EVALUATION OF ASYMPTOTIC BEHAVIOR IN A PRIVACY-PRESERVING MODEL THAT PROTECTS FMRI DATA FROM UNFORESEEN PRIVACY ATTACKS USING COMPRESSED SENSING AND LEARNING.

Naseeb Thapaliya
Directed by: Dr. Shan Suthaharan
Department of Computer Science, UNCG

September 12, 2019

Abstract

This project aims to investigate the asymptotic behavior of a privacy-preserving predictive model for protecting fMRI data from unforeseen privacy attacks. In the previous works, the transition behavior of fMRI signals are characterized by evaluating compressed sensing and compressed learning methods with two-state Markov chain. The study showed that the transition probabilities could be used to construct a compressed sensing matrix, which transformed the signals for compressed learning to build a privacy-preserving model. The asymptotic analysis of this model would expand on the transition behavior, and describe the limiting behavior of the compressed sensing matrix, and, hence, give a precise characterization of the performance of the these models under different defined limits of large sizes. The end goal is to improve the compressed learning algorithm to create a more efficient privacy-preserving model for the fMRI dataset studying the asymptotic behavior of the model.

Contents

0.1 Introduction 2

0.2 *Understanding of Data:* 3

0.3 *Two-state Markov Chain for Computing Transition Probabilities:* 6

0.1 Introduction

The StarPlus fMRI Experiment conducted by Carnegie Mellon University Center for Cognitive Brain Imaging (CCBI) presented that the brain contains different significant region of interests(ROI's) which are responsible for different human behaviour and opinions. The functional magnetic resonance imaging(fMRI) data is simply the data set which contains information about these ROI's in the form of signal values. So, in other words we can interpret that the regions of interests in our brains can be represented by different signal values which are responsible for how human reacts to certain things. This illustrates further, that if these fMRI data was to be subjected to public analysis, then it could result in exploitation of human behaviours in important sectors such as running biased election campaigns, false marketing and many more. To make it more clear, you can assume the scenario that your brain regions of interest is exposed to some third party entity, and then, they use this information to explore your thought process and how you perceive different things, and use it against you or for their self benefits. This scenario is really scary, also because it gives away the mental medical history of the individual and leaves them vulnerable.

Identifying the critical importance to secure sensitive personal data, the research project aims to study compressed sensing and develop compressed machine learning models that protects values of the original data, by compressing the original features masking their values with sets of data. The hypothesis of the project is that, the activities of compressed sensing can be carried out by using two-state markov chain, and its transition probabilities and asymptotic behaviors can be ananlyzed for the feature extraction.

0.2 Understanding of Data:

The first and of the one most part of the project is to understand the ins and outs of the fMRI data. The fMRI data is taken from the Carnegie Mellon University's StarPlus fMRI data site [**?**], and was developed by Tom Mitchell along with Wei Wang at the Carnegie Mellon University's Center for Cognitive Brain Imaging (CCBI) [**?**].

The experiment consists of set of trials and the fMRI data could be attributed into each of these trials. In these trials, the participant was subjected to either a picture or a sentence, and then was instructed to let the researcher know if the sentence was in anyway related to the picture. Half of the trials started with the picture shown first and the other half started with the sentence shown first. In between these trials, some time was allocated to intervals, where the participants are simply rested or instructed to gaze at a fixation point on the screen. For each subject, 50 such trials were carried out and each trials lasted for the total of 27 seconds. The 27 seconds of the trial could be broken down such that, for the first 4 seconds, a sentence or a picture is shown which acted as a stimulus for the subject's brain. Then, after 4 seconds has elapsed, the stimulus was replaced by a blank screen where the subject gazed at for 4 seconds. After that, based on what was shown as the first stimuli (i.e. picture or a sentence), the second stimuli was shown to the subject for 4 seconds. If the first stimuli was a picture, then a sentence was shown, and vice versa. Following this, the second stimulis was removed from the screen, and the final 15 seconds was allocated as a rest period for the subject. Like this, the total trial time taken was 27 seconds. It is important to note, that the stimuli either sentence or picture screen are categorised as different labels for the classification process. The labels for the unbalanced dataset were 0, 1, 2, and 3. A label of 0 means the data in this segment should be ignored. A value of 1 means the segment is during a time when the subject is at rest or it is a fixation interval. Condition value of 2 signifies that it is a sentence or picture trial, where the sentence is not negated. Finally, a condition value of 3 signifies it is a sentence or picture trial where the sentence is negated. Then, to avoid any class characteristics error during classification, only two labels 1 or 2 were taken. Here, if the first stimuli was a picture, then the label 'P'= 1 was assigned, whereas, if the first stimuli was a sentence, then the label was changed to 'S' = 2.

The process was repeatedly carried out in different sequence for different trials, and image scans was recorded for processing at each trials in every 500 msec. Thus, total of 54 fmri 3D image scans were recorded for an individual trial which lasted for 27 seconds. Digital image processing was carried out on each of these 3D images to generate a set of data based on the voxels(simply 3D pixels) values of the fMRI scans. These, generated data that forms the fMRI dataset. In the scans of the brain, 25 particular regions were identified as regions of interests(ROI's) i.e. the regions which are responsible to generate brain activities when the subject was introduced to different stimulus. These ROI's comprises the values that are the fMRI data. After, detail study and classification of the regions it was further identified that out of those 25 ROI's only 7 ROI's played a crucial role in the of the brain when introduced to different stimuli. These 7 ROI's were categorised as: 'CALC', 'LIPL', 'LT', 'LTRIA', 'LOPER', 'LIPS', and 'LDLPFC'.

Now, this experiment was performed on total 6 different subjects, hence, there are 6 different dataset available for analysis. Each datasets were further represented by three variables; 1. Meta: This variable provides information about the data set. 2. Info: This variable defines the experiment in terms of a sequence of 'trials'. 'info' is a 1x54 struct array, describing the 54 time intervals, or trials. Most of these time intervals correspond to trials during which the subject views a single picture and a single sentence, and presses a button to indicate whether the sentence correctly describes the picture. Other time intervals correspond to rest periods. 3. data: This variable consist values for the image intensity values, upon which our experimentation is performed. The variable data consist of the observed data. The data structure 'data' is a 54x1 cell array, where each cell is one trial. Each element in the cell array is NxV of the fMRI observations. To better understand and define the 'data' structure, the element data$\{x\}(t,v)$ returns the fMRI observation of voxel v, at time t within trial x.

Now, there are total 6 subjects upon which these experiments were carried out. Consequently, there are 6 different fMRI dataset availabe for our analysis. The first dataset is of subject 04847(unique number for identification). For the particular dataset, the dimension of the data was found to be 50 x 253,692. Where, 50 are the number of trials or observations and 253,692 are the number of features or predictors. Clearly, the case is of high dimensionality since (features>Observations). which is one of the domain characterstics error. Here, 253,692 features are extracted from the voxels which are taken from the 3D images, as number of voxels for this image is 4698. Since, there were 54 images, and from each image 4698 voxels were extracted, this gives the total of (52 X 4698) 253,692 features. These dimensions are including that of all the 25 ROI's. But only, when 7 ROI's ('CALC', 'LIPL', 'LT', 'LTRIA', 'LOPER', 'LIPS', and 'LDLPFC') are selected, the number of voxels is reduced to 1,715. Now, when using the reduced number of voxels, 1,715, multiplied by the number of images in each trial, 54, the feature space is now 92,610.

Furthermore, th fMRI data from all the 6 subjects are combined creating a combined data set having massive dimension of 50 X 1315332 for the 25 ROI's. Here, note that the data set for subject 05675 had only 49 trials instead of 50 trials, and, an extra trial taking the mean of all the rows was added making it total 50 trials so that all the data of all the subjects could be merged without any problem. When, only 7 ROI's was taken, the total dimension of the combined data set was reduced to 50 X 472050 dimension data, where 50 are the number of trials and 472,050 are the number of features. In the experiment, the validation was performed on the following combined data considering it as an unseen data.

0.3 *Two-state Markov Chain for Computing Transition Probabilities:*

Theory of compressed sensing states that the signal x can only be retained if can be characterised by the sparse representation of the linear transform. In compressed sensing, the fMRI data is interpreted as signals and the stochastic behavior of the signals is characterized by the two-state markov chain which generates sparsity required for the compressed sensing matrix. The most basic property of a Markov chain is that only the recent point in the sequence affects what happens next. This means that for each trial sequence only the previous point has any affect on what can happen next. Here, as two state markov chain, there are two states given by 0 or 1 each signal is further characterized by 0 or 1, where 0 creates the sparsity required. We can look at the following figure to understand the basic working of the Two-state Markov chain relevant to our project. Here, the way in which the state changes for each dataset is observed, was that for each observers' data point, if the previous point $n-1$ was greater than the currently observed data point n, then the current point was marked as a 0. For example, if the previous data $n-1$ was 1.231 and the current data n is 0.32 then the n is marked as a 0. Furthermore, If the previous data $n-1$ was smaller than the current data n, then the current data was marked as a 1. For each sequence then, we can create a transition matrix with the probabilities of a $t00$, $t01$, $t10$, and $t11$.

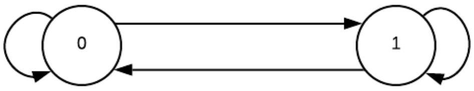

Figure 1: Markov Chain Example

Likewise, applying concept of Two-state Markov chain to the whole data set, new transition matrix was created. Now, this transition matrix consisted of 0 and 1 signals which would be applied to the original data set. From, this transition matrix, transition probabilities were computed for all trials. Then, n-step transition probability matrix was calculated, such that the asymptotic behaviour could be analyzed of the fMRI data. The initial block diagram are as follows:

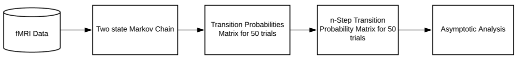
fMRI Data
Two state Markov Chain
Transition Probabilities Matrix for 50 trials
n-Step Transition Probability Matrix for 50 trials
Asymptotic Analysis

Figure 2: Initial Process Diagram