Journal of Hardware and Systems Security (2018) 2:240–250
https://doi.org/10.1007/s41635-018-0041-6

A Novel Counterfeit Detection Approach for Integrated Circuit Supply Chain Assurance

Preston D. Frazier[1] · E. Thomas Gilmore III[1] · Isaac J. Collins II[1] · Wardell E. Samotshozo[1] · Mohamed F. Chouikha[1]

Received: 15 February 2018 / Accepted: 4 June 2018 / Published online: 19 June 2018

Abstract

The electronics industry has become a primary target in the global market of counterfeiting. Counterfeit electronic parts transverse through the supply chain end up in critical avionics, industrial, medical, and military systems, and the financial loss due to these parts is in the billions. A vast majority of counterfeit parts within the electronics industry are integrated circuits. In this paper, a new (near real-time) counterfeit detection process, which is based upon infrared thermal imaging, intensive statistical analysis, and machine learning, to differentiate between authentic and inauthentic electronic parts is presented and then showcased as a highly accurate and cost-effective method to verify hardware authenticity.

Keywords Counterfeit integrated circuit detection · Infrared imaging · Hardware security · Image processing

1 Introduction

The counterfeiting of electronic parts is a potential $96 billion enterprise [1] which creates brand damage for the commercial manufacturers and potentially threatens national security particularly for the USA and its allies. The supply chain of US Department of Defense (US DoD)—which is supplied by some of the leading electronics manufacturers—has been characterized as "high-risk," due in part to its supply chain vendors ineffective and inefficient supply chain risk management (SCRM) practices and procedures [2]. The consequences of counterfeiting have an adverse effect on the reliability of integrated circuits (ICs) in the hardware (H/W) systems they compose. Poor reliability of electronic components leads to reduced performance as well as potential operational failure. The potential failure of critical systems, such as aerospace, defense, and financial systems, which inadvertently incorporate counterfeit electronic parts is the reason why this is an important issue. The H/W reliability issues caused by the proliferation of counterfeit parts have been documented [3].

The steady increase of counterfeit electronic components entering the production supply chains of various IC manufacturers is primarily due to the rampant expansion of the production of H/W systems within the electronic industry and a significant increase of electronic waste (*e-waste*) [4]. Electronic waste is generally defined as unwanted ICs which were mishandled, sanded, or damaged during the retrieval of their components. In the USA, many small electronic part vendors procure parts from brokers, who are assumed to be legitimate. Yet, many of these intermediaries purchase counterfeit items which may be *e-waste* and enter them into the *distribution phase* of the supply chain [5]. However, many of the leading manufacturers of ICs have placed great emphasis on their SCRM processes to thwart counterfeiting to greatly mitigate the risk of operational loss or degradation of their products and uphold their brands [6].

Among the leading electronic component manufacturers, Texas Instruments (TI) and the Intel Corporation use similar standards to mitigate vulnerabilities within their supply chain to impede counterfeiting [7, 8]. In this paper, we focus on Intel and TI, due specifically to their high name recognition and reputation for H/W reliability. Also, analog and programmable ICs, such as those produced by TI and Intel, respectively, have the highest and second highest occurrences of counterfeiting of all semiconductors [9]. The leading counterfeit detection techniques [10, 11] such as material analysis like Fourier transform infrared spectroscopy (FTIR), confocal scanning acoustic microscopy (C-SAM), and aging analysis such as Tehranipoor's work neural network modeling of aging mechanism and Guin's research in combating IC recycling are all utilized within on-chip structures, and their

✉ Preston D. Frazier
preston.frazier@howard.edu

[1] Department of Electrical and Computer Engineering, Howard University, Washington, DC 20059, USA

implementation is either not cost effective (based on the cost of the board) or is destructive in nature [12–23]. Also, there have been material analysis work employing terahertz (THz) pulsed laser systems by Ahi. The THz systems are presently not widely used for counterfeit detection as the resolutions of THz images are not as precise as X-ray microscopy [24]. Yet, THz systems are effective and non-destructive material analysis method to authenticate electronic components [25–27]. Other novel counterfeit detection processes, such as parametric testing including hue-saturation-intensity transformation, and emission spectrum analysis, Markis's work with supervised machine learning, and Bhunia's efforts in scan-based authentication are non-invasive and function in near real time, but they are either labor intensive or do not test for a broad range of counterfeit triggers such as inconsistent markings and thermal stress [28–35]. There have been novel approaches to thwart and detect counterfeit ICs through the utilization of embedded nano-signatures (ENS) onto the electronic components [36, 37]. ENS are fabricated at the manufacturer side of the supply chain and a cipher key and the coding lookup tables are provided to the consumer using a secure direct line between the authentic manufacturer and the consumer [36]. This novel approach of ENS basically interdiction of fraudulent ICs into the supply chain as potential counterfeiters would not have the ability to decrypt the nano-signatures on the electronic parts. Yet, this method may be viewed as expensive process by the manufacturers given the nominal cost of the parts being encrypted. There are also structural tests for counterfeit detection such as malicious alteration recognition and verification by emission of light (MARVEL), which employs optical diagnostics and electrical tests to detect chip alterations. Yet, MARVEL is not sophisticated enough to analyze certain ICs [38]. Other counterfeit detection approaches such as Chen and Hu et al. [39] have examined utilizing the unique current and voltage characteristics of transistors employed in ICs to ascertain counterfeit ones as well as Zheng's work [40] exploiting dynamic supply current to detect counterfeit ICs. Yet, this emerging technique needs to be further work to fully understand its potential. Also, there is a counterfeit detection processes analyzing printed circuit (PCB) unique signatures based on variations in its trace impedances [41]; this approach is also labor intensive. There is a novel counterfeit detection method that analyzes non-volatile memory of system on chip (SoC) ICs [42], but its application is not broad. A vast majority of the aforementioned counterfeit detection techniques have been applied to prevent fraudulent semiconductors from initially entering the supply chain. However, a more crucial challenge facing many system integrators (e.g., US DoD) is these methods do not adequately address the issue of fraudulent parts already in the supply chain (i.e., counterfeit components that have the correct—or equivalent—die and those that come from original component manufacturer (OCM)-approved second party vendors). There have been several works utilizing infrared thermography (IRT)—recording of images after or while thermally stimulating the inspected component—as non-destructive inspection (NDI) method that the authors have examined. Zhang's work with utilizing to IRT and signal-to-noise ratio (SNR) measures as a NDI process to ascertain impact loading in fiber-reinforced polymer specimens and defects in polymer composite materials [43, 44] as well as employing micro-laser line thermography, and finite element analysis as a NDI process to discover micro-sized flaws in stitched carbon fiber-reinforced polymer composites [45] has applicability in the detection of counterfeit ICs. Also, Fernandes et al. [46] utilizes IRT to analyze fiber orientation on laminates.

In this paper, we showcase an NDI method to assess counterfeit ICs from non-counterfeit ICs. This technique is similar to IRT. By applying thermal imaging, statistical analysis based on a time registration algorithm, and machine learning algorithms, we are able to showcase a superior ability to identify non-counterfeit ICs from counterfeit ones. The remainder of the paper is structured as follows. The next section furnishes an elucidation of the new approach for detecting counterfeit parts by employing ICA and leveraging one of the leading supervised learning algorithms with dynamic time warping-aligned features. While the testing environment for the experiments conducted for this work is presented in the third section. The fourth section showcases the results along with a comparative analysis of the three leading classifiers for the Intel and TI PCBs, and the conclusions are noted in the fifth and final sections.

2 Counterfeit Detection Approach

Our current research in ascertaining counterfeit parts is done by employing blind source separation (BSS) to analyze the validity of potential counterfeit PCB against a benchmark device, "Gold Standard." The Gold Standard is an electronic device proven to be legitimate either via product verification through the OCM or certified brokers or by way of passing previously run counterfeit detection tests. Using this new approach to focus on individual components' infrared (IR) signal emission from both the Gold Standard and the alleged counterfeit PCB is a way to effectively prevent supply chain infiltration by inauthentic devices.

An overview of our IR analysis counterfeit detection approach is presented in Fig. 1. The high-level illustration is based on the applied algorithms mentioned in the previous section and presented in this section. The methodology as depicted in the aforementioned figure is based on the

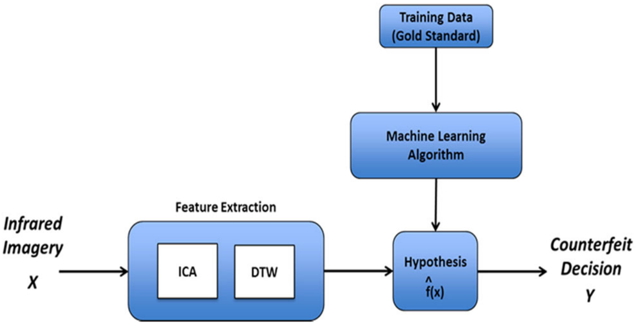

Fig. 1 Overview of the counterfeit detection methodology

collection of multiple thermal signatures given off by various OCM ICs. A classical machine learning approach is presented where the input of the potential counterfeit PCB is denoted by *X*, i.e., the feature data, and the output is *Y*, the classification label. There should exist a relationship or pattern between the input and output values. This relationship is accomplished by the function $y = f(x)$, which is known as the target function. However, $f(x)$ is an unknown function so the learning algorithm tries to guess a "hypothesis" function $\hat{f}(x)$ that approximates the unknown function $f(x)$. The set of all possible hypotheses is known as the Hypotheses set $\hat{F}(x)$, and the goal of the machine learning algorithm is to ascertain the final hypothesis that best approximates the unknown target function.

2.1 Concept of Blind Source Separation

Blind source separation (BSS) is a concept where the separation of a set of signals from a set of mixed signals can be achieved, without prior knowledge about the content or structure of the mixed signals. This can be achieved using to assumption that the original source signals are mutually statistically independent. The mathematical representation for BSS is presented using the following equation:

$$\boldsymbol{x}(\boldsymbol{t}) = \boldsymbol{A}\cdot\boldsymbol{s}(\boldsymbol{t}) \tag{1}$$

where the set of original source signals, $s(t) = (s_1(t), \ldots, s_n(t))^T$, is mixed using the matrix, $A = [a_{ij}] \in \mathbb{R}^{mxn}$, to produce a set of mixed signals, $x(t) = (x_1(t), \ldots, x_n(t))^T$. Usually, n is equal to m. When $m > n$, the system of equations is overdetermined and the unmixing can be obtained via conventional linear methods. When $n > m$, the system is underdetermined and a non-linear method must be used to recover the original signals from the mixture, respectively. These signals can be multidimensional which the case for this research is. Extending this mathematical representation to the problem of electronic components verification, the thermal emissions emitted by the electronic components on the integrated circuit board are represented by $s(t)$ which are assumed to be statistically independent, A represents the mixing matrix, and $x(t)$ represents overall board signatures [47].

2.2 Independent Component Analysis and the Fast Independent Component Analysis Algorithm

Independent component analysis (ICA) is a computational method for discovering embedded structures from within mixed signals. ICA assumes a statistical model whereby the observed multivariate signals are linear or nonlinear mixtures of some unknown hidden variables. The mixing coefficients are also unknown, and these hidden variables are considered both non-Gaussian and mutually independent. Finally, it is these hidden variables that are known as the independent components of the observed data. It is through the ICA approach that these independent components can be determined. *Fast independent component analysis* (FastICA) is an efficient and well-known algorithm for independent component analysis. FastICA uses Newton's method on an approximation for negentropy, negentropy being its measurement of non-Gaussianity. This method is selection-based on the estimated statistical measures of the original signals. FastICA is particularly fast simply because of the numerical method and approximation it uses [48].

As a means to demonstrate the FastICA algorithm, we utilized two independent source signals from an examined PCB, captured by a pair of IR cameras, which are to be mixed then separated. Please note, further experimental details of the PCBs used will be described later in the manuscript. The IR signatures from different electronic components on the PCBs along with any noise present would be the inputs of the two cameras. Inputting these two captured unique mixtures into the FastICA algorithm will allow the recovery of any of the individual signals present on the PCB. In our approach, we recover unique thermal signatures of test board components off of the PCB examined to produce a result to be compared to known authentic board, i.e., *Gold Standard*. After FastICA is applied, the matrix in (1) rotated back to its original axis and re-projected into the original coordinate frame. The rotation is performed by minimizing the Gaussianity of the data projected on both axes [fixed point ICA]. By rotating the axis, FastICA is able to recover the original sources which are statistically independent. This property of this effective process comes from the central limit theorem which basically states any linear composite of two independent random variables is considered to be more normal (Gaussian) than the original variables alone [48].

2.3 Machine Learning Techniques

Support vector machine (SVM), a supervised machine learning algorithm typically used for classification or regression problems, was implemented in this framework due to its effective in high dimensional spaces (collected IR measurements from the *Gold Standard*). This algorithm, also known as support vector networks [49], is a machine learning techniques that assesses observed data to determine patterns based on statistics. The research problem presented here is posed as a binary or binomial classification task with the goal classifying thermal emissions from the test board into two categories, i.e., counterfeit or not counterfeit, respectively. Binary classification is dichotomization applied to this challenge, and therefore, an important point is that in many practical binary classification problems, the two classes or categories are not symmetric, meaning that rather than overall accuracy, the relative proportion of different types of errors is of interest. For example, in testing electronic boards, a false positive (detecting a counterfeit component when it is not present) is considered differently from a false negative (not detecting a counterfeit component when it is present). To reiterate, for this research, we initially use two classes ($z \in \pm 1$) noted counterfeit and not counterfeit (ergo authentic).

A set of *Gold Standard* ICs developed from a set of trusted devices was used to train the classifier. These devices were obtained directly from the manufacturer, respectively. For this research, there is no requirement for a priori information about potential counterfeit PCB characteristics. A set of thermal measurements were initially captured from the trusted ICs via multiple infrared camera:

$$\mathbf{Y}_{\mathrm{i}} = \{Y_1, Y_2, \cdots, Y_k, \cdots, Y_n\} \tag{2}$$

which represents the IR signature vector of the ith camera ($i = 1$ or 2) and n denotes the thermal emission measurements captured over the predetermined time interval. These observations were within a tolerance that deemed them authentic $\mathbf{Y}_j = (Y_{jt_{low}}, Y_{jt_{high}})$, $j = 1, \cdots, n$.

In other words, there is an acceptable region of IR signatures for the *Gold Standard* and only ICs that are authentic or have limited process variations will be used to train the classifier. The *Gold Standard* was generalized by device type and defined statistically using a learning algorithm that attempts to determine the hidden structure within the IR signatures being tested. For this paper, we initially leveraged a series of two class classifiers to assign a decision function, f, where $f(\mathbf{Y}) = 1$ when the PCB is designated to be authentic and $f(\mathbf{Y}) = -1$ when the PCB is determined to be counterfeit. Once the machine learning algorithm was trained, the classifier was capable of determining whether a test PCB, not from the OCM or their authorized distributors, were counterfeit. Further information on this type of classifier may be found in [49].

As part of our performance assessment of machine learning algorithms and ability to detect counterfeit devices, the naive Bayes approach was evaluated. This algorithm is one of the leading supervised learning techniques given its simplicity to implement. Additionally, naive Bayes is recognized as an especially accurate classifier when used with larger training sets [50].

The naive Bayes classifier was consistently trained to detect whether the PCB compared to the *Gold Standard* was counterfeit over variety of different manufacturers. Further treatment of this machine learning algorithm is deferred to [51].

The third and final machine learning algorithm considered was learning vector quantization (LVQ). LVQ is a nearest-neighbor-based algorithm composed of a set number of processing modules. Each module consists of $n \times 1$ reference vector and is associated with one of the mapping of the input data in (2). Further treatment of this algorithm is deferred to [52].

2.4 Time Registration

A preprocessing procedure to align temporal signals of the *Gold Standard* and the potentially counterfeit IC's thermal signatures is required. This is needed to address differences in both signal compression and time scale. Here, dynamic time warping (DTW), a versatile algorithm to accurately map discrepancies among varying time indices [53], is employed. DTW is used to generate the coordinated features for the aforementioned machine learning algorithms. Specifically, the normalizing factor and the minimum unnormalized distance between the *Gold Standard* and the commercial manufacturer devices from the ICA are additional features leveraged for both training and testing the supervised learning techniques described.

DTW is a similarity measure [54], which represents the distance between the reference measurements in (2) and the test samples denoted below

$$\mathbf{T}_i = \{T_1, T_2, \cdots, T_l, \cdots, T_m\} \tag{3}$$

where m represents observed thermal signals over time. Given the pair of signals in (2) and (3), to align these two signals employing DTW, a distance matrix $[n \times m]$, $\mathbf{D}$, containing Euclidean distances between all pairs of points, $[\mathbf{Y}_i, \mathbf{T}_j]$ is constructed:

$$d\left(Y_k, T_l\right) = |Y_k - T_l| \tag{4}$$

Each matrix element (k, l), where k, $l > 1$, is related to the precise sequencing between the points Y_k and T_l. DTW is proven efficient computationally in ascertaining the optimal path because it identifies a sequence of partial paths and maintains the best local path [55]. This is achieved by recursion to determine the cumulative distance. The cumulative matrix **P** for the warping path is then defined as

$$P(k,l) = d(Y_k, T_l) + \min\{P(k-1, l-1); P(k, l-1); P(k-1, l)\} \qquad (5)$$

The optimal total distance between thermal emissions, **Y** and **T**, after registration is achieved and can be denoted as $q_{DTW} = P(k, l)$. Utilizing DTW, we are able to accurately compare the similarity of time series with different lengths. Next, the H/W environment used in the research is introduced.

3 Inspection of the Leading Integrated Circuit Manufacturers' Hardware

We conducted an initial analysis on authentic PCBs received from Intel and TI. We examined Intel Galileo and TI MSP-EXP430G2 as they are the leading ICs. We also procured numerous non-OCM PCBs to register as the potential counterfeits for this initial examination. We conducted external visual inspections and captured optical information.

The authors did not visually notice any apparent optical differences between the Intel manufactured ICs and the non-OCM Intel Galileo ICs. Regarding the non-OCM purchased TI MSP-EXP430G2, there were boards missing several markings, such as Restriction of Hazardous Substances (RoHS) symbol and pin identification numbers, in comparison to the OCM TI MSP-EXP430G2 ICs. Also, a few of the non-OCM purchased MSP-EXP430G2 ICs were of a darker color of red and had an additional (mismarked) labels in contrast to the TI-manufactured MSP-EXP430G2 ICs. Figures 2 and 3 display a described *Gold Standard* (authentic) and one of the purported counterfeit (inauthentic) PCBs for Intel and TI, respectively.

We used two data sets for our experiments, which were developed through acquisition of IR imagery and application of the ICA algorithm. Test data sets for all the Intel and TI boards were acquired and consisted of 24-bit, red-green-blue (RGB) images which were captured using a pair of FLIR Systems A655sc® IR cameras at a rate of 30 frames per second (fps). For purpose of these experiments, the camera resolution was reduced from a maximum resolution of 640 × 480 pixels to 160 × 128 pixels to improve computational performance while maintaining efficacy, and the camera lenses were positioned approximately 7 in. vertically above the test boards, 5 in. apart, and at an angle of 45° with the focus primarily on the boards' processor. Long wave infrared (LWIR) was used which covers the most common thermal range of 7 or 8 μm to 14 μm. This range was desired because it is the largest coverage of IR camera spectral ranges and can be used on a wide variety of testing boards. We employed the MATLAB 2011b software (S/W) for signal analysis and Visual C++ (2010) with Open Source Computer Vision (OpenCV) specifically for real-time signal analysis running within a Windows Operating System (O/S) environment. All machine learning experiments were conducted using the Python programming language and scikit-learn. Scikit-learn is an open source machine learning library for the Python programming language. Additionally, Python numerical and scientific libraries NumPy and SciPy were used. The program's end-to-end evaluation time to assess a test board was approximately 3 s per experimental trial. The resulting thermal signatures are showcased.

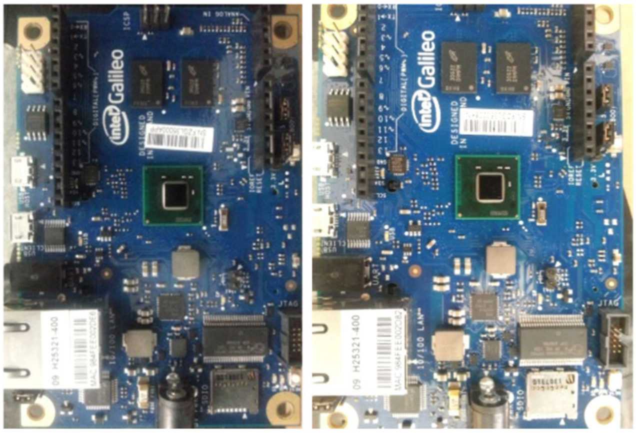
Fig. 2 Images of the Intel Galileo Gold Standard (on the left) and a potential inauthenic board (on the right)

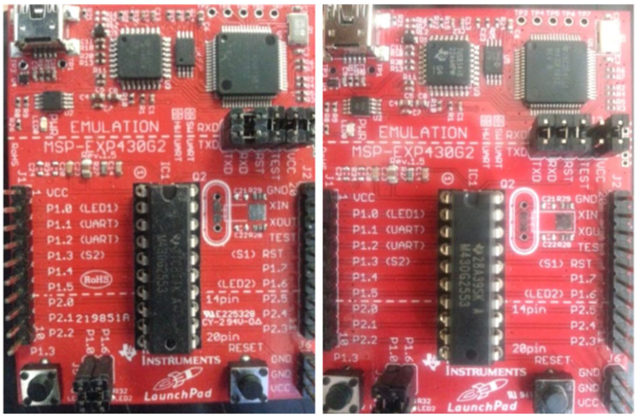
Fig. 3 Images of the TI MSP-EXP430G2 Gold Standard (on the left) and a potential inauthentic board (on the right)

3.1 Inspection Environment for Intel

For the experimentation, we obtained our non-OCM Intel Galileo boards online. The online companies were chosen due to the availability of the Galileo boards and price point (which is a key factor in purchasing electronic components). The H/W specifications for the Galileo PCBs are stated in Table 1. The PCBs were provided power internally—individual power supplies (five-volt output)—and externally from a function generator. The specifications for the voltage pulse

Table 1 Specifications and testing environment details for examined hardware

Hardware specifications	Intel	Texas Instruments (TI)
Board name	Galileo	MSP-EXP430G2
Board type	32-bit Mocrocontroller	Low power mixed signal microcontroller
Memory	8 Mbyte NOR flash	16kB flash
Operational voltage (V)	3.3–5	3.3–5
Dimensions (mm)	123.8 (L) × 72.0 (W)	66.675 (L) × 50.8 (W)
Peripherals	Full sized mini PCI slot, 100 Mb Ethernet port, Micro-SD slot, RS-232 serial port, USB Host and Client ports	MSP430G2553 IC, MSP430G2452 IC, Micro Crystal Oscillator 32.768 kHz
Testing pulse specifications		
Frequency (milli = 10^{-3} Hz)	205	65
Peak-to-peak voltage (amplitude volts)	10.0	3.3
Voltage offset (DC volts)	0.0	3.3
Applied signal type	Sinusoidal	Sinusoidal
Testing ambient temperature range (°F)	74–81.3	72.4–81.6

from the generator used on each test board are listed in Table 1. One of the OCM Galileo ICs procured was designated as the *Gold Standard* (a priori). The resulting thermal images for Intel Galileo PCBs can be seen in Fig. 4.

3.2 Inspection Environment for Texas Instruments

The test environment for the TI MSP-EXP430G2 PCBs was similar to the one set up for the Intel ICs. We obtained the non-OCM PCBs from a reputable online vendor due to the availability and cost point. We produced a generalized test pulse signal to send to the boards. However, due to the different H/W specifications for the TI PCBs (as shown in Table 1), it necessitated a more uniquely tailored test signal. One of the TI boards was designated as the *Gold Standard* (a priori).

The output of the function generator was connected to the *Ground* (GND) and *Test* pins of each of the experimental TI PCBs. A power source was supplied to the main GND and voltage peak-to-peak pins of these experimental boards. With the initial pulse parameter values, the desired test pulse output was not optimal visually, i.e., the signal period was too frequent to capture by the thermal cameras used. Therefore, various adjustments were made. We decided to employ a more optimal frequency in order to produce more visible periods in the range of seconds as opposed to minutes (listed in Tables 1 and 2). This decision reduced the total algorithm run time to 14- and 16-s periods for the manufacturer's processor and IC, respectively. Since the TI H/W is designed to function independently of the power supply, offset and peak-to-peak voltages were utilized to allow the board to receive sufficient voltage to remain functioning with the addition of a pulse voltage. The resulting thermal images for the TI MSP-EXP430G2 PCBs can be seen in Fig. 5.

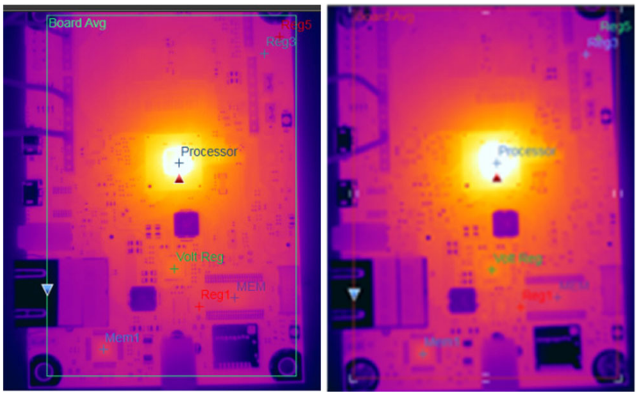

Fig. 4 Thermal screen shot of one of the authentic Intel Galileo experimental PCBs (dubbed the Gold Standard) (on the left) and one of a possibly counterfeit Intel Galileo experimental PCBs (on the right)

4 Device Authenticity Verification Results

We present the results of our examination on the practicality of this counterfeit detection approach—implementation of thermal imagining with DTW features and a supervised learning algorithm—for determining whether a PCB is authentic or possibly counterfeit and thereby unreliable. We conducted an extensive series of simulations to validate the theoretical methodology and technical approach described in this work. We first generated the *Gold Standard* via ICA using our authentic test boards. The experimental simulations consisted of multiple IR video test data with an application of the ICA algorithm. For each experiment, several LWIR videos were acquired each approximately 5 min in length, and we assumed that each individual electronic component on the board has the same kind of temporal dependencies (i.e., non-stationary smoothly changing variances). Additionally, each test board utilized a specific test load, and the videos were recorded

Table 2 Classification summary and insights

Algorithm	Parameter type	Parameter set	Key insights
Support vector machine (SVM)	Kernel-type cost gamma	Radial basis function 10, 20, 30, 40, 50, 60, 70, 80, 90, 100 2–2, 2–1, 0, 21, 22, 23, 24, 25, 26, 27	Highly accurate, performed consistently for counterfeit detection of tested electronic devices Performed well for high dimensional data sets Inefficient classification training process May not scale well for "industry scale" applications
Naive Bayes	Model kernel type	Multinomial, Boolean, Bernoulli Radial basis function	Highly accurate, performed consistently for counterfeit detection of tested electronic devices Computationally simple and low complexity Converges quicker to solution than SVM and LVQ algorithms
Learning vector quantization (LVQ)	Learning rate Learning rule 1st layer hidden neurons	0.01, 0.02, 0.03, 0.04, 0.05, 0.06, 0.07, 0.08 LVQ1, LVQ2 4, 8, 16	Least accurate classifier and inconsistent detection performance against tested electronic devices Difficult to generalize across new device types due to dependency on distance or similarity metrics Highly computational and complex; long training times

precisely 10 min after initial powering of the boards to prevent any transients from being captured in the data set.

Integrated Circuit Data Set: A set of four variables (f_1,f_2, f_3,f_4), comprising the unnormalized distance, the accumulated distance, the normalizing factor, and the optional path, computed between the *Gold Standard* and the test data was employed as an input to the classifier. The data set for the Intel Galileo was arbitrarily divided into a training sample of 1667 points and a test set of 1485 samples, and the data set for the TI MSP-EXP430G2 was arbitrarily divided into a training sample of 5188 points and a test set of 4757 points. The general practice is to split the data sets into a training and test set. Training data is the data on which the machine learning algorithms learn to perform the necessary correlation tasks (e.g., classify, cluster, learn the attributes) thereby determining whether a test PCB is or is not counterfeit. The algorithms are trained with the training set and tested via the test set to ascertain how well it generalizes to data it has never seen before. The algorithms' performance on the test sets provide insight into how well the model is performing. In k-fold cross-validation, the original data set is randomly partitioned into k equal size subsamples. Of the k subsamples, a single subsample is retained as the validation data for testing the model, and the remaining k-1 subsamples are used as training data. The cross-validation process is then repeated k times (the folds), with each of the k subsamples used exactly once as the validation data. A value of k equal to 10 was used for the experiments presented in this paper.

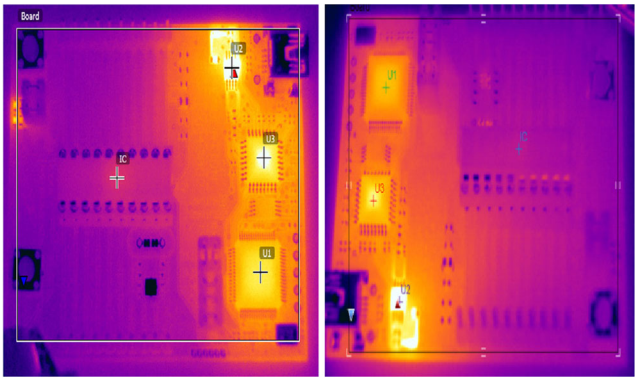

Fig. 5 Thermal screen shot of one of the authentic TI MSP-EXP430G2 experimental PCBs (dubbed the *Gold Standard*) (on the left) and one of a possibly counterfeit TI MSP-EXP430G2 experimental PCBs (on the right)

Piecewise linear-discriminant functions for decomposing the patterns correlating to the three designated categories—authentic, counterfeit, and unknown—were derived utilizing the points in the training set. The ICs designated as "unknown" are due to the fact our process could not clearly distinguish whether that particular board was authentic or counterfeit. Those PCBs classified as "unknown" would require further testing to ensure whether they are counterfeit or not. The contingency tables for organizing the samples in both the Intel and TI test sets for the advertised supervised learning algorithms are shown in Tables 3, 4, and 5 and Tables 6, 7, and 8, respectively.

In the contingency table representing classification performance of the LVQ algorithm against Intel PCBs (Table 3), the authentic boards was accurately classified precisely 89.3% of the time, whereas counterfeit boards were detected 84% of the time. The unknown boards were identified correctly at a rate of 74.2%. For the contingency table depicting classification performance of the naive Bayes algorithm against Intel PCBs (Table 4), the authentic boards was correctly classified approximately 91.4% of the time, whereas counterfeit boards were detected 92% of the time. The unknown boards were designated properly at a rate of 80.3%. For the contingency table portraying the classification performance of the SVM algorithm against Intel PCBs (Table 5), the authentic boards was properly classified exactly 91.1% of the time, whereas counterfeit boards were detected 89.3% of the time. The unknown boards were designated correctly at a rate of 81.8%.

Table 3 Contingency table for the classification of Intel PCBs (LVQ)

		Assigned category			Total
		Authentic	Counterfeit	Unknown	
True category	Authentic	1201	130	13	1344
	Counterfeit	11	63	1	75
	Unknown	9	8	49	66
Total		1221	201	63	1485

Table 5 Contingency table for the classification of Intel PCBs (SVM)

		Assigned category			Total
		Authentic	Counterfeit	Unknown	
True category	Authentic	1224	116	4	1344
	Counterfeit	3	67	5	75
	Unknown	8	4	54	66
Total		1235	187	63	1485

In the contingency table representing classification performance of the LVQ algorithm against TI PCBs (Table 6), the authentic boards was correctly precisely 87.9% of the time, whereas counterfeit boards were detected 89.7% of the time. The unknown boards were identified properly at a rate of 75.5%. For the contingency table portraying the classification performance of the naive Bayes algorithm against TI PCBs (Table 7), the authentic boards was properly classified exactly 89.6% of the time, whereas counterfeit boards were detected 91.9% of the time. The unknown boards were identified correctly at a rate of 71.8%. For the contingency table portraying the classification performance of the SVM algorithm against Intel PCBs (Table 8), the authentic boards was properly classified exactly 91.3% of the time, whereas counterfeit boards were detected 91.3% of the time. The unknown boards were designated properly at a rate of 81.5%.

The overall accuracy of each classification scheme is achieved by taking the summation of the diagonal elements in the contingency table and then dividing the sum by the total number of points in the test set and is showcased in Table 9. For the Intel PCBs, naive Bayes classifier correctly verified the parts precisely 90.91% (slightly better than 90.57% for SVM). Meanwhile, for the TI PCBs, SVM classifier accurately verified the parts approximately 89.62% (marginally better than 89.44% for naive Bayes). The aforementioned two learning algorithms demonstrate significant performance advantages over the LVQ approach in terms of classification accuracy. Yet, there are several factors, which could be considered to improve these classification results. For example, with the SVM-based approach, one can explore the use of various kernel functions or research alternatives for handling a multiclass problem. Similarly, the performance of the LVQ algorithm can be improved through the optimal trade-off of additional training data and processing time. These considerations were beyond the scope of this publication in the authors' opinion, where our goal was to develop a successful non-invasive counterfeit detection capability for ICs, through the original use of thermal imaging. To fully facilitate selection of an algorithm approach, one must not only consider classification accuracy but also performance criterion such as training time, linearity, the number of algorithm parameters, and the number of input features, respectively. The scale-invariant feature transform algorithm was used to detect and generate the local features in infrared images. This approach for image feature generation transforms an image into a large collection of feature vectors, each of which is invariant to image translation, scaling, and rotation, partially invariant to illumination changes and robust to local geometric distortion. For the reasons presented, the authors recommend the SVM approach.

Table 2 furnishes a summary of the key insights generated by the authors' analyses and identifies the performance attributes of each of the aforementioned classifiers. As shown for the classification algorithms, key parameters include the kernel type, which are similarity functions (i.e., functions that the domain expert provides to a machine learning algorithm). In this paper, we used a radial basis function, which is a popular kernel function employed for learning algorithms. For the SVM algorithm listed in the table, the cost parameter controls the impact of misclassification in the training data. The cost controls the influence of each individual support vector and entails a trading error penalty for stability. The parameter listed as gamma is simply a free parameter of the radial basis function and contributes to the shape of the SVM hyerplane. Other parameters of note in Table 2 include the predictor

Table 4 Contingency table for the classification of Intel PCBs (naive Bayes)

		Assigned category			Total
		Authentic	Counterfeit	Unknown	
True category	Authentic	1228	111	5	1344
	Counterfeit	3	69	3	75
	Unknown	8	5	53	66
Total		1239	185	61	1485

Table 6 Contingency table for the classification of TI PCBs (LVQ)

		Assigned category			Total
		Authentic	Counterfeit	Unknown	
True category	Authentic	3605	297	198	4100
	Counterfeit	35	454	17	506
	Unknown	23	14	114	151
Total		3663	765	329	4757

Table 7 Contingency table for the classification of TI PCBs (naive Bayes)

		Assigned category			Total
		Authentic	Counterfeit	Unknown	
True category	Authentic	3672	270	158	4100
	Counterfeit	29	465	12	506
	Unknown	17	16	118	151
Total		3718	751	288	4757

models used for the naive Bayes classifier such as Boolean. There is the learning rate for LVQ, which is a constant used in artificial neural network learning algorithms to affect the speed of learning. The LVQ classifier also utilizes a learning rule for training. LVQ1 is implemented within the competitive layer of the neural network, and LVQ2 is a supplemental learning rule that may be applied only after first applying LVQ1 (LVQ2 can improve the result of the first learning rule). Finally, the first layer hidden neuron parameter refers to a simple model of a biological neuron used in neural networks to perform a small part of the overall computation for the LVQ algorithm. It has inputs from other neurons, each with an associated weight (i.e., a number which indicates the degree of importance which the particular neuron attaches to that input).

Since the SVM technique was recognized as best in show, we conducted a sensitivity analysis to study of how the uncertainty in the output of the system (numerical or otherwise) can be apportioned to different system parameters. For the analysis, we focused on the SVM gamma parameter as well as the radial basis function. The gamma parameter defines how far the influence of a single training example reaches, with low values meaning *far* and high values meaning *close*. The gamma parameters can be seen as the inverse of the radius of influence of samples selected by the model as support vectors. Figure 6 shows the receiver operating characteristic (ROC) curves, which demonstrates the impact to the performance of the machine learning algorithm. The minimum and maximum area under the curve (AUC) is shown for the gamma modifications. In machine learning and statistics, an ROC curve is a graphical plot that illustrates the performance of a classifier system as its discrimination threshold is varied. The curve is created by plotting the true positive rate (TPR), or correct detection rate, against the false positive rate (FPR)—also known as the false alarm rate—at various threshold settings. The TPR is also known as sensitivity or the sensitivity index.

Table 8 Contingency table for the classification of TI PCBs (SVM)

		Assigned category			Total
		Authentic	Counterfeit	Unknown	
True category	Authentic	3678	262	160	4100
	Counterfeit	35	462	9	506
	Unknown	15	13	123	151
Total		3728	737	292	4757

Table 9 Overall accuracy of classification of the test set per classifier

Hardware authenticity verification			
	LVQ	Naive Bayes	SVM
Intel	88.42%	90.91%	90.57%
TI	87.22%	89.44%	89.62%

5 Conclusions

In this paper, a new non-destructive counterfeit detection technique was showcased to examine the authenticity of ICs by utilizing ICA and DTW for enhanced feature extraction and a few prominent supervised learning algorithms for classification. The experimental results and analyses demonstrated the technique's effectiveness in distinguishing between counterfeit and authentic ICs. The primary benefit of our approach is that it provides observability indirectly into system behavior of electronic components in real-time. Temporal insight into how the states of electronic components change over time (ergo not just a static snapshot of the behavior from the individual sensors). This technique is cost effective because the IR image analyses can detect counterfeit electronic components at the board level within a PCB. Inexpensive components (e.g., capacitors, diodes) are often subject to counterfeiting [3]. This new counterfeit detection method would lessen the likelihood of system failure or poor performance of systems incorporating potential counterfeit ICs. Future research will focus on using higher resolution IR imagery to improve authentication accuracy, developing a confidence index within each classification (e.g., "99% authentic"), examining other machine learning approaches, employing a unary

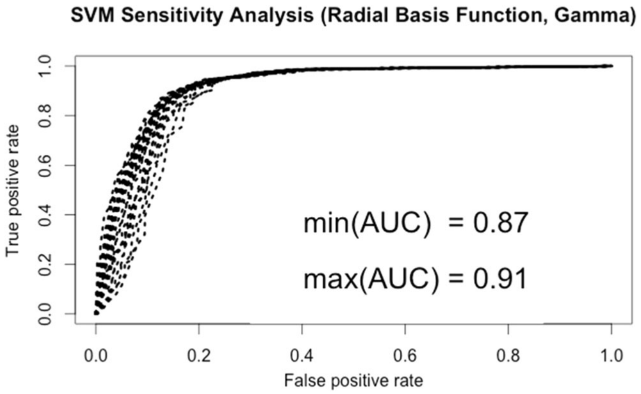

Fig. 6 Sensitivity analysis via ROC curves for a SVM approach

classification, and analyzing ICs from other semiconductor manufacturers.

References

1. U.S. General Accountability Office (2016) Counterfeit parts: U.S. Department of Defense (DoD) needs to improve reporting and oversight to reduce supply chain risk
2. Bumgarner J, Coleman G, Smith A, Willems M, Wren S (2011) U.S. Department of Defense's 2010 Comprehensive Inventory Management Improvement Plan
3. Hughitt B (2008) Counterfeit electronic parts. In: Trilateral Safety and Mission Assurance Conference. National Aeronautics and Space Administration (NASA), European Space Agency (ESA), Japan Aerospace Exploration Agency (JAXA)
4. Birdsong, B, Schipp, F (2012) U.S. Missile Defense Agency (MDA) Counterfeit Awareness Training—avoidance, detection, containment, and reporting briefing
5. McFadden F, Arnold R (2010) Supply chain risk mitigation for IT electronics. In: 2010 IEEE International Conference on Technologies for Homeland Security (HST). IEEE, pp. 49–55
6. Collins, I, Frazier, P, Gilmore, E, Chouikha, M (2014) Industry study of supply chain risk management practices and ways to improve hardware reliability. In: 3rd Annual IEEE International Reliability Innovations Conference. IEEE
7. Intel Corporation (2012) Intel risk assessment 2 summary. https://supplier.intel.com/static/eicc/2012_Final_Intel_RA2_summary.pdf. Accessed: 30 July 2012
8. Texas Instruments (2014) Sustainability: supply chain accountability: transparency. http://www.ti.com/corp/docs/csr/transparency.html. Accessed: 17 July 2014
9. IHS Technology (2012) Top 5 most counterfeited parts represent a $169 billion potential challenge for global semiconductor market. http://www.isuppli.com/Semiconductor-Value-Chain/News/pages/Top-5-Most-Counterfeited-Parts-Represent-a-$169-Billion-Potential-Challenge-for-Global-Semiconductor-Market.aspx. Accessed: 4 November 2014
10. Guin U, Huang K, DiMase D, Carulli J, Tehranipoor M, Makris Y (2014) Counterfeit integrated circuits: a rising threat in the global semiconductor supply chain. Proc IEEE 102(8):1207–1228
11. Tehranipoor M, Guin U, Forte D (2015) Counterfeit integrated circuits: detection and avoidance. Springer, New York
12. Sheppard C, Shotton D (1997) Confocal laser scanning microscopy. Springer, New York
13. Chatterjee K, Das D (2007) Semiconductor manufacturers' efforts to improve trust in the electronic part supply chain. IEEE Trans Compon Packag Technol 30(3):547–549
14. Shrivasta A, Azarian M, Morillo C, Sood B, Pecht M (2014) Detection and reliability risks of counterfeit electrolytic capacitors. IEEE Trans Reliab 63(2):468–479
15. Cushing M, Mortin D, Stadterman T, Malhorta A (1993) Comparison of electronics – reliability assessment approaches. IEEE Trans Reliab 42(4):542–546
16. Zhang X, Tehranipoor M (2014) Design of on-chip lightweight sensors for effective detection of recycled ICs. IEEE Trans VLSI Syst 22(5):1016–1029
17. Dogan H, Forte D, Tehranipoo*r* M (2014) Aging analysis for recycled FPGA detection. In: 2014 International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT). IEEE, pp. 171–176
18. Alam M, Tehranipoor M, Forte D (2016) Recycled FPGA detection using exhaustive LUT path delay characterization. In: 2016 IEEE international test conference (ITC). IEEE, pp. 1–10
19. Shakya B, Guin U, Tehranipoor M, Forte D (2015) Performance optimization for on-chip sensors to detect recycled ICs. In: 33rd IEEE International Conference on Computer Design (ICCD) IEEE, pp. 289–295
20. Guin U, Zhang X, Forte D, Tehranipoor M (2016) Design of accurate low-cost on-chip structures for protecting integrated circuits against recycling. IEEE Trans VLSI Syst 24(4):1233–1246
21. Guin U, Zhang X, Forte D, Tehranipoor M (2014) Low-cost on-chip structures for combating die and IC recycling. In: 2014 51st ACM/EDAC/IEEE Design Automation Conference (DAC). IEEE, pp. 1–6
22. Huang K, Liu Y, Korolija N, Carulli J, Makris Y (2015) Recycled IC detection based on statistical methods. IEEE Trans Comput-Aided Design Integr Circuits Syst 34(6):947–960
23. Alam, M, Chowdhury, S, Tehranipoor, M, Guin, U (2018) Robust, low-cost, and accurate detection of recycled ICs using digital signatures. In: IEEE International Symposium on Hardware Oriented Security and Trust (HOST). IEEE, pp. 1–6
24. Mahmood K, Latorre-Carmona P, Shahbazmohamadi S, Pla F, Javidi B (2015) Real-time automated counterfeit integrated circuit detection using X-ray microscopy. Appl Opt 54(13): 25–32
25. Ahi, K, Asadizanjani, N, Shahbazmohamadi, S, Tehranipoor, M, Anwar, M (2015) Terahertz characterization of electronic components and comparison of terahertz imaging with X-ray imaging techniques. In: Terahertz physics, devices, and systems IX: advanced applications in industry and defense. SPIE
26. Ahi, K, Anwar, M (2016) Advanced terahertz techniques for quality control and counterfeit detection. In: terahertz physics, devices, and systems X: advanced applications in industry and defense. SPIE
27. Ahi K, Shahbazmohamadi S, Asadizanjani N (2018) Quality control and authentication of packaged integrated circuits using enhanced-spatial-resolution terahertz time-domain spectroscopy and imaging. Opt Lasers Eng 104:274–284
28. Huang K, Carulli J, Makris Y (2013) Counterfeit electronics: a rising threat in the semiconductor manufacturing industry. In: 2013 IEEE International Test Conference (ITC). IEEE, pp. 1–4
29. Huang K, Carulli J, Makris Y (2012) Parametric counterfeit IC detection via support vector machines. In: 2012 IEEE International Symposium on Defect and Fault Tolerance in Very-large-scale integration and Nanotechnology Systems (DFT). IEEE, pp. 7–12
30. Zheng Y, Wang X, Bhunia S (2015) SACCI: scan-based characterization through clock phase sweep for counterfeit chip detection. IEEE Trans VLSI Syst 23(5):831–841
31. Pecht M (2013) Bogus: electronic manufacturing and consumers confront a rising tide of counterfeit electronics. IEEE Spectr 43(37): 37–46
32. Huang H, Boyer A, Dhia S (2014) The detection of counterfeit integrated circuit by the use of electromagnetic fingerprint. In: 2014 International Symposium on Electromagnetic Compatibility (EMC Europe 2014). IEEE, pp. 1118–1122
33. Li J, Wang J, Li Z, Li B (2013) A novel algorithm of IC defect images enhancement based on histogram equalization and IHS transform. In: 2013 IEEE International Conference on Anti-Counterfeiting, Security and Identification (ASID). IEEE, pp. 1–5
34. Welke S, Johnson B, Aylor J (1995) Reliability modeling of hardware/software systems. IEEE Trans Reliab 44(3):468–479
35. Blais R (1969) True reliability versus inspection efficiency. IEEE Trans Reliab 18(4):201–203

36. Ahi K, Rivera A, Mazadi A, Anwar M (2017) Fabrication of robust nano-signatures for identification of authentic electronic components and counterfeit avoidance. Int J High Speed Electron Sys 26(3):3–11
37. Ahi K, Rivera A, Mazadi A, Anwar M (2017) Encrypted electron beam lithography nano-signatures for authentication, microelectronics and optoelectronics. Int J High Speed Electron Sys 26(3): 134–146
38. Song P, Stellari F, Pfeiffer D, Culp J, Weger A, Bonnoit A, Wisnieff B, Taubenblatt M (2011) MARVEL—malicious alteration recognition and verification by emission of light. In: 2011 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST). IEEE, pp. 117–121
39. Chen A, Hu X, Jin Y, Niemier M, Yin X (2016) Using emerging technologies for hardware security beyond PUFs. In: 2016 IEEE Design, Automation & Test in Europe Conference & Exhibition (DATE) IEEE, pp. 1544–1549
40. Zheng, Y, Basak, A, Bhunia, S (2014) CACI: dynamic current analysis towards robust recycled chip identification. In: 51st annual ACM/EDAC/IEEE design automation conference (DAC)
41. Zheng F, Hennessy A, Bhunia S (2015) Robust counterfeit PCB detection exploiting intrinsic trace impedance variations. In: 2015 IEEE 33rd Very Large Scale Integration (VLSI) Test Symposium (VTS). IEEE, pp. 1–6
42. Guo, Z, Xu, X, Tehranipoor, M, Forte, D (2017) FFD: a framework for fake flash detection. In: 51st Annual ACM/EDAC/IEEE Design Automation Conference (DAC). IEEE
43. Zhang H, Sfarra S, Sarasini F, Ibarra-Castanedo C, Perilli S, Fernandes H, Duan Y, Peeters J, Maldague X (2018) Optical and mechanical excitation thermography for impact response in basalt-carbon hybrid fiber-reinforced composite laminates. IEEE Trans Ind Informat 14(2):831–841
44. Zhang H, Robitalle F, Grosse C, Ibarra-Castanedo C, Ocana-Martins J, Sfarra S, Maldague X (2018) Optical excitation thermography for Twill/Plain weaves and stitched fabric dry carbon fibre preform inspection. Compos A: Appl Sci Manuf 107(4):282–293
45. Zhang H, Yu L, Hasler U, Fernandes H, Genest M, Robitaille F, Joncas S, Holub W, Sheng Y, Maldague X (2016) An experimental and analytical study of micro-laser line thermography on micro-sized flaws in stitched carbon fiber reinforced polymer composites. Compos Sci Technol 126(4):17–26
46. Fernandes H, Zhang H, Figueiredo A, Malheiros F, Ignacio L, Sfarra S, Ibarra-Castanedo C, Guimaraes G, Maldague X (2018) Machine learning and infrared thermography for fiber orientation assessment on randomly-oriented strands parts. Sensors 18(1):1–16
47. Parra L (2002) Tutorial on blind source separation and independent component analysis. Adaptive Image & Signal Processing Group, Sarnoff Corporation, Princeton
48. Gilmore E, Frazier P, Collins I, Reid W, Chouikha M (2013) Infrared analysis for counterfeit electronic parts detection and supply chain validation. J Environ Sys Dec 33(4):477–485
49. Cortes C, Vapnik A (1995) Support vector networks. Mach Learn 20(3):273–297
50. Friedman N, Geiger G, Goldszmidt M (1997) Bayesian network classifiers. Mach Learn 29:131–161
51. Lewis D (1988) Naïve (Bayes) at forty: the independence assumption in information retrieval. In: 10th European Conference on Machine Learning. IEEE, pp. 4–15
52. Kohonen T (1988) An introduction to neural computing. Neural Netw 1:3–16
53. Rabiner L, Rosenberg A, Levinson S (1978) Considerations in dynamic time warping algorithms for discrete word recognition. IEEE Trans Acoust Speech Signal Process 26(6):575–582
54. Myers C, Rabiner L (1981) A comparative study of several dynamic time-warping algorithms for connected word recognition. Bell Syst Tech J 60(7):1389–1409
55. Weng Y, Zhu Z (2003) Time series clustering based on shape dynamic time warping using cloud models. In: 2003 International Conference on Machine Learning. IEEE, pp 236–241