ABSTRACT

Online transaction fraud is a risk brought about by technological advancements, one of which involves fraudulent payment evidence through forged payment proof screenshots. Scammers often target elderly individuals who have limited digital literacy, while delays in SMS banking monitoring also provide opportunities for fraudsters to commit their crimes. This threat results in significant financial losses and undermines trust in the affected banking systems. Classifying original and fake payment proof screenshots is one approach to strengthening transaction security and reducing fraud incidents. This classification used a Backpropagation Neural Network method with Gray Level Co-occurrence Matrix (GLCM) feature extraction, focusing on payment proof screenshots from Bank BRI transactions through the BRImo application. The scenario involves finding the best model by experimenting with preprocessing, GLCM angle and distance features, and neural network architecture during the training and testing phases. The average accuracy test result for the preprocessing scenario is 94%, while without preprocessing, the accuracy is 96%. For the GLCM angle and distance scenario, "All and 1" achieved an average accuracy of 94%, while "All and 5" achieved an average accuracy of 95%. In the neural network scenario, Model 1 achieved an average accuracy of 94%, and Model 2 achieved an average accuracy of 95%. Based on these test results, the model without preprocessing using the best features achieved a higher accuracy, demonstrating its capability to perform classification effectively.

Keywords : Classification, Screenshot, Bank BRI, GLCM, Artifical Neural Network, Backpropagation