**CONCLUSION**

Even though there are many kinds of CAPTCHAs, text-based CAPTCHAs are commonly used even if they are not the most secure option because they are cheap, convenient, and user friendly. Because text-based CAPTCHAs are more vulnerable to attacks and less secure than originally intended, improvements need to be made. Finding ways to solve text-based CAPTCHAs that are more efficient and more accurate is a great way to increase their security by finding their weaknesses. Overall, CNN is an efficient and accurate method of recognizing CAPTCHAs, and there could be more developments in using it to improve the security of text-based CAPTCHAs. To determine if CNN networks which have less structural complexity and shorter runtimes could be used to accurately recognize CAPTCHAs with character adhesions and background noise, our team constructed three CNN networks that are structurally more efficient than many of the current methods of high accuracy CAPTCHA recognition, and tested them on three different CAPTCHA datasets. The results show that even though these networks have less structural complexity, they are still capable of reaching high accuracy recognition, such as 94.67% accuracy for Network 1 on the first dataset, with only 1070 samples from each dataset selected for training. Even on instances where the accuracy is low, we believe the accuracy could be greatly improved with more training. These results suggested that the third dataset, which is composed of all 26 upper case and lower case letters and 10 digits randomly with character adhesions, slant, and dots and lines in the background as distractions, was considerably harder for the models to recognize compared to the other two datasets, and it required more training to reach a desired accuracy. The future security of text-based CAPTCHAs remains an open problem and is part of our ongoing work.