Title: Error-Correcting Codes allow Privacy and Quality Assurance in Crowdsourcing

Authors: Aditya Vempaty[1], Lav R. Varshney[2], Pramod K. Varshney[1]

Abstract: Due to the low-pay of crowd workers, they are often unreliable. And due to the crowd workers' anonymity, requesters prefer to maintain the privacy of their work to be done. Herein we develop methods to ensure reliable work delivery while preserving some level of privacy to the requester's data. For this purpose, by considering an image classification task, we use a combination of random perturbation to mask the sensitive data and error-correcting codes for quality assurance. We also consider the possibility of collusion attacks by malicious crowd workers and discuss the tradeoffs between cost, and the goals of privacy and quality assurance.

The proposed technique consists of two major elements: data perturbation before it is presented to the workers so as to preserve privacy, and the use of data fusion techniques based on principles of error-correcting codes to ensure reliable classification. Since the workers only have access to noisy versions of the input, performance could be degraded. Error-correcting codes enable reliable fusion of this data. Consider a crowdsourcing system consisting of N crowd workers who are given the task of classifying a given image into a set of M possible classes. To preserve privacy, we first add random noise to the image to mask the sensitive data of the image. To ensure correct classification, we devise easy-to-answer binary questions by modeling this system as a binary code matrix of size M x N. The rows correspond to the different classes while the columns correspond to the different questions to the workers. After receiving the N workers' response, the vector of answers is compared to the different rows of the code matrix. The final class is decided as the one corresponding to the row which is "closest" to the received vector where the Hamming distance metric is used to quantify the distance between vectors. The redundancy and error-correcting capability of error-correcting codes ensure quality assurance. The code matrix is designed so as to minimize the misclassification probability. There is a tradeoff between the level of privacy and the level of unreliability. However, the use of error-correcting codes simultaneously counteracts both causes of individual error as observed in our results.

By using the code matrix based information aggregation, we can mitigate the random discrepancies among the data provided by the workers. However, we need to be aware of a possible threat in this scheme. Malicious workers could collude to infer the true data by sharing their perturbed input data. We observe that, for a fixed number of colluding workers and a fixed probability of successful collusion (which is a function of the perturbation noise), the probability of classification error can be limited by increasing the total number of workers taking part in the task. However, it is costly to invoke a larger crowd. Therefore, there is a tradeoff between privacy, reliability, and cost. We develop mathematical models to study the precise tradeoffs between task performance quality, level of privacy against collusion attacks, and cost of invoking a large crowd. Such a study provides design strategies and principles for crowd work.

This abstract is partly based on our work previously published as [1][2]

[1] A. Vempaty, L. R. Varshney, and P. K. Varshney, "Reliable Classification by Unreliable Crowds," in Proceedings of 2013 IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP), Vancouver, Canada, 26-31 May 2013.
[2] L. R. Varshney, "Privacy and Reliability in Crowdsourcing Service Delivery," in Proceedings of the 2012 SRII Global Conference, San Jose, California, 24-27 July 2012.

[1] Aditya Vempaty and Pramod K. Varshney are with the Department of EECS, Syracuse University, Syracuse, NY, email: {avempaty,varshney}@syr.edu

[2] Lav R. Varshney is with IBM Thomas J. Watson Research Center, Yorktown Heights, NY,
email: varshney@alum.mit.edu