Using VGG19 with SVM for Resistor Defect Detection using the SolDef_AI Dataset

John Mark Klamut

December 2024

1 Introduction

In the field of hardware cybersecurity, traditional manual inspection methods for detecting and classifying defects in electronic components are rapidly being replaced by machine learning applications. As technology becomes more integrated into every aspect of our lives, the need for secure and reliable hardware has never been greater. Malicious alterations to printed circuit boards (PCBs) and their components pose a significant threat, as they can compromise the integrity of critical systems. For a deeper dive into the importance of hardware cybersecurity and the risks of tampered electronics, The Big Hack is an excellent resource, highlighting the vulnerabilities in hardware supply chains and the innovative techniques being developed to secure them [1].

In my current research, I am exploring machine learning approaches to detect tampered or defective PCB components. This project focuses on detecting whether a resistor is defective or benign by analyzing its alignment relative to its soldering pad. Proper alignment is crucial, as misaligned components may signal manufacturing defects or potential tampering.

I use a pre-trained VGG19 deep learning model to extract features from images of the resistors. These extracted features, which represent the visual and structural characteristics of the components, are then passed to a Support Vector Machine (SVM) classifier. The SVM determines whether the resistor is classified as defective or non-defective based on these features. The final results need some more work as I only achieve an accuracy of 74 percent. However, by automating defect detection, this project demonstrates the potential for machine learning to improve the efficiency, accuracy, and scalability of hardware inspections.

As a overview of this final project proposal, Section 2 will briefly explain the working parts of the VGG19 model that is used for extracting the features, and will cover the SolDef dataset. In Section 3, the overall model for the experiment will be explained in detail. In Section 4, the experimental results will be explained. Finally, in Section 5 the future work and the conclusion will be presented.

2 Background

2.1 VGG19

VGG19, introduced in the 2014 paper ”Very Deep Convolutional Networks for Large-Scale Image Recognition” by Karen Simonyan and Andrew Zisserman [2], is a deep convolutional neural network designed for image classification. The architecture consists of 19 layers: 16 convolutional layers followed by 3 fully connected layers as seen in the image provided. Some of the key components of the VGG19 architecture are the 3x3 kernel filters with a stride of 1 and a padding of 1 to preserve spatial resolution. Additionally, an activation function(ReLU) is applied to introduce non-linearity into the model. Finally, max pooling is utilized to reduce spatial dimensions while retaining important information between the convolutional layers[2].

The convolutional layers of VGG19 capture low-level features such as edges, textures, and colors in early layers, and progressively more complex patterns and semantic structures in deeper layers. VGG19 comes with pretrained versions in PyTorch and TensorFlow that utilize the ImageNet dataset. When using a pretrained VGG19 model for feature extraction, the convolutional layers are typically frozen, meaning their weights are not updated during training. This preserves the feature representations learned on ImageNet. In this application, the last three fully connected convolution layers of the pretrained VGG19 model are discarded. This allows the model to focus on detecting differences in edges and general image features, rather than the specific features learned from the ImageNet dataset.[2].

2.2 SolDef_AI Dataset

The SolDef_AI Dataset is a publicly available dataset designed for defect detection in SMT resistors. It includes two types of defects: solder amount (indicating whether a resistor has too much or too little solder) and alignment (whether a resistor is properly centered on its solder pad). The dataset can be accessed here: https://www.kaggle.com/datasets/mauriziocalabrese/soldef-ai-pcb-dataset-for-defect-detection[3].

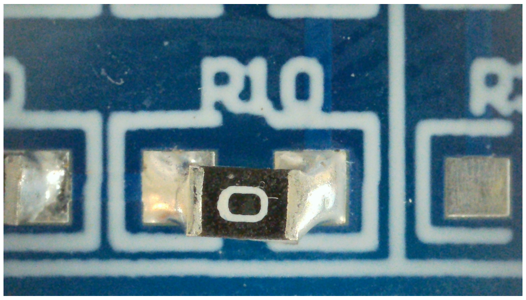


Figure 1: Off Centered(Defective) Resistor

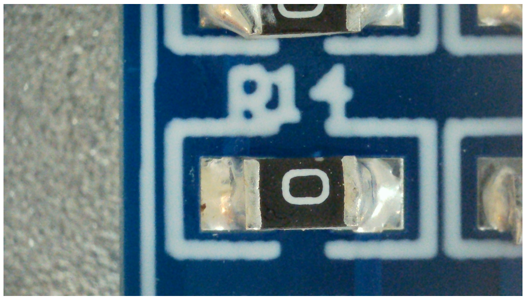


Figure 2: Centered(Benign) Resistor

The dataset contains 1,150 images of SMT resistors, each captured from three different viewpoints. The resistors are captured from a top view, 45 degree angle view, and an axonometric view. For this project, the experiment focuses exclusively on the top(bird's-eye) view and alignment defects, as shown in Figure 1 and Figure 2. There are a total of 460 top view images available in the dataset from the provided 1150 images. Out of the 460 top view images, only 230 of them are labeled. These 230 images are split evenly between resistors that are benign and resistors that are defective. Since

SVMs are supervised learning models that require labeled data, our model will be trained exclusively on these 230 labeled top view resistor images[3].

3 Model

The model presented here builds upon the findings of Alam et al. [4], who conducted a similar experiment involving the detection of defective epoxy in integrated circuits. In their work, they utilized a VGG16 model, a convolutional neural network (CNN) that is a predecessor of VGG19. By extracting relevant features from the images, they applied a k-means clustering algorithm to group similar features and identify defective epoxy samples based on these clusters[4].

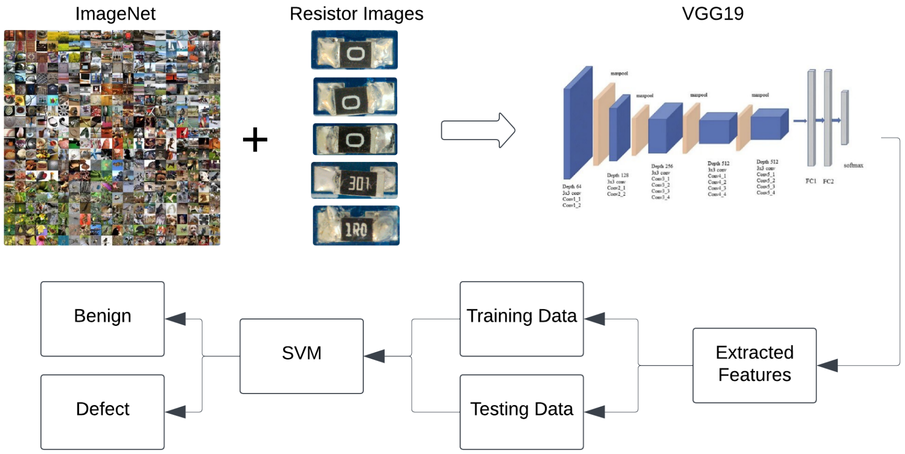


Figure 3: Visualization of the Pipeline [5]

The pretrained VGG19 dataset is used to extract the features of the 230 labeled resistors described in Section 2.2. With the combination of the ImageNet dataset and the newly added resistor images, VGG19 outputs the unique features of each of the 230 images as a numerical array. The extracted features from the VGG19 model serve as the input to a SVM classifier, which is trained to distinguish between defective and benign samples. The SVM is particularly well-suited for this task as it is adept at finding a hyperplane that separates classes in the feature space with maximum margin. Using the labeled dataset, the SVM learns to map the extracted features as either benign or defective, effectively training it to classify unseen samples with similar patterns. Between the VGG19 and SVM step, a logistic regression model is applied to reduce the dimensionality of the data. This excludes extracted features that are outliers, hence only training the SVM with features that occur regularly, or features that have large weights. In the experiment section, the results of using a logistic regression model and not using a logistic regression model will be compared.

By combining the feature extraction capabilities of the VGG19 model with the classification power of the SVM, the pipeline can detect whether the resistor images are defective or not to some accuracy. Figure 3 illustrates the end-to-end workflow of this process, beginning with the feature extraction step and concluding with the classification of images into their respective categories.

4 Experiment

As described before, the data used is from the SolDef_AI dataset. The first step in running the pipeline is to crop each of the images to include just the resistor. This is a crucial step as the VGG19 model should only extract features that are related to the resistor and not the background of the image. Figure 4 shows the cropped photo.

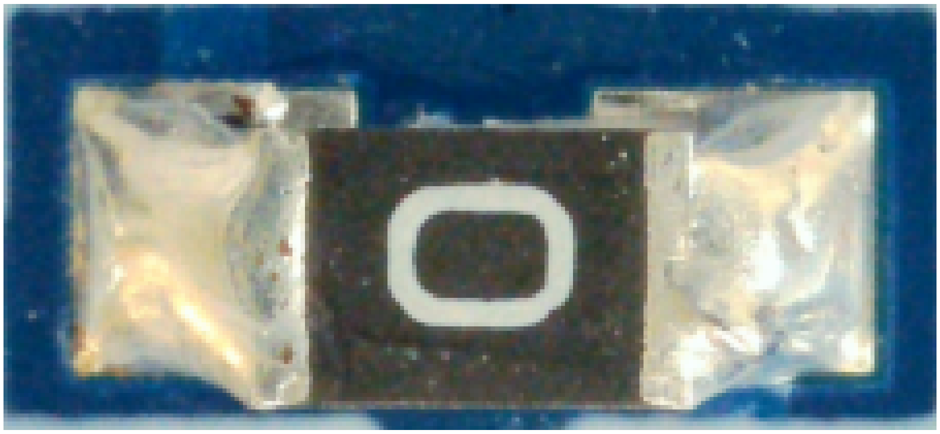
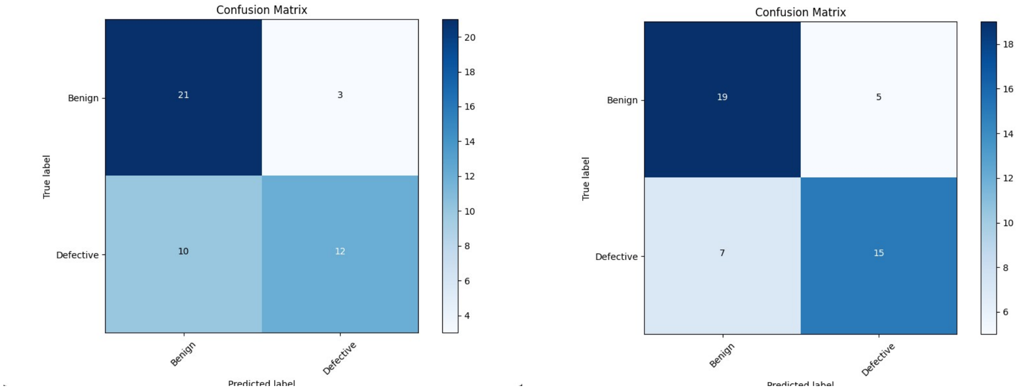


Figure 4: Cropped Resistor Image

For this experiment, two pipelines are used to test the difference between the results of the data dimensionality. The pipeline without the logistic regression is experiment 1, and the pipeline with the logistic regression is experiment 2. The results can be seen in Figure 5. The overall accuracy for experiment 1 and experiment 2 respectfully is 72% and 74%. Although the average accuracy is about the same in both experiments, experiment 2 proved much better results compared to experiment 1 when it came to identifying defects correctly. Experiment 1 had a high recall rate for detecting benign data 88%. However, experiment 1 only had a recall rate of 55% when identifying defected data. Experiment 2, which had a slightly lower recall rate at 79% when identifying benign data, had a much higher recall rate identifying defective data, 69%. The reason behind the imbalance between the benign and defect data in experiment 1 is due to the expansive feature set the SVM is trained on. Without the data dimensionality reduction, each image sample outputs more unique features. This results in the SVM model overfitting to the benign data, as it struggles to generalize the patterns indicative of defects due to the higher variability in the feature space. By introducing the logistic regression model for dimensionality reduction in experiment 2, the feature set becomes more compact and focused, helping the SVM better distinguish between benign and defective data. This dimensionality reduction minimizes noise and redundant information, allowing the classifier to emphasize the most relevant features for defect detection.



(a) Pipeline without Logistic Regression

(b) Pipeline with Logistic Regression

Figure 5: Confusion Matrix

5 Conclusion and Future Work

The results of the experiment highlight the strengths and weaknesses of the VGG19-SVM pipeline. With an accuracy of only about 74%, the pipeline isn't nearly accurate enough for real world scenerios. However, the results indicate that with additional improvements, better results are a possibility in future iterations. To improve the model, several future enhancements can be considered. First, increasing the size and diversity of the dataset, particularly for defective resistors, could significantly improve the model's ability to generalize. This could include data augmentation techniques such as rotating, scaling, or altering the brightness of the existing defective resistors to simulate a wider range of defect patterns. Using different data dimensionality reduction techniques, such as PCA, or incorporating more robust machine learning models for classification such as a CNN or a General Adversial Network(GAN), could provide better results as well. Overall, improvements that can be made to the current model. The current model, as is, proves to the possibility of using machine learning for defect detection in resistors, but it also highlights the challenges that need to be addressed. The combination of VGG19 for feature extraction and SVM for classification demonstrates a promising approach, yet its limitations emphasize the importance of refining both the dataset and the model.

References

[1] D. Mehta, H. Lu, O. P. Paradis, M. A. M. S., M. T. Rahman, Y. Iskander, P. Chawla, D. Woodard, M. M. Tehranipoor, and N. Asadizanjani, "The big hack explained," *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, vol. 16, pp. 1 – 25, 2020.

[2] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," 2015.

[3] G. Fontana, M. Calabrese, L. Agnusdei, G. Papadia, and A. Del Prete, "Soldefai: An open source pcb dataset for mask r-cnn defect detection in soldering processes of electronic components," *Journal of Manufacturing and Materials Processing*, vol. 8, no. 3, 2024.

[4] L. Alam and N. Kehtarnavaz, “Improving recognition of defective epoxy images in integrated circuit manufacturing by data augmentation,” *Sensors*, vol. 24, p. 738, 01 2024.

[5] R. Hewage, “Extract features, visualize filters and feature maps in vgg16 and vgg19 cnn models,” 2024.