faster R-CNN with the proposed CSA can effectively detect and identify the adhesion cells under the conditions of the limited samples of adhesion cells.Resolution gets decreased. This method is not ideal for thick organisms or particles.But due to this it has thick specimens which can appear distorted sometimes.

By combining Faster R-CNN with Deep Lab, Tang et al. [10] overcame the challenging task of segmenting the liver from other organ tissues in clinical images and achieved automatic liver segmentation. In his research paper “Deep Lab: Semantic Image Segmentation with Deep Convolutional Nets, Atrous Convolution, and Fully Connected CRFs” the task of semantic image segmentation with Deep Learning and make three main contributions that are experimentally shown to have substantial practical merit are addressed. First, convolution with up sampled filters, or ‘atrous convolution’, as a powerful tool in dense prediction tasks is highlighted. Atrous convolution allows us to explicitly control the resolution at which feature responses are computed within Deep Convolutional Neural Networks. It also allows us to effectively enlarge the field of view of filters to incorporate larger context without increasing the number of parameters or the amount of computation Second, atrous spatial pyramid pooling (ASPP) to robustly segment objects at multiple scales is proposed Selvaraj and Varatharajan [11] use the hash function to improve the ability of watermarking to protect the integrity of digital medical images. In their research paper, it is explained that the ever-growing numbers of medical digital images and the need to share them among specialists and hospitals for better and more accurate diagnosis require that patients' privacy be protected. As a result of this, there is a need for medical image watermarking (MIW). However, MIW needs to be performed with special care for two reasons. Firstly, the watermarking procedure cannot compromise the quality of the image. Secondly, confidential patient information embedded within the image should be flawlessly retrievable without risk of error after image decompressing. Despite extensive research undertaken in this area, there is still no method available to fulfill all the requirements of MIW. This paper aims to provide a useful survey on watermarking and offer a clear perspective for interested researchers by analyzing the strengths and weaknesses of different existing models. However, in general, the quality of the watermarked images is reduced to a certain extent.

Zheng et al. used GC to protect the medical image privacy from the external cloud database. Unfortunately, GC is also unpractical due to the same reason as HE. In addition, the differential privacy (DP) technique can also be used to protect the image denoising from external cloud databases. The design enables the cloud hosting encrypted databases to provide secure query-based image denoising services. Considering that image denoising intrinsically demands high quality similar image patches, the design builds upon recent advancements on secure similarity search.

## III. System Architecture

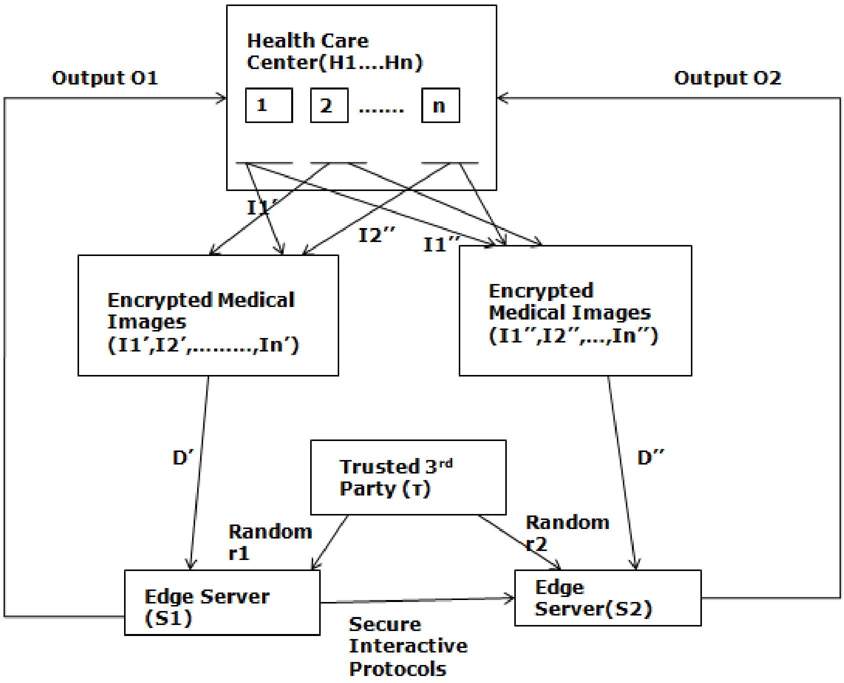
Health Care Center(H1....Hn)
1
2
.......
n
Output O1
Output O2
I1′
I2″
I1″
Encrypted Medical Images (I1′,I2′,.........,In′)
Encrypted Medical Images (I1″,I2″,...,In″)
D′
D″
Trusted 3rd Party (T)
Random r1
Random r2
Edge Server (S1)
Edge Server(S2)
Secure Interactive Protocols

Fig 1. System Architecture of proposed system

The figure 1 depicts a high level overview of system architecture of the proposed system. The System model and attack model for the required system is explained below.

### A. System Model

There are four types of participants namely the Health care centers two edge centers and the trusted third party

- H1,H2 ….Hn are health care centers ,which train a Faster R-CNN based medical object detection model. Health care centers do not want to reveal their data to be known by other except the patient's pathology health care centers. They are sent to the edge servers for storage and computations.

- S1 and S2 are two outsourced edge servers for intensive computations tasks. They are trained without knowing the plain text of medical images. The final outputs are sending to the health care centers using secure computations channels.
- There is trusted third party which serves as a random value generator.
- Encrypted data
- D′ = {Ik′ | k ε {1,2,.....n}}
- D″ = {Ik″ | k ε {1,2,.....n}}
- Send to the two edge servers for storage and computations

### B. Attack Model

Curious but honest model attack which refuse to know the data belongings to others that can benefit themselves. It's a hypothesis that edge servers cannot collude with each other. This hypothesis is important because the plain text can be recovered easily. In addition to this there is also a third party generator which is used to generate random values. It is to be noted that the above assumptions are used in secret sharing based privacy preserving of medical images in object detection.

### C. Secret Sharing Based Sub Protocols

In Our proposed system, inspite of revealing the medical data to the cloud servers, all operations and implementations must be done in a privacy preserving way. So Coordinate Rotation Digital Computer Algorithm (CORDIC) algorithm is used and implemented. Compared with existing protocols [12] new protocols can reduce the communication latency noises and provides low computations errors.

Based on Coordinate Rotation Digital Computer Algorithm (CORDIC) and the additive secret sharing techniques we design several secure computation sub – protocols [13, 14]

- Secure Division protocol SDiv
- Secure logarithm protocol SLog
- Secure exponentiation protocol SExp

### D. Secure Iterations of Cordic

CORDIC was first proposed by Volder et al. It is used to perform several mathematical functions with only addition and shift operations .CORDIC iterative methods that we consider namely secure linear vectoring mode (Live), secure hyperbolic rotation mode (HyVec) , and secure hyperbolic rotation mode (HypRot).[15]

**Protocol 1** Secure Linear Vectoring Mode Iteration

**INPUT** S1 has input µ1 ′,ν1 ′ and ὺ1 ′; S2 has input µ 1 ″, ν1 ″ and ὺ1 ″; the maximum no. of iterations be m

**OUTPUT** S1 outputs ὺm′ ; s2 outputs ὺm″

```
Set a public known index i ← 1
While i ≤ m do
(τ i ′ , τi″) ←2SCmp(υi , 0) − 1.
υ'i+1←υi'+τ' ·µ1'· 2^(-i) and υ''i+1←υi+τ''. µ1''· 2^(-i)
υ'i+1←υi' -τ'. 2^(-i) and υ''i+1←υi'' -τ''. 2^(-i)
Go for next iterations
End while
```

To complete the computation of LiVec there are four variants used in and to represent the target vectors after I times of vector rotations.υ'I denotes the sum of phase position after I times of vector rotations. τ' represents the rotation directions.

**Protocol 2** Secure Hyperbolic Vectoring Mode Iteration

**INPUT** S1 has input µ 1 ′, ν1 ′ and ὺ1 ′; S2 has input µ 1 ″, ν1 ″ and ὺ1 ″; the maximum no. Of iterations be m

**OUTPUT S1** outputs ὺm′; s2 outputs ὺm″

```
Set a public known index i ← 1
While i ≤ m do
(τ i ′ , τi″) ←2SCmp(υi , 0) – 1
µ'i+1←µi'+τi' ·υi'· 2^(-i) and µ''i+1←µi''+τi'' ·υi''· 2^(-i)
υ'i+1←υi'+τi' ·µ1'· 2^(-i) and υ''i+1←υi+τi''. µ1''· 2^(-i)
υ'i+1←υi' -τi'. Tanh^ (-1). 2^ (-i) and υ''i+1←υi'' –τi''. Tanh^ (-1). 2^(-i)
```

```
    if i%3 is 1 then
        do the ith iteration again
    else
        Go for next iteration.
    end if

End while
```

This type of protocol also needs four types of variants. There are also intermediate values. As LiVec rotates on hyperbola, the trigonometric function tanh is introduced in this protocol.

**Protocol 3** Secure Hyperbolic Rotation Mode Iteration

**INPUT** S1 has input μ 1 ′,ν1 ′ and ủ1 ′; S2 has input μ 1 ″,ν1 ″ and ủ1 ″; The maximum no. Of iterations be m
**OUTPUT** S1 outputs ủm′ ; s2 outputs ủm″

```
Set a public known index i ← 1
While i ≤ m do
    (-τ i ′ , -τi″) ← - 2SCmp(υi , 0) – 1
    μ'i+1←μi’+τi’ ·υi’· 2^(-i) and μ’'i+1←μi’’+τi’’ ·υi’’· 2^(-i)
    υ'i+1←υi’+τi’ ·μ1’· 2^(-i) and υ’'i+1←υi+τi’’. μ1’’· 2^(-i)
    υ'i+1←υi’ -τi’. Tanh^ (-1). 2^(-i) and υ’'i+1←υi’’ –τi’’. Tanh^ (-1). 2^(-i)
    if i%3 is 1 then
        do the ith iteration again
    else
        Go for next iteration.
    end if
end while
```

To calculate SExp, we use HypRot; the iterative process of HypRot is completed and updated in this protocol.

**Protocol 4** Secure Division Protocol

**INPUT** S1 has input μ 1 ′,ν1 ′ ; S2 has input μ 1 ″,ν1 ″**;** The maximum no. Of iterations be m
**OUTPUT** S1 outputs f’; S2 outputs f ’’

```
(η’,η’’,ε)←SME(μ)
(α’,α’’)←LiVec(η,1,0,m)
α ‘= α’.2^(ε) and α ‘‘= α ‘’.2^(ε)
(f’,f’’) ←SMul(α , v)
S1 and S2 return f’ and f’’ respectively
```

S1 and S2 first convert μ into single precision format [11] which then ensures the input of LiVec within the valid range.To ensure convergence μ must be greater than 1 and less than 2. Compared with existing protocols the number of messages is decreased from 8n to 2n.

**PROTOCOL 5** SECURE NATURAL LOGARITHM PROTOCOL

**INPUT** S1 has input μ 1 ′, ν1 ′; S2 has input μ 1 ″, ν1 ″**;** the maximum no. Of iterations be m
**OUTPUT** S1 outputs f’; S2 outputs f ’’

```
(η’,η’’,ε)←SME(μ)
(α’,α’’)←HypVec(η+1, η-1,0,m)
F’ ←2 α ‘+ ε. Log2 and F’ ←2 α ‘’
S1 and S2 return f’ and f’’ respectively
```

This protocol outputs (f’, f’’) where μ = μ’ + μ’’. F’ and f’’ are random shares of logarithmic result.To guarantee convergence the conditions for loop termination in SME becomes the mantissa between 0.1069 and 9.5383.

**Protocol 6** Secure Natural Exponential Protocol

```
INPUT S1 has input μ 1 ′,ν1 ′ ; S2 has input μ 1 ″,ν1; The maximum no. Of iterations be m
OUTPUT S1 outputs f’; S2 outputs f ’’
    1. μ‘ = α’ + β’ and μ‘’ = α’’ + β’’ where  α’ and  α’’ are integers and 0 <β’< 1 , 0 <β’’< 1
    2. [(γ’,γ’’),(δ’,δ’’)] ←HypRot (1/Rn ,0,β,m) where Rn =π(i=1 to n-1)√1-2^(-2i)
    3. S1 computes a←e^(α’) and split it into random shares  a←α’+ a’’
    4.  S2 computes b←e^(α’’) and split it into random shares  b←b’+ b’’
    5. S1 sends a’’ to s2 and s2 sends b’ to s1
    6. (ϱ’,ϱ’’)←Smul (a,b)
    7. (f’,f’’) ←Smul(ϱ,γ+δ)
    8. S1 and s2 return f’ and f’’ respectively
    9. The outputs of second iterations of SMul, f’ and f’’ are two random shares of natural exponentiations
       results of μ.
```

## IV. Proposed System

In this section we provide the implementation details of Our proposed system and feasibility of extending to a multi party settings.The figure 2 depicts Secure Deep Learning Based Object Detection in Medical Images

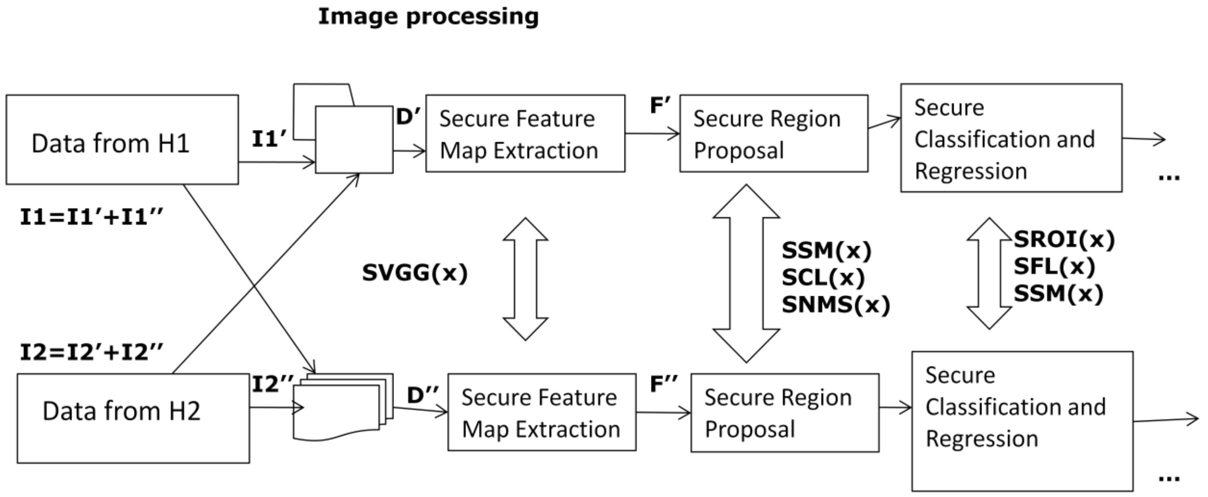

Fig 2. Secure Deep Learning Based Object Detection in Medical Images

### High Level Overview

The proposed system is composed of three stages namely secure feature map extraction, secure region proposal, secure regression and classification.  First, Our proposed system splits the medical images pixels into random shares and uploads it to the edge servers. Secondly, all computations are performed secretly using secure protocols

### A. Secure Feature Map Extraction

The input of SVGG is secretly shared pixels maps of medical images with fixed size that is D’ and D’’. SVGG is based on ImageNet but involves three basic neural layers .The three types of secure protocols is used. Here secure convolution layer (SCL) for filtering the images dimension is used. The activation function which is introduced to nonlinear data is used .Here activation function of Secure RELU layer (SRL) is introduced…Here, Secure pooling layer (SPL) is used for dimension reduction of images. Here VGG is used as a feature extractor.The output of this layer is shared feature maps F’ and F’’.

### B. Secure Region Proposal

It consists of anchor generation layer (ANL) and secure PRN network (SPRN).The goal is to operate anchor recommendations by using IoU algorithm and getting a series of anchors without leaking any medical image feature information .Choosing good anchor by invoking two SCL layers, one secure softmax function (SSM) and one secure non – maximum suppression protocol (SNMS) and then moved to the next stage.

### C. Secure Regression and Classification

This region completes the bounding box regression and object classification task without disclosing the image feature information .Here; two SCLs are substituted with SFLs.

### D. Secure Feature Map Extraction :

Before the medical images are send to the SRPN they are applied to the SVGG to extract the feature map. SVGG consists of three layers: SCL, SRL and SPL.VGG is a feature extraction Convolution Network Architecture for image recognition proposed by Visual Geometry Group. Using pre-trained model in Keras, VGG is used to extract the feature of a given image. Here SVGG a secure privacy preserving VGG feature extraction is used where it contains Secure Convolution Layer, Secure Pooling Layer and a Secure ReLU Layer.

### E. Secure Region Proposal

SRPN produces a set of candidate regions called anchors. In secure Region Proposal network anchor generation layer is added. Here the AGL scans the entire medical images features map and outputs nine kinds of anchor boxes with varying sizes. The computation process of IoU does not need data exchange and can be locally completed by S1 and S2 compute the Intersection over union.

$$\text{IoU} = \frac{\text{Area of overlapping}}{\text{Area of union}}$$

In Region Proposal Network SRPN filters and recommends the good regions under Region of Interest layers. For training SRPN and ranking the region proposals two SCL’s are used. The region proposal layer in Faster RCNN is novel region proposal layer which makes it feasible to achieve real time performance with the Fast RCNN. The CNN learns to classify from feature maps, RPN learns to generate these candidate boxes from feature maps. SSM can be used as

Pi= SSM (i) = SDiv (SExp (Ocls(i)’), SExp (O’cls(0)) + SExp (O’cls(1))),
Pi’’=SSM (i) = SDiv (SExp (Ocls(i)’), SExp (O’cls(0)) + SExp (O’cls(1)))

The loss function is computed for the log loss part of classifications and the smooth L1 part for box bounding regression.

Llog =(pi’,yi’) = SMul (yi’,Slog(pi’)) + SMul (1-yi’, Slog(1-pi’))
Llog =(pi’’,yi’’) = SMul (yi’,Slog(pi’’)) + SMul (1-yi’’, Slog(1-pi’’))

The three basic previously proposed secret shring sub-protocols SMul, SAdd and SCmp

**Protocol 9** Secure Comparison Protocol (SCmp)

- **INPUTS** Random shares (μ′, μ″) and (ν′,ν″)
- **OUTPUTS** : (f′,f″) where (f′+ f″) = 0 if μ>ν otherwise (f′+ f″) =1

Two intermediate values are exchanged between two edge servers

**PROTOCOL 10 Secure** Addition Protocol (SAdd)

- **INPUTS** Random shares (μ′, μ″) and (ν′,ν″)
- **OUTPUTS** : (f′,f″) where (f′+ f″) = μ + ν

No intermediate values are exchanged between two edge servers

**Protocol 11** Secure Multiplication Protocol (Smul)

- **INPUTS** Random shares (μ′, μ″) and (ν′,ν″)
- **OUTPUTS** (f′,f″) where (f′+ f″) = μ. ν
- Four intermediate values are exchanged between two edge servers

In this stage, the proposed system invokes SROI to reshape the size of the region proposal produced by SRPN and two fully connected layers to generate the final output. The proposed system computes the classification and regression co efficient in a similar way to SRPN.

## V. Results and Experimental Settings

Data privacy is the most important issue in the coming decade. Hence, Privacy protection of medical images is a necessary one. Faster Regional Conventional Neural Network base object detection has been considered an ideal approach for these problem .Here two datasets are taken. The first dataset is the Image CLEF medical image dataset which is publicly available https://www.imageclef.org/datasets and provided by the IRMA group from the University Hospital of Aachen, Germany. The dataset is the nuclei of the human body which is taken from the Kaggle website https://www.kaggle.com/c/data-science-bowl-2018 . The processor which is used is Intel® Core Tm i5-6200 CPU @2.50.GHz. Python version 3 is required. Python Libraries including NumPy, Matplotlib, Pandas, Keras and Tensor Flow are required. Pandas are a widely used open source Python library for data science, data analysis, and machine learning activities. Tensor Flow is an open source machine learning platform that runs from start to finish. It has a large, flexible ecosystem of tools, libraries, and community resources that allow academics to advance the state-of-the-art in machine learning and developers to quickly construct and deploy ML applications.

### A. Experimentation Results

To preserve the medical images firstly all the medical images were encrypted and then send to the health care centres by random shares .To evaluate this the IMAGECLEF datasets and nuclei in divergent images were taken to test in the Faster RCNN. Here first the images are pre-processed and resized to the required dimensions. Then the images are converted to grey scale for easier computations. Then the most important step is feature selection. All 2000 medical images for training and 500 images for validation are set. The model used to extract the feature maps is VGG16.Numpy and tensor flow libraries were used to accelerate the parallel computations. All the secure sub protocols were randomly set to default 50.The learning rate was set to 0.001default.The secretly shared images were generated by splitting the pixels of the original images into random shares. The images look like noisy images and cannot reveal any information about the original images. It is found that images were transformed into two disorganised and meaningless images after they are secretly shared. The phenomenon means that the statistical distribution of feature of the original medical image is hidden .Hence the medical images are privacy preserved.

To evaluate the performance secret shared sub protocols were used and trained for medical images. Faster RCNN is used for object detection of images as shown in fig. 5.

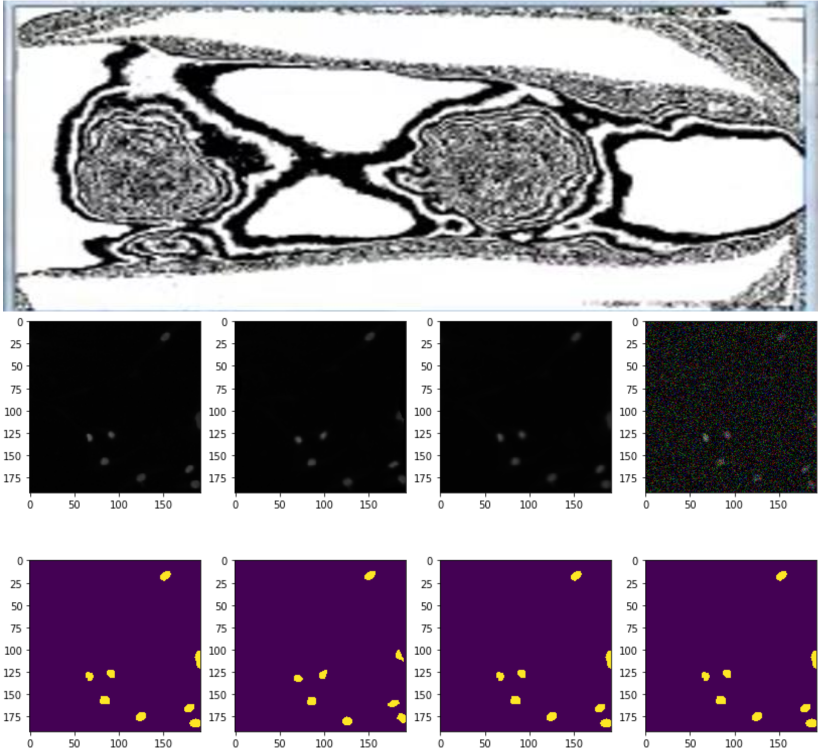

Fig. 3 Object detected in medical image

| Performance Measures | Results obtained |
|---|---|
| sensitivity | 97.05 |
| Specificity | 50.0 |
| Precision | 97.85 |
| Recall | 97.05 |
| Accuracy | 94.44 |
| F-Measure | 0.9705 |

Fig 4 Performance analysis results of the proposed system

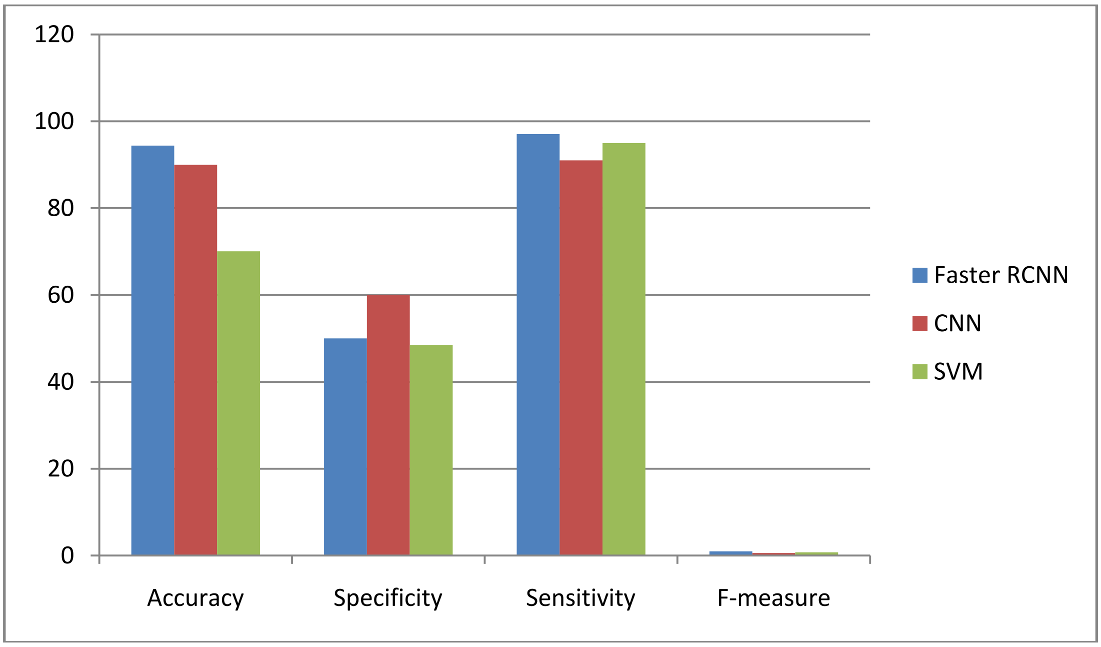

Fig.5 Comparison of the proposed system with existing algorithms

The results obtained in the experiment are graphically represented in Fig 4. The project results with sensitivity 97.05%, Specificity 50.0%, Precision 97.85%, Recall 97.05%, NPV 0.5%,FPR 0.5%, Accuracy 94.44%, Kappa Coefficient 0.47058, Jaccard Coefficient 0.942857, False Acceptance Rate 50.0, False Rejection Rate 2.3411 and F-Measure 0.9705. The high performance measure is obtained due to the fact of secure sub protocols used. The input size of each sub-protocol is n; m is the maximum iteration number of LiVec, HypVec and HypRot; TMul, TSMul and TSCmp are the runtimes of local multiplication, secure multiplication and secure comparison functions, where TMul < TSMul < TSCmp is measured.

## VI. Conclusion and Future Work

In this paper we have proposed secure object detection for medical images. We have used CORDIC algorithms to reduce the communication overhead between medical images and obtained the results. Then for object detection of medical images we have used Faster RCNN which is the most highly emerging object detector. Based on this medical centers can collaborate to train more accurate and more reliable models. Here we have proposed a series of interactive protocols to implement the training and inference process of our system, which included feature extraction, region proposal, classification and bounding box regression. Future work includes the medical images can be trained with different other models to preserve it to have less security risk and have lesser computation error.

## VII. Competing Interests

The authors declare that they have no competing interests**.**

## VIII. Acknowledgements

The authors would like to thank Revathi for useful discussions and suggestions.

## IX. References

[1]. W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges" IEEE Internet Things J., vol.

[2]. S. K. Pandey and R. R. Janghel, "Recent deep learning techniques, challenges and its applications for medical healthcare system: A review,"

[3]. G. Litjens et al, "A survey on deep learning in medical image analysis,"Med. Image Anal., vol. 42, pp. 60–88, Dec. 2017.

[4]. Y. Yang, W. Zhang, D. Liang, and N. Yu, "A ROI-based high capacity reversible data hiding scheme with contrast enhancement for medical images," Multimedia Tools Appl.,

[5]. L. Wang, L. Li, L. Jin, L. Jing, B. B. Gupta, and L. Xia, "Compressive sensing of medical images with confidentially homomorphic aggregations," IEEE Internet Things J.,

[6]. Y. Zheng, H. Cui, C. Wang, and J. Zhou, "Privacy-preserving image denoising from external cloud databases," IEEE Trans. Inf. Forensics Security,2017

[7]. M. Abadi et al., "Deep learning with differential privacy," in Proc. ACM SIGSAC Conf. Comput. Commun. Security, 2016

[8]. Krishnan and M. L. Das, "Medical image security with cheater identification using secret sharing scheme," in Proc. Int. Conf. Signal, Netw., Comput., Syst., 2017

[9]. S. Ren, K. He, R. Girshick, and J. Sun, "Faster R-CNN: Towards realtime object detection with region proposal networks," in Proc. Adv. Neural Inf. Process. Syst. (NIPS), 2015

[10]. K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," 2014

[11]. P. Belanovi´c and M. Leeser, "A library of parameterized floating-point modules and their use," in Proc. Int. Conf. Field Programm. Logic Appl. Berlin, Germany: Springer, 2002,

[12]. Z. Ma, Y. Liu, X. Liu, J. Ma, and K. Ren, "Lightweight privacy preserving ensemble classification for face recognition," IEEE Internet Things J., vol. 6, no. 3

[13]. X. Liu, R. Deng, K.-K. R. Choo, and Y. Yang, "Privacy-preserving reinforcement learning design for patient-centric dynamic treatment regimes," *IEEE Trans. Emerg. Topics Comput.*, to be published

[14]. X. Liu,R. H. Deng, K.-K. R. Choo, and J. Weng, "An efficient privacy preserving outsourced calculation toolkit with multiple keys," IEEE Trans. Inf. Forensics Security, vol. 11, no. 11,

[15]. J. E. Volder, "The CORDIC trigonometric computing technique," *IRE Trans. Electron. Comput.,* vol. EC-8, no. 3

[16]. Q. Fan, L. Brown, and J. Smith, "A closer look at faster R-CNN for vehicle detection," in *Proc. IEEE Intell. vehicles Symp. (IV),* Jun. 2016, pp. 124–129.

[17]. H. Jiang and E. Learned-Miller, "Face detection with the faster R-CNN," in *Proc. 12th IEEE Int. Conf. Autom. Face Gesture Recognit. (FG),* May/Jun. 2017

[18]. J. Zhang, H. Hu, S. Chen, Y. Huang, and Q. Guan, "Cancer cells detection in phase contrast microscopy images based on faster R-CNN," in *Proc. IEEE 9th Int. Symp. Comput. Intell. Design (ISCID),* vol. 1, Dec. 2016.

[19]. L.-C. Chen, G. Papandreou, I. Kokkinos, K. Murphy, and A. L. Yuille, "DeepLab:, Semantic image segmentation with deep convolutional nets, atrous convolution, and fully connected CRFs," *IEEE Trans. Pattern Anal. Mach. Intell.,* vol. 40, no. 4

[20]. P. Selvaraj and R. Varatharajan, "Whirlpool algorithm with hash function based watermarking algorithm for the secured transmission of digital medical images," *Mobile Netw. Appl.*