A Survey on Circuit Recognition using Machine Learning

Kallakunta Ravi Kumar

Associate professor, Department of ECE, Koneru Lakshmaiah Education Foundation,
Guntur, AP

Abstract:

Characteristic aspects of circuits and putting required algorithms were useful in resolving various software issues. For machinery reliability reviews, reverse engineering is a pre-requisite, method of bringing out first-level elements from bit-level elements. As ceptical circuit was given, alassical perspective is to find a group of applicant functions and to use approved strategies for marking them. characteristic helpful options of famous justifications and collection recommended aspirants of hidden chunk, square measure necessary moves. Convolutional neural networks are used mostly in machine learning since in the view of fact that are typically pre-set options are not required. Deep networks with numerous process sheets are useful for learning hidden structures of objects throughout existing methods. In this work, it is important for representing logic circuits for CNN process, A replacement circuit illustration is evolved for organizing the circuit-based convolution for functioning with energetic pooling. supported this formatting, a deep learning framework mistreatment CNNs to acknowledge circuit functionalities was engineered. Compared to reference strategies supported support vector machines (SVM), practical exhibits the effectiveness of planned CNN methodology for each circuit codification also as operate recognition and placement. With correct training, logic gate elements with hidden bugs, the planned framework identify the elements with an accuracy in the range of 80-92%, and capable of finding malware elements in the hardware integrated circuits.

Keywords: Circuit Recognition, Machine Learning, Hardware Security, Image Recognition, Reverse Engineering

1. INTRODUCTION

To secure any hardware system, reverse engineering was an important step to check the vulnerabilities in the system. Reverse engineering can be explained as back engineering; it is just like scientific research the only variation is reverse engineering can be used in computer fields. For uprooting the first-level components from a low or bit-level design we are using reverse engineering. A method to validate a set of operations apply some validate methods to verify it. The Algorithm supervised learning[1], a subdivision of machine learning techniques that depends ina data set or instruction set. It covers some group of input examinations and projected outputs. Identifying some different aspects of first-level concerns and accumulating real information about mysterious blocks are important for reverse engineering.

CNNs are accustomed in machine learning because it does not require pre-defined features. Deep networks with different refinement layers are helpful in learning obscure structures in the training process. This paper presented a different circuit presentation and constructs a substructure with CNNs to identify circuit features. Examinations represent the operativeness of the suggested method for the categorization of circuits. An image described as a matrix of picture elements that are arranged in the format of rows and columns [2]. Every small picture element here considered as a grayscale image. a grayscale image is normally called a black and white image but the name itself indicates and include multiple shades of grey.

In 8-bit grayscale image, each component in the picture have some specified strength which ranges from 0 to 255. here 0 indicates (black) and 255 represents (white). The range of the pixel values depends upon the color depth of an image [3]. The grayscale images are two types of images: vector graphics and bitmaps. The most common file formats are GIF and JPEG. These images are will be taken in to account for validation of the hardware IC design. In hardware reverse engineering, the extracted images and then the IC net list can be generated, and then the logic can be reproduced. It helps to validate the security of IC after manufacturing. In this work, we took different benchmark circuits to train and tested the circuits for identification of the circuit elements using CNN.

The present paper is organized as follows: Section 2 consists of related work, Section 3describes the proposed methodology, Section 4depicts the experimental setup and working of the setup, Section 5 demonstrates the Results and Discussions, and finally Section 6 presents the conclusion of the work.

2. RELATED WORK

Souhail et al. presented a multiple objects detection technique using OpenCV libraries [5]. Cascade classifiers were used in object detection, applicable to simple to complex applications. Maliha Khan et al. presented a face identification and detection method for identification using Principal Component Analysis [4]. It resulted less amount of data storage for feature space to denote the data. Shopa et al. demonstrated a traffic sign recognition platform, the traffic symbols in a video sequence recorded by the existing vehicle camera. With the help of open CV, the images were classified accurately, even in the disturbed background environment. The results were compared with different threshold techniques corresponding computational complexity.

During an integrated circuit design to fabrication flow, several steps need to follow for a malware free and without any damages. During the IC design flow, the IC hardware was also vulnerable to more attacks like scan chain attacks [7] and reverse engineering techniques. To provide safety and strong cryptographic keys to provide strong protection to the crypto system, a secured physical unclonable function based random number generator was proposed [8] to prevent from image based reverse engineering attacks [10, 11].

Pictures are the most common form of spreading information. pictures incisively convey information about their positions, sizes, etc. Image selection is a method of describing the relevant data type and source and also some relevant instruments to collect data. After an image is being retrieved and integrated from different sources and filtered, it is loaded into a storage system that may be a cloud. They are divided into three types. Picture reducing, picture quality, recreation, calculation Extended. As mentioned, human beings are foremost visual creatures. Human beings not only see the things to conclude them and also search for variance. Let us consider a digital picture. A digital pictures will consider all values are in a different format. It willtake only a numerical values[4]. It ranges depend on the brightness of the image i.e 0(black) to 255(white). Another name for digital picture can be called as an array of discrete spots. These spots are known as pixels. Commonly, they are divided into a rectangular shape of pixels. So that, each pixel itself can be is a small rectangle. once it is completed, All pixel was given in a pixel number that represents the pixel color [5, 12]. Moreover, if the area of the pixel is too short then the discrete characteristics are not visible to the human eye. This has some benefits in image processing.

Machine Learning is a subcategory of Artificial Intelligence. Where machines learn on their own through their experience without being explicitly programmed. Machine Learning is categorized as Supervised, unsupervised, and reinforcement learning, In this work, asupervised learning is described as an example of inputs and corresponding required outputs provided by the system. SVM full form is support vector machines. These are supervised learning paradigms that inspect the data for classification. SVMs can be used to solve the text organization. The main goal is to divide the given information in the best possible way[6]. Machine learning studies and predicts the output based on their observations, While AI indicates an agent interaction with the environment and actions.

Recognizing hardware bugs in a different models it is a great exciting because many big range circuits such as arithmetic operator boundaries have disappeared in gate level circuits. In the course of fabrication, there are some defects usually found on circuit boards[7]. To overcome this issue, we are using reverse engineer a gate-level circuit. This process consists of two parts. i) designing a gate-level circuit into logic blocks. ii) Arranging small-level circuit blocks to high-level elements. In general, reverse engineering is nothing but identifying and placing practical equipments from gate level circuits. The keep going frameworks beginning with discovering group of person words and operators with operative approaches, and registered some normal methods to each person[8].So that demonstrating with normal methods is time complex. To validate a equipment that can be a person, special characteristics are identified to notice the particle equipment. for example ,used simulation graphs of a normal block to identify the arithmetic operators. Even so, that the attributes and varieties of specified properties adequately impact the accuracy of people search, and to be sure about the performance of the overall algorithm.

3. Proposed Methodology

A convolution neural network (CNN) is a deep learning algorithm. It takes the input image then it provides the priority according to weights, structures and ability to segregate one from the other. Fig.1 depicts the present methodology of the circuit recognition system. It uses the inside shape of data with the convolution layers which contain computational units. These networks are broadly used in image processing and computer vision. Some present-day research also applies to text simplify and graph structure. A considerable benefit of CNN in the presence of need on physical efforts in planning and identifying different varieties. Few of the machine learning methods depend on applicable varieties as attentions to goal a large -end targets. Meanwhile, Itneed pre-processing of information or data. This network is need for spotting important ways that may need or need not be physically described in another function.

Step 1: Summarize the needed components for representing the circuits to work with CNNs. This will applies to another circumstances need for some entities and transformed to an array of vectors penetrated with real digits will work with CNNs.

Step 2: Introduce a complex action on circuits to constitute between structural and functional properties. This working leads to two data formats with various data sizes and representation abilities.

Step 3: Use the dynamic grouping to separate a logic element into a constant number of groups. The last presentation of a circuit will maintain the globally related position of groups.

Step 4: conceive the most important thing to identify typical properties for each group.

Step 5: With CNNs, we construct a structure to categorize and identify arithmetic operators from gate-level circuits. Practical output in various things are discussed and presented. This structure can serve in the reverse engineering of circuits. For example, given a suspicious circuit, the above mentioned can advice the most applicable operator use for further problems, and the idea is to detecting functions thatcan be applied to malware detection in various circuits.

Step 6: SVM also used, a supervised learning algorithm used for classification of hyper planes, to identify circuits based on a group of unknown properties and also features produced for CNNs. This work successfully implemented CNNs for circuit recognition.

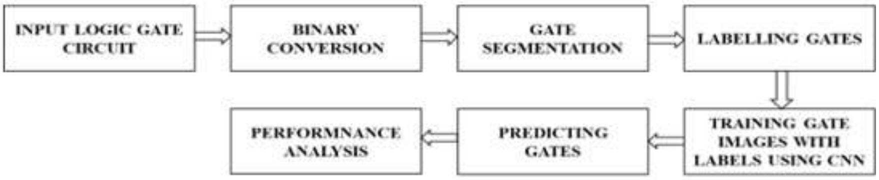

Fig.1 Block Diagram of proposed methodology

4. Experimental Setup and Working

The circuit elements recognition system is implemented on Windows 10 Operating system includes Intel i7 core with 16GB RAM. The training of the network is carried out on the same machine for recognizing the different circuit elements.

In this process, Initially, we took an Input logic gate as an image. Image selection is defined as a process of determining the suitable data type and source and also relevant instruments to gather data. Image loading indicates the load element. Afterimage is retrieved and added from different sources, cleaned and generated then loaded to a system where it can be stored such as the cloud. Then the image is converted into binary also called a binary conversion. Fig. 2 shows an example of a full adder circuit and Fig.3 shows the different logic gate elements. A binary image can be described as an image that consists of some pixels that can have one of the two colors, usually black and white. The images are also known as bit or two-level images which indicates that every pixel will be placed in a single bit either 0 or 1. These binary pictures are generated from color images through segmentation. Segmentation can be defined as allocating each pixel in the source image. In Image processing, image division is the segregating of an image into different segments or pixels. It is used to identify and boundaries. After segmentation, the upcoming step is classification. for classifying the images, we used a supervised learning algorithm which is also known as CNN. CNN is usually applied to identifying visual imagery they can also be called shift variant or space invariant networks depends on architecture and characteristics. The main building block for CNN is a convolutional layer. In general, the network layers are fully connected in which a neuron is connected in the upcoming layer. Coming to predictive analysis these algorithms try to achieve a low possibility of error occurrence by using either bagging or boosting. Then, the result is generated in gate forms.

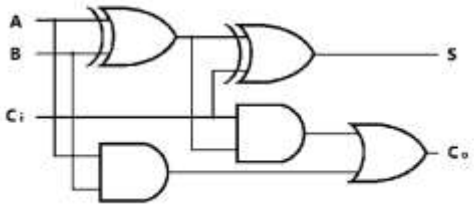

Fig. 2 Full Adder Circuit

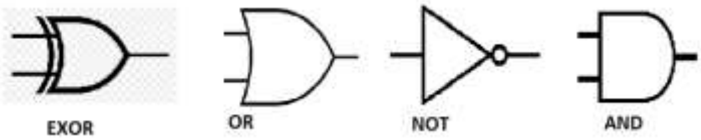

Fig.3 Circuit Elements

5. Results and Discussion

The experimental validation of presented methodology shown in the Table.1 and Table.2. To check the performance, few circuits and ISCAS’85 bench marks circuits are considered. Initially, the basic logic gates namely, AND, OR, EXOR and NOT gates are trained, then after that these gates are identified and counted by the same trained net from the different test circuits and ISCAS’85 benchmark circuits. This can predict the class name accurately and indicator shows how well a given indicator can figure the calculation of expect property of each circuit element.

The important performance metric accuracy will be evaluated depend on the final classification and prediction. This final methodology is evaluated as follows. Accuracy is defined as the ratio of sum of True Positive and Negative to the sum of True Positive, True Negative, False Positive and Negative value of logic elements in test circuits. Table.1 describes the number of gate

elementes like AND, EX-OR, OR and NOT in the benchmark circuits. Table.2 shows the performance analysis of proposed methodology, that proved the identification of logic circuit elements of test circuits.

Table.1 Test Circuits

CIRCUITS	AND	EX-OR	OR	NOT	COUNT
FULL ADDER	2	2	1	-	5
HALF ADDER	1	1	-	-	2
FULL SUBTRACTOR	2	2	1	2	7
HALF SUBTRACTOR	1	1	-	1	3
BINARY MULTIPLIER	6	2	-	-	8
DECODER (2*4)	4	-	-	-	4
MULTIPLEXER (4*1)	4	-	1	-	5
DEMULTIPLEXER (1*4)	4	-	-	-	4
C17	6	-	-	6	12

Table.2 Performance analysis of the proposed methodology.

CIRCUIT	AND	EX-OR	OR	NOT	COUNT (REAL)	COUNT (PREDICTED)	ACCURACY
FULL ADDER	2	2	1	-	5	5	98.4
HALF ADDER	1	1	-	-	2	2	97
FULL SUBTRACTOR	2	1	1	1	7	5	71.4
HALF SUBTRACTOR	1	1	-	1	3	3	96
BINARY MULTIPLIER	4	1	-	-	8	5	62.5
DECODER (2*4)	4	-	-	-	4	4	96.8
MULTIPLEXER (4*1)	4	-	0	-	5	4	80
DEMULTIPLEXER (1*4)	3	-	-	-	4	3	80
C17	6	-	-	6	12	11	91

CONCLUSION

In this work, a deep learning method CNN is implemented to recognize circuit elements for addressing computer-aided design problems. For recognizing a circuit, a framework was proposed, which consists of circuit convolution and other layers and a classical CNN. Experimental results reveal that it can be effective in both in-circuit classification and identification of an operator embedded in test circuits. Here, a few circuits and ISCAS'85 benchmark circuits are tested to evaluate the proposed methodology performance. From the output, it is verified that the proposed methodology proved the accuracy in between 80-92%.

7. REFERENCES

[1] Hsieh, Jun-Wei. "Fast stitching algorithm for moving object detection and mosaic construction." Image and Vision Computing, Vol. 22, no. 4 pp. 291-306, 2004.

[2] Shopa, P., N. Sumitha, and P. S. K. Patra. "Traffic sign detection and recognition using OpenCV." In IEEE International Conference on information communication and embedded systems (ICICES2014), pp. 1-6, 2014.

[3] Paul, Liton Chandra, and Abdulla Al Sumam. "Face recognition using principal component analysis method.", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) vol.1, no. 9, pp. 135-139, 2012.

[4] Khan, Maliha, Sudeshna Chakraborty, Rani Astya, and ShavetaKhepra. "Face Detection and Recognition Using OpenCV." In IEEE International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), pp. 116-119, 2019.

[5] Guennouni, Souhail, Ali Ahaitouf, and AnassMansouri. "Multiple object detection using OpenCV on an embedded platform." In 2014 Third IEEE International Colloquium in Information Science and Technology (CIST), pp. 374-377, 2014.

[6] Chen, Kaili, and Meiling Wang. "Image stitching algorithm research based on OpenCV." In IEEE 33rd Chinese Control Conference, pp. 7292-7297, 2014.

[7] S. Kalanadhabhatta, K. K. Anumandla, S. Khursheed and A. Acharyya, "Secure Scan Design with a Novel Methodology of Scan Camouflaging," In Proceedings of *European Conference on Circuit Theory and Design (ECCTD)*, Sofia, Bulgaria, pp. 1-4, 2016.

[8] S. Kalanadhabhatta, D. Kumar, K. K. Anumandla, S. A. Reddy and A. Acharyya, "PUF-Based Secure Chaotic Random Number Generator Design Methodology," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 28, no. 7, pp. 1740-1744, July 2014.

[9] Becker, Steffen, Carina Wiesen, Nils Albartus, NikolRummel, and ChristofPaar. "An Exploratory Study of Hardware Reverse Engineering—Technical and Cognitive Processes." In *Sixteenth Symposium on Usable Privacy and Security (SOUPS)*, pp. 285-300, 2019.

[10] Tan, Qinhan, SeetalPotluri, and Aydin Aysu. "Efficacy of Satisfiability-Based Attacks in the Presence of Circuit Reverse-Engineering Errors." In IEEE International Symposium on Circuits and Systems (ISCAS), pp. 1-5, 2018.

[11] Anumandla, Kiran Kumar, RangababuPeesapati, Samrat L. Sabat, and Siba K. Udgata. "SoC based floating point implementation of differential evolution algorithm using FPGA." Design Automation for Embedded Systems 16, no. 4 (2012): 221-240.

[12] Anumandla, Kiran Kumar, Samrat L. Sabat, RangababuPeesapati, Prabu AV, JRK Kumar Dabbakuti, and Ranjita Rout. "Optimal spectrum and power allocation using evolutionary algorithms for cognitive radio networks." Internet Technology Letters: e207.