Environ Syst Decis (2013) 33:477–485
DOI 10.1007/s10669-013-9482-1

Infrared analysis for counterfeit electronic parts detection and supply chain validation

E. Thomas Gilmore · Preston D. Frazier ·
Isaac J. Collins II · William Reid · M. F. Chouikha

Published online: 23 November 2013

Abstract Within the electronics industry, counterfeit electronic components entering the supply chain have steadily become an increasing threat accounting for more than 8 % of global merchandise trade and an annual $600 billion enterprise. Currently, there are not many cost-effective and nonintrusive solutions for counterfeit detection of electronic parts. In this paper, the authors present a statistical approach for detecting counterfeit components based on infrared (IR) analysis by the use of independent component analysis (ICA). As a prominent higher-order statistical analysis technique, ICA is capable of extracting relevant features from IR data. The latest applications and the extended algorithms of ICA have been elucidated for the purposes of classification and identification of counterfeit electronic parts. The theoretical framework of ICA is presented along with extensive experimental results to illustrate its feature extraction function in counterfeit electronic parts detection.

Keywords Infrared analysis · Counterfeit detection · Supply chain validation · Independent component analysis

Opinions, interpretations, conclusions, and recommendations are those of the authors and not necessarily endorsed by the U.S. Government.

E. T. Gilmore (✉) · P. D. Frazier · I. J. Collins II · W. Reid · M. F. Chouikha
Communications and Signal Processing Laboratory, Howard University, Washington, DC 20059, USA
e-mail: ethomasg@gmail.com

1 Introduction

Supply chain risk management (SCRM) is an increasingly important aspect of business today. In 2009, President Obama accepted the recommendations of the Cyberspace Policy Review which built upon the Comprehensive National Cybersecurity Initiative National Security Council (National Security Council 2009). There are twelve initiatives, which are designed to strengthen the United States' security in cyberspace. The eleventh initiative is to develop a multipronged approach for global SCRM (National Security Council 2009). Globalization has allowed companies the opportunity to expand their enterprises outside of the United States, yet this has escalated risks due to their complex supply chain. The range of negative exposure of a company's supply chain goes from the increased unreliability of counterfeit electronics parts, to the susceptibility of fraudulent parts, to data exfiltration and adversary-controlled Trojan horses embedded in electronic chips and parts (McFadden and Arnold 2010).

There are many ways to describe a counterfeit part. In the electronics manufacturing industry, a counterfeit is a substitute or unauthorized copy, a part in which the materials used or its performance has been changed without notice, or a substandard component misrepresented by the supplier. In the electronics distributor industry, counterfeits are items that are produced or distributed in violation of intellectual property rights, copyrights, or trademark laws. There are also fraudulent parts, which, according to the SAE International Aerospace Standard (AS) 5553, are items that are deliberately altered in such a way as to misrepresent the actual quality of the item with intent to defraud or deceive the purchaser. The U.S. Department of Energy defines a counterfeit as a substitute without legal right or authority to do so, or one whose material, performance, or characteristics are knowingly misrepresented (Hughitt 2008). The many definitions of a bogus part show how enormous the problem is becoming in the electronics industry. High-tech products, such as batteries, computer hardware (H/W), and electronic games, accounted for three of the top ten products seized by the U.S. Customs and Border Protection in 2004 (Pecht and Tiku 2006). In 2011, consumer electronics made up the bulk of counterfeit goods imported into the United States accounting for 22 % of total seizures and an estimated retail value of $101.2 million (Dickler 2012). The value of counterfeit parts entering into the United States is in the hundreds of millions, and recent data show that the number will continue to grow. To combat this issue, there are many organizations in the government as well as private industry currently developing methods to identify and eliminate counterfeit parts from entering their supply chains.

The U.S. Missile Defense Agency (MDA) has taken measures to mitigate the amount of counterfeit parts entering their supply chain. The MDA's number one rule on counterfeit parts avoidance is to always buy a product from authorized or trusted sources whenever possible (Johnson 2012). The methods proposed to ensure compliance to rule number one are to manage obsolescence, use an independent distributor (ID) only as a last resort, knowing how to find an authorized source, and requiring management approval for purchases from unauthorized sources. Rule number two of counterfeit parts avoidance is to assess unauthorized sources on-site (Johnson 2012). This is done by creating a decision matrix and then assigning a rank to the attributes that are most important to the company. Rules number one and two go hand in hand. Properly vetting a distributor can save both time and money. The U.S. MDA uses thorough checks into a company's past history to ensure that the parts they are selling are guaranteed quality. A third rule in counterfeit parts avoidance is to require minimum inspection and test for all open market purchases (Johnson 2012). This involves a series of visual inspections, X-ray fluorescence, X-ray analysis, die verification, scanning acoustic microscopy, and various other tests to ensure counterfeits are detected. Though testing is an important part in keeping counterfeit parts out of the supply chain, these tests are costly, inconvenient, and sometimes destructive. The U.S. MDA's last stated rule of counterfeit parts avoidance is flow down bogus parts requirements to their suppliers (Johnson 2012). This means that all contractors and subcontractors shall have procedures in place to meet the agency's minimum standards. This is very similar to the National Aeronautics and Space Administration's (NASA's) contractor and subcontractor supply chain requirements. The goal is to only work with reputable companies with strict guidelines with regard to what flows through the supply chain.

Production of integrated circuits (ICs) in the United States has decreased at least 11 %, whereas in Asian countries, it has increased almost 20 % (Birdsong 2012). This is in part due to small businesses in the United States locating thousands of parts numbers from brokers' lists assumed to be legitimate, and purchasing unknowingly counterfeit items which then enter the supply chain through the distribution phase. Other contributing factors to the lowered production of ICs in the United States are uncertainties of the definition of "counterfeit," where these erroneous electrical components are obtained, electronic waste (eWaste), and the current means of preventing entrance of the ICs into the supply chain.

Even with preventive measures in place, counterfeits are still making their way into the supply chain. Our SCRM approach to this problem is to employ imaging as a nondestructive and noninvasive means of detecting counterfeit electronic components. Our solution uses infrared (IR) cameras in a fixed position to capture overhead perspective of a printed circuit board (PCB) which is mounted on a movable platform. The camera captures full 360° video footage of the PCB and records the IR signatures of each component on the board. By using a source separation method, specifically independent component analysis (ICA), the authors are able to differentiate between the IR signatures and performance characteristics of each component on the board. These signatures are then compared to the signatures of legitimate components to determine authenticity. This research would be effective in assisting customers in their SCRM.

The supply chain consists of six (6) major phases, which include design, fabrication, assembly, distribution, maintenance, and disposal (McFadden and Arnold 2010), where design, fabrication, and assembly are generally referred to as the production phases. As stated in Bumgarner et al. (2010), ineffective and inefficient inventory management practices and procedures have put the Department of Defense's (DoD's) supply chain at risk.

The SAE International Standard for counterfeit parts (AS5553) offers multiple examples of what is considered a counterfeit part including parts that do not contain the proper internal construction, have been used, refurbished or reclaimed but represented as new, or sold with modified labeling or markings intended to misrepresent. As previously stated, there is a difference between fraudulent and counterfeit. Yet, the U.S. MDA considers the term "counterfeit parts" to include both fraudulent and counterfeit products as to ensure the inclusion of all illegal practices. With this definition in mind, there are brokers who either knowingly or unintentionally obtain counterfeit parts from illegitimate sources. To counterbalance this, one must verify that parts are obtained from credible sources through verification with the original component manufacturer (OCM), an aftermarket manufacturer (AM), authorized “Franchised” distributors (AD), or an ID. An OCM is an organization that “designs and/or engineers a part and is pursuing the intellectual property rights to that part (Birdsong and Schipp 2012).” The AM is a manufacturer who is authorized by the OCM to produce and sell replacement parts, produces parts using dies or wafers manufactured by and traceable to an OCM, or reverse-engineers obsolete parts without violation of intellectual property rights (Birdsong and Schipp 2012). An AD is a distributor with which the OCM “has a contractual agreement to distribute its product,” and an ID purchases parts with “the intention to sell and redistribute them back into the market (Birdsong and Schipp 2012)” without having contractual agreements or obligations with OCMs. Although these organizations tend to employ traceability with their products, the possibility that they sell a product which they purchased from an unauthorized source still exists. In this case, the organization is treated with caution as an ID or broker distributor.

2 Current approaches to counterfeit parts detection

China receives 90 % of the Asian recycling market (Birdsong and Schipp 2012); eWaste must be tested for “high-risk” counterfeit ICs (processors/controllers, memory, operational amplifiers, switches, and field programmable gate arrays). eWaste is largely comprised of unwanted parts that were mishandled, sanded, or uncontrollably heated during part removal. Due to these ineffective handling, the die cracks or becomes delaminated and these mistreated parts tend to have immediate or latent electronic discharge (ESD) failures. Higher or lower temperature tests, tighter production parameters and performance specifications, vibration or shock resistance, and radiation hardening are all tests used to detect any likely failures, but also dramatically impact part price (Birdsong and Schipp 2012). The current methods in place to prevent counterfeits entering the supply chain vary based on company standards and practices. One may consult the Electronic Resellers Association International (ERAI), which is a privately held global trade association that monitors/mediates issues affecting the global supply chain of electronics including the supply of counterfeit and substandard parts (Birdsong and Schipp 2012). The challenge with this method is that not all companies confer with the ERAI when counterfeits are found in their supply chain, thus leading to an incomplete knowledge base of the most accurate and recent counterfeit statistics. Another resource available is the DoD’s Government-Industry Data Exchange Program (GIDEP). This useful program seeks to reduce expenditures of resources by sharing essential information during all supply chain phases of systems and equipment. Participating members are allowed access to information on failure experience, suspect counterfeits, diminishing manufacturing sources, and material shortages, reliability, and maintainability as long as they also provide technical information to add to the database for other members (Birdsong and Schipp 2012). A more manageable method is for a company to regulate “obsolescence” by increasing design awareness through using components with multiple OCMs or choosing multisourced parts whenever possible. Confirming which distributors are authorized through the OCM’s Web site, checking for ERAI and qualified suppliers list-distributors memberships, AS certifications, a lack of ERAI reports or complaints, and site testing are other proven methods to prevent counterfeit supply chain entrance (Stein 2012).

Currently, there are not many cost-effective solutions for counterfeit detection at the PCB level using IR analysis. However, there are techniques in which individual ICs are analyzed, eventually resulting in the examination of an entire PCB. Present-day counterfeit detection techniques include general optical scans (any of the various ways to visually detect counterfeit markings), confocal scanning acoustic microscopy, surface profilometry, Raman spectroscopy, X-ray photoelectron spectroscopy, and a number of other techniques. Along with the aforementioned technologies, procedures are needed in order to prevent counterfeits from initially entering the supply chain including quality system audits and procurement requirements. Procedural examples are requesting valid manufacturer certifications and ensuring supply chain traceability which assures the tracking of the supply chain back to the manufacturer of all electrical, electronic, and electromechanical components and devices (Hughitt 2008). Although these counterfeit detection techniques and parts authentication tools are available for both commercial and government use, they are not viable due to their cost per use and manufacturing and maintenance costs as well as the fact they destructive in nature to the devices being tested and do not test for a broad range of counterfeit triggers.

Since the supply chain is susceptible to counterfeit intrusion, it is beneficial to know how to identify a potential threat by understanding the AS characterization of both fraudulence and counterfeit and how to prevent them from entering the supply chain all together. With this background knowledge of how supply chains operate when dealing with counterfeit devices, the remainder of the paper will focus on the development of a novel analysis for counterfeit PCB detection employing IR.

The utilization of blind source separation (BSS) method along with the “Golden Standard” approach is one approach which has yet to be utilized for the purpose of detecting fraudulent ICs. This technique will allow for counterfeit detection at the board level nondestructively. The authors show it is possible to test multiple ICs at the board level from various angles, compare the various signatures (through the use of spatiotemporal analysis) of the individual ICs, and determine the likelihood that counterfeits were used while factoring testing apparatus manufacturing/procurement costs, ease of use, and maintenance costs. Specifically, we initially demonstrate that individual ICs produce unique thermal signatures that can be ascertained and analyzed at the board level through the BSS method and then be compared to a benchmark (i.e., *Golden Standard*) device to test for counterfeit, while maintaining cost efficiency.

Due to the increasing threat of counterfeit merchandise trade and industry, the authors' proposed research focus of using BSS along with the *Golden Standard* approach is one that can assist in the prevention of counterfeits from entering the supply chain. This prevention will save industries, such as DoD, estimated billions of dollars lost annually due to the current infiltration of bogus parts into the supply chain.

3 Blind source separation counterfeit parts detection approach

The research focus is to view thermal or IR signals emitted from both the previously discussed "Golden Standard" and confirmed counterfeit PCBs for comparative evaluation. To reiterate, a "Golden Standard" or benchmark device is one that is proven to be legitimate either via product verification through the manufacturer or certified brokers, or by way of passing previously run counterfeit detection tests that are to be used in conjunction with our approach during the supply chain's assembly, distribution, or maintenance stages. When examining the signals, it is important to know how to elucidate specific patterns. Our novel approach that incorporates BSS, more specifically ICA, is used to analyze specific signal compositions within a general mixed signal.

BSS is a statistical approach to separate and analyze individual signals from an observed mixture of a group of signals (Jadhav and Bhalchandra 2008), often while multiple interfering components and additional noise are present. This technique was first introduced in 1986 by Herault and Jutten (1987) and was expanded upon eight (8) years later by Comon (1994). In Comon (1994) is when it was originally referred to as ICA, an extension of principal component analysis (PCA). Comon designed a practical optimization criterion to search a linear transformation that minimizes statistical dependence between components. This new application could include blind identification and deconvolution (Herault and Jutten 1987). This broader range of the application is one of the many benefits of BSS over other common image-processing techniques such as PCA.

Another application of BSS that would otherwise be off limits to PCA is the detection and localization of sources, not limited to signals or images. In statistics, it is recognized that for non-Gaussian signals, uncorrelated signals are not necessarily independent. To disassociate these types of signals, one only needs to consider the second-order statistics. Yet, higher-order statistics (HOS) are needed (Jadhav and Bhalchandra 2008) to decompose a signal as independent. This fact points to the relationship between PCA and ICA. PCA is able to extract features from a signal; ICA is capable of initiating complete independence of previously mixed signals.

With the proposed problem of detecting counterfeit electronic devices at the board level, the authors realize the extension of PCA not only saves time and costs when needing to separate mixed thermal signals from an entire PCB, but ultimately will allow for increased effectiveness in analyzing results. Additionally, BSS is capable of taking into account various assumptions, such as all signals are independent of each other. Therefore, the source signals are treated equally before the algorithm is run (or is considered "centered"), white sources and white mixed signals are considered to be noise, and the information is orthogonal (the transpose of the matrix is equal to its inverse) as well as any unknowns, which are prevalent when analyzing a PCB at the board level. Our process allows us to accurately extract individual signals and evaluate and compare them independently. This novel approach is more efficient and beneficial than other techniques.

BSS is a method for analyzing individual components while multiple interfering components and additional noise are present. This method is represented using the equation:

$$X = AS + N \tag{1}$$

where X represents an observed m-dimensional random vector, A represents an unknown full-rank real matrix, S represents unknown n-dimensional source signals, and N represents an initially unknown noise factor (often assumed to be white Gaussian). The overall goal of this general-case (BSS) equation is to recover unknown A and S given only X. In the case of analyzing multiple thermal signatures given off by multiple ICs on a single board, S represents the individual signals from ICs on the board being evaluated, A represents abundance of information per pixel, and X represents signature of the board as a whole (Parra 2002). Thus, Eq. (1) using ICA assumptions can be used for any specified number of ICs and can be rewritten as:

$$X = \sum\nolimits_{i=1}^{n} a_i S_i \tag{2}$$

BSS is typically based on the assumption that the observed signals are linear superpositions of underlying hidden source signals. Let us denote the n source signals by

$s_1(t)\ldots, s_n(t)$, and the observed signals by $x_1(t)\ldots, x_m(t)$. Let a_{ij} denote the coefficients in the linear mixing between the sources $s_j(t)$ and the observed signal, $x_i(t)$. The source signals can be collected in a vector as shown in Eq. (3)

$$s(t) = (s_1(t)\ldots, s_n(t))^T \tag{3}$$

and similarly for the observed signal vector illustrated in Eq. (4):

$$x(t) = (x_1(t)\ldots, x_n(t))^T \tag{4}$$

Now, the mixing matrix can be written as

$$x(t) = As(t),$$

where the matrix

$$A = |a_{ij}| \tag{5}$$

collects the mixing coefficients. No particular assumptions on the mixing coefficients are made. Some weak structural assumptions are often made; for example, it is typically assumed that the mixing matrix is square (ergo the number of source signals equals the number of observed signals, $n = m$). The challenge of BSS is how to estimate both the source signals $s_i(t)$ and the mixing matrix $\boldsymbol{A}$, based on observations of the $x_i(t)$ alone (Jutten and Herault 1991). The word “blind” refers primarily to the impossibility of directly observing the source signals. If the source signals could be partly observed, the problem could be solved by basic linear regression techniques. However, more sophisticated methods are required, which are based on the statistical properties of the source signals.

In most methods, the source signals are assumed statistically independent. Then, the model can be estimated if the source signals fulfill some additional assumptions. We list two of the most commonly used ones for our implementation of the technique. First, if all the components, except perhaps one, have non-Gaussian distributions, then the ensuing model is called ICA, and many techniques are available for estimation of the model. Second, if the components have nonstationary, smoothly changing variances, then the model can be estimated as well. Based on the distribution of IR radiation spectrum, an IR sensor can be classified as one of the following categories according to its wavelength (Holliday and Kay 2005):

- Short-wave IR (SWIR): 0.7–3 µm
- Midwave IR (MWIR): >3–6 µm
- Long-wave IR (LWIR): >6–15 µm
- Far IR (FIR): >15–1,000 µm

IR energy is emitted by all materials above 0° K as thermal radiations. The upper limit of FIR occurs in a region where it is difficult to envision the output from a source as heat (peak radiation occurs at 3° K). At normal temperature, an electronic component radiates most strongly in the IR range at about ten (10) µm, which apparently corresponds to the LWIR. As a result, LWIR sensors were used for this research. In the next section, we demonstrate our novel approach.

4 Independent component analysis algorithm

First, we will present the preprocessing performed by the ICA algorithm before actually applying ICA.

4.1 Whitening the data

The initial step in the ICA algorithm is to whiten the data, i.e., the removal of any correlations in the data. The geometrical interpretation is that it restores the initial “shape” of the data and that the ICA algorithm must only rotate the resulting matrix (Gilmore 2011).

4.2 The ICA algorithm

Intuitively, you can imagine that ICA rotates the whitened matrix back to the original signal space. It performs the rotation by minimizing the Gaussianity of the data projected on both axes (ergo fixed point ICA). By rotating the axis and minimizing Gaussianity of the projection, the ICA is able to recover the original sources that are statistically independent (Note: this property comes from the central limit theorem which states that any linear mixture of two (2) independent random variables is more Gaussian than the original variables) (Gilmore 2011).

To illustrate the ICA algorithm, we provide a simple example here to convey the concept. As previously mentioned, ICA is a technique to separate linearly mixed sources. For instance, we try to mix and then separate two sources. Figure 1 depicts the time courses of two (2) independent sources.

Then, we linearly mix these two original sources from Fig. 1 as shown in Fig. 2. In Fig. 2, we can arbitrarily define the top mixed signal,

$$ms_1(t) = s_1(t) - 2s_2(t) \tag{6a}$$

and the second mixed signal

$$ms_2(t) = 1.5s_1(t) + 3.5s_2(t). \tag{6b}$$

In our approach, this represents IR signals obtained from the PCB board.

Inputting arbitrary Eq. (6a) and (6b) into the ICA algorithm allows for the recovery of the original signals as shown in Fig. 3. More specifically, using the procedure outlined previously, we can estimate the weights a_{ij}, i.e., the individual source signal contributions, based on the

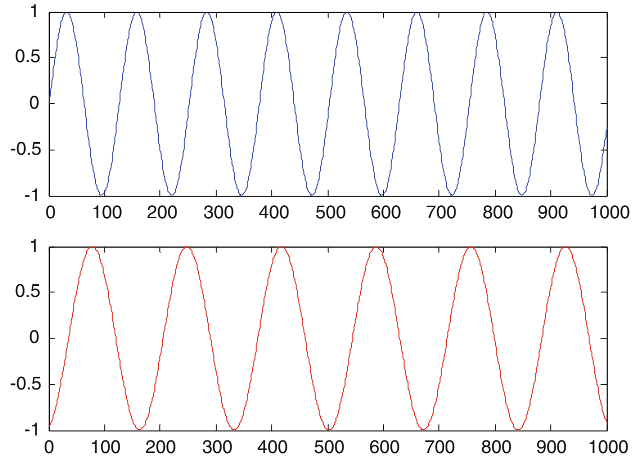

Fig. 1 A pair of independent source signals

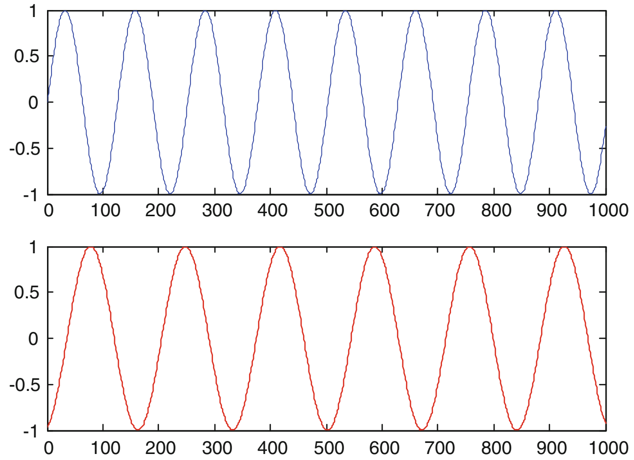

Fig. 3 Recovery of original source signals via ICA

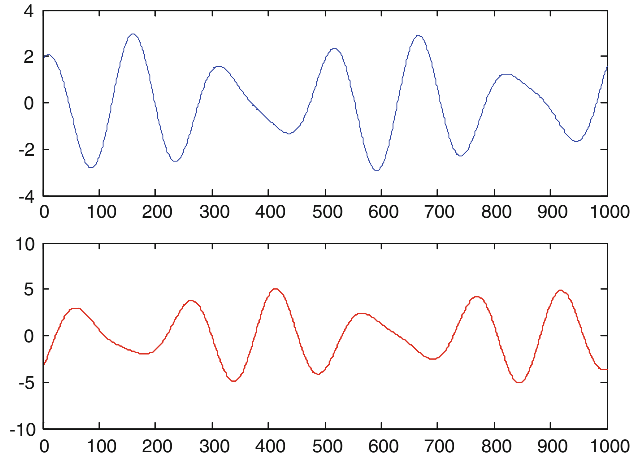

Fig. 2 Mixed signal representations from independent source signals

information of their independence. This technique allows us to separate the two (2) original source signals, $s_1(t)$ and $s_2(t)$, from their mixtures, $x_1(t)$ and $x_2(t)$. For the authors' approach, which will be demonstrated in the simulations, we seek to recover the individual, unique thermal signatures for the components on a PCB for comparison with a benchmark based on known authentic electronic parts.

5 Experimentation setup

We conducted a series of simulations in an attempt to validate the theoretical methodology and technical approach described above. Two PCBs were used for experimental evaluation, one authentic PCB and one counterfeit PCB. It should be noted that the PCBs were visually similar and consisted of similar design, i.e., component types, layouts, etc. In essence, each test board was indistinguishable both visually and its physical characteristics. The PCBs consisted of a circuit with a Hummingbird field programmable gate array (FPGA). The test boards supplied for the purposes of our evaluation and findings were provided courtesy of the U.S. Naval Surface Warfare Center Crane Division.

The simulations consisted of multiple LWIR video test data with an application of the FastICA algorithm using kurtosis. FastICA is closest to the double-blind method of the BSS based on independence and described above. In each simulation, several LWIR videos were acquired each consisting of approximately 5 min in length. Additionally, these test videos were recorded precisely 10 min after initial powering of the boards to prevent any transients from being captured in the data set. Furthermore, it should be noted that all experimental analyses were conducted in an off-line manner.

Twenty-four-bit Red–Green–Blue (RGB) images were acquired using a FLIR Systems ThermoVision A320® IR camera at a rate of 30 frames per second (fps) and a resolution of 160 × 128 pixels. For the purpose of our experiment, the camera lenses were placed approximately 7 inches vertically above the PCB-mounted breadboard with the focus placed mainly on the boards' processor. Figure 4 showcases a sample RGB and grayscale image. LWIR was used which covers the most common thermal range of 7 or 8 microns to 14 microns. 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. This research employed the MATLAB 2011b software (S/W) for signal analysis, Visual C++ (2010) with Open Source Computer Vision (OpenCV) specifically for further real-time signal analysis running within a Windows Operating System (O/S) environment. The program execution time was approximately 3 s for each experimental run.

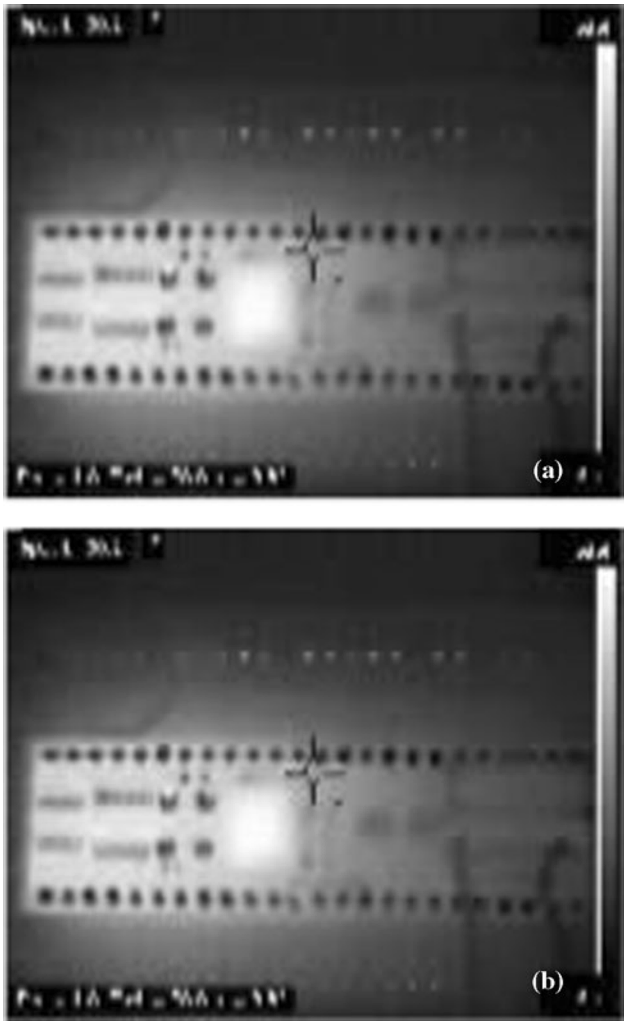

Fig. 4 **a** Twenty-four-bit RGB IR image of test evaluation board, **b** 8-bit grayscale IR image of the test evaluation board. Images acquired using FLIR A320 camera at a 30 frames per second (fps) sample rate, and a resolution of 160 × 128 pixels

6 Simulation results

Based on Eq. (3), each of the recorded signals is a weighted sum of the video signals emitted by the chip components on the PCB, which we denote by $s_1(t)$ and $s_2(t)$. Therefore, incorporating Eq. (4) provides the following linear equations:

$$x_1(t) = a_{11}s_1 + a_{12}s_2 \tag{7a}$$

$$x_2(t) = a_{21}s_1 + a_{22}s_2 \tag{7b}$$

where a_{11}, a_{12}, a_{21}, and a_{22} are parameters that are dependent upon the distance of the cameras from the board components. From this model, we estimate the unique thermal contributions from the electrical components $s_1(t)$ and $s_2(t)$, using only the recorded signals $x_1(t)$ and $x_2(t)$. Obviously since the parameters a_{ij} are unknown, this problem is considerably difficult. For simplicity, we omitted any time delays or other extraneous factors from our simplified mixing model and assume that signals $s_1(t)$ and $s_2(t)$ are statistically independent. As an illustration, Fig. 5 depicts a signal of the total thermal emissions from one of our PCBs, i.e., the aforementioned mixed signal. Using mixed signals representative of those depicted in Fig. 5, ICA was used to estimate the a_{ij} based on the information of their independence, which allows us to separate the two original source signals $s_1(t)$ and $s_2(t)$, i.e., the unique thermal signatures for the PCB components, from the mixtures $x_1(t)$ and $x_2(t)$, i.e., the overall thermal emission signals.

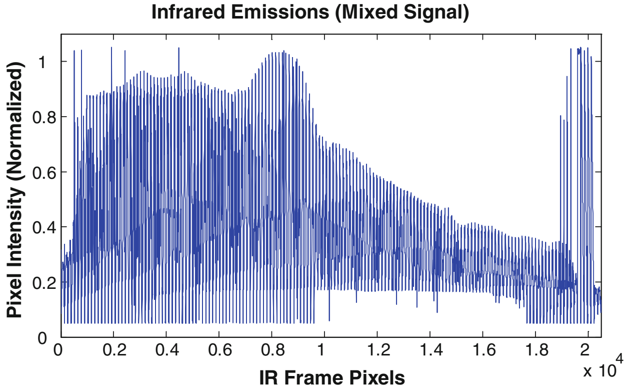

Fig. 5 Thermal emission image in lexicographical order, which represents the mixed observation and input to the developed ICA algorithm

Finally, we investigate the performance of the ICA as a means of not only separating the unique thermal contributions of each PCB component. We first generate a "Gold Standard" via ICA using our authentic test board. Figure 6 depicts the primary independent component for the FPGA on our authentic evaluation board compared to another independent component obtained from test data. As shown, the signature obtained from the test board matches the benchmark component. Thereby, our technique verifies the test board is authentic, at least from the perspective of its thermal signature.

Finally, we tested our approach against IR video acquired from additional test data of suspected counterfeit or altered PCB components. Figure 7 shows a comparison between the independent components generated from the suspected counterfeit PCB and our "Gold Standard" generated from a known authentic PCB. The illustrations demonstrate that the FPGA from the suspected counterfeit or altered board exhibits a different independent component and does not match that of our gold standard.

This experiment was conducted with approximately two dozen data sets with the same data characterization described above. Figure 8 graphically depicts our findings

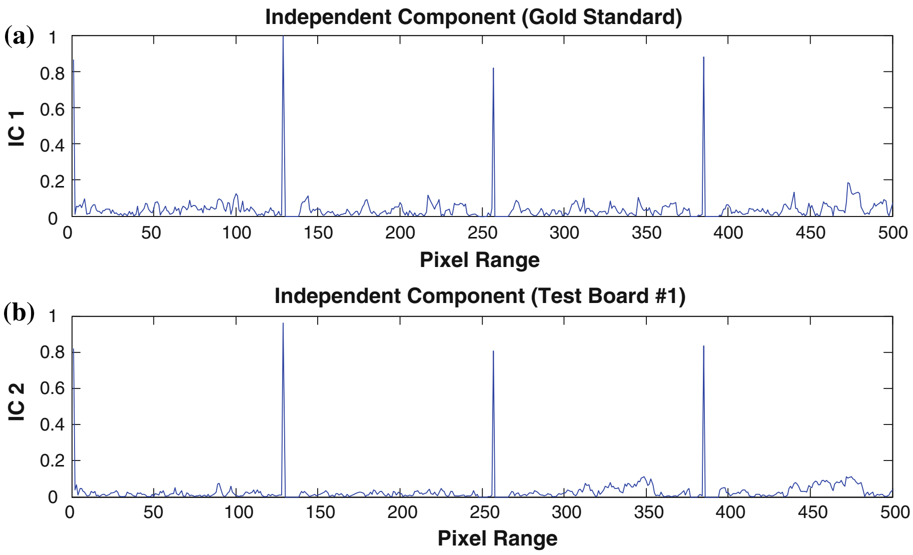

Fig. 6 Illustration of source separation via ICA, and demonstration of board authentication (from a thermal emissions perspective only). **a** Primary independent component that represents a "Gold Standard," **b** primary independent component from a different source

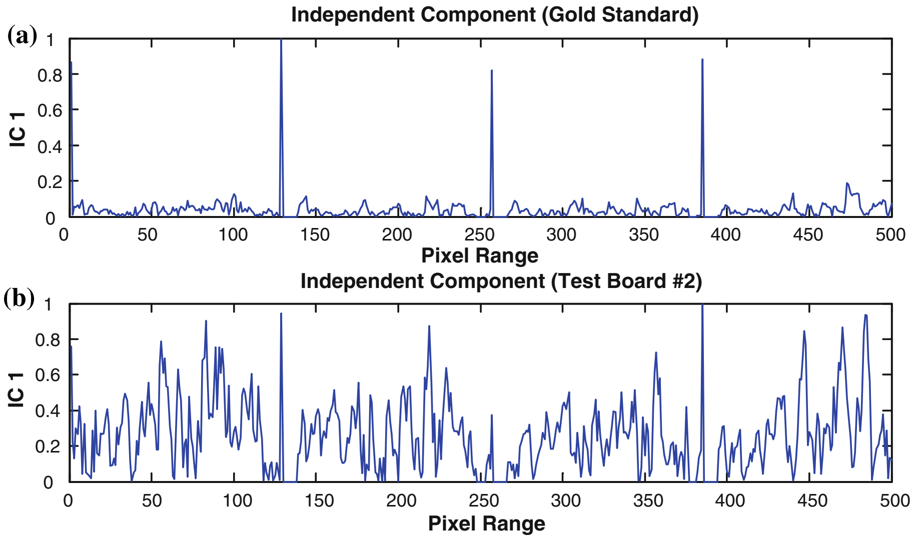

Fig. 7 Illustration of source separation via ICA, and demonstration of counterfeit detection (from a thermal emissions perspective only). **a** Primary independent component that represents a "Gold Standard," **b** primary independent component from a different source

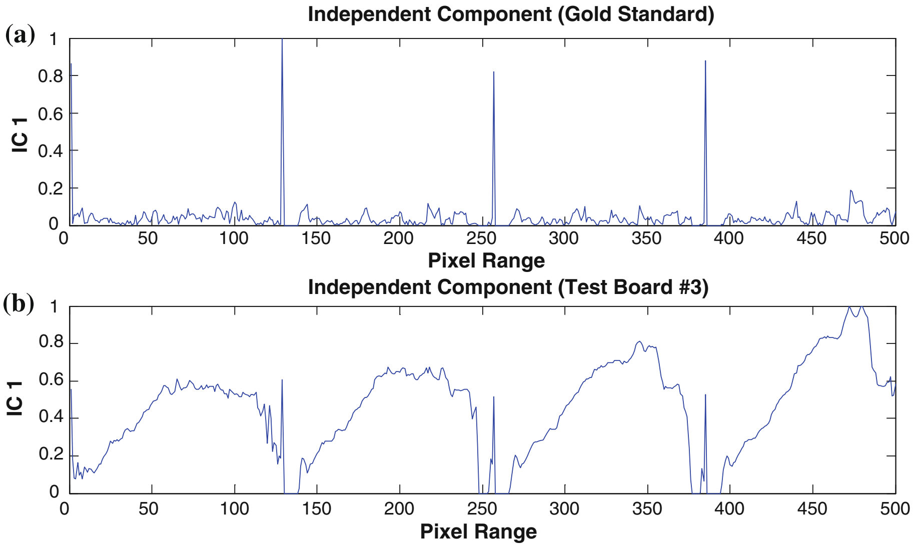

Fig. 8 Illustration of source separation via ICA, and demonstration of counterfeit detection (from a thermal emissions perspective only). **a** Primary independent component that represents a "Gold Standard," **b** primary independent component from a different source

from a second simulation run where a suspected counterfeit board is gauged against our benchmark. Similarly to the previous example, this illustration demonstrates that the FPGA from our suspected counterfeit board also exhibits a different independent component and does not match that of our benchmark PCB. Therefore, it can also be recognized as not authentic, i.e., counterfeit or altered.

7 Conclusion

In this paper, we have proposed a framework for separating thermal signals obtained from PCB to ascertain whether the electrical component may be counterfeit. We assumed that each individual electronic component on the board has the same kind of temporal dependencies as well as they have nonstationary smoothly changing variances. This made it possible to propose a cumulant-based contrast function that was shown to separate the unique thermal or IR signatures without necessitating estimation of a model of the source dependencies. Additionally, these unique signatures were able to be compared to a "Gold Standard" generated from known authentic electronic parts.

The methodology presented was dependent upon acquiring the IR imagery off-line prior to applying the ICA algorithm, and it was required to separate mixtures of sub-Gaussian, skewed, near-Gaussian, and super-Gaussian source signals to obtain the desired source signals. Future research will focus on an adaptive approach where the IR imagery can be captured in near real-time versus off-line. Also for forthcoming work, we will investigate an adaptive ICA algorithm based on fully multiplicative orthogonal group. This type of process can instantaneously separate mixtures of sub-Gaussian and super-Gaussian source signals as well as separate skewed and/or near-Gaussian signals, which are common in the IR imagery of our application.

Acknowledgments This work was supported by the U.S. Missile Defense Agency under contract award HQ0147-12-C-6020.

References

Birdsong B (2012) Trusted Electronics Summit 2012. The U.S. Missile Defense Agency Electronics Quality Assurance Trusted Electronics Summit

Birdsong B, Schipp F (2012) Missile Defense Agency (MDA) counterfeit awareness training—avoidance, detection, containment, and reporting briefing. MDA, US

Bumgarner J, Coleman G, Smith A, Willems M, Wren S (2010) Department of defense 2010 comprehensive inventory management improvement plan. The Department of Defense

Comon P (1994) Independent component analysis, a new concept? Signal Process 3:287–314

Dickler J (2012) Top 10 counterfeit goods (Online). Available: http://money.cnn.com/galleries/2012/pf/1202/gallery.counterfeit-goods/index.html

Gilmore ET (2011) Fundamental performance limits in image fusion, Ph.D. Dissertation, Howard University, Washington, D.C

Herault J, Jutten C (1987) Space or time adaptive signal processing by neural network models. The Proceeding for the American Institute of Physics (AIP) Conference Proceedings on Neural Networks for Computing. 206–211

Holliday AJ, Kay J (2005) The use of infrared viewing systems in electrical control equipment. The Proceedings for the 2005 Pulp and Paper Industry Technical Conference, Jacksonville, FL. 291–295

Hughitt B (2008) counterfeit electronic parts. Trilateral safety and mission assurance conference, National Aeronautics and Space Administration (NASA) European Space Agency (ESA) Japan Aerospace Exploration Agency (JAXA), April 2008

Jadhav SD, Bhalchandra A (2008) Blind source separation: trends of new age-a review. The Proceedings for the 2008 Institution of Engineering and Technology (IET) International Conference on Wireless, Mobile and Multimedia Networks, Mumbai, India. 251–254

Johnson NB (2012) How NASA fights counterfeiting (Online). Available: http://www.federaltimes.com/article/20121130/DEPARTMENTS01/311300005/How-NASA-fights-counterfeiting

Jutten C, Herault J (1991) Blind separation of sources, Part I: an adaptive algorithm based on neuromimetic architecture. Signal Process 24:1–10

McFadden F, Arnold R (2010) Supply chain risk mitigation for IT electronics. The Proceedings of the 2010 IEEE International Conference on Technologies for Homeland Security (HST), Waltham, MA, 49–55

National Security Council. The Comprehensive National Cybersecurity Initiative (2009). Available: http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative

Parra L (2002) Tutorial on blind source separation and independent component analysis. Adaptive Image & Signal Processing Group, Sarnoff Corporation

Pecht M, Tiku S (2006) Bogus: electronic manufacturing and consumers confront a rising tide of counterfeit electronics. IEEE Spectr 43:37–46

Stein J (2012) Government-Industry Data Exchange Program (GIDEP) facts sheet. Government-Industry Data Exchange Program