Physical Inspection for Counterfeit Detection

Kevin King, David Orosz, Christopher Smedberg

May 2, 2013

Abstract

Integrated circuits (ICs) are an integral part of the modern electronics industry. In turn, counterfeiting these chips has become an illegitimate way to save money and maintain high profits. As counterfeit chips are much less reliable than their authentic counterparts, serious harm (to both devices and their users) can come out of using them. We can however try to detect counterfeits before they are used, reducing any chance of equipment harm and unneeded expenses. We will focus our efforts on revealing exterior defects that are caused by the most common methods of counterfeiting. This can be done by using a scanning electron microscope to image and uncover irregularities caused by the counterfeiting process, and through a physical inspection of the exterior. Using the combined results of these tests we can issue a grade for each individual chip and help to alienate the counterfeits.

1 Introduction

As integrated circuits are used in most of today’s technologies, their cost and effectiveness play an important role in the fabrication of devices. Due to the importance of cost, the problem of counterfeiting chips has risen over the past few decades. Today, counterfeiting is a billion-dollar industry that relies on out-sourcing manual labor to third-world countries. In 2011 the estimated cost of counterfeit chips in the US supply chain was over $5 Billion\(^1\). There are many different types of counterfeiting, but the most prevalent (and most problematic) is recycling of ICs. In fact, 80\% of all counterfeit chips are recycled. Around the world, electronic devices containing valuable parts are discarded. Many of these un-usable devices are sent to developing countries, where the useful ICs are taken off and resold into the market (at a much cheaper price than new ICs). This whole process causes already unreliable chips to become even more unstable. While cost-effective, the negative impacts of recycling ICs greatly outweigh the benefits.

2 Original Problem Statement

\(^1\) "Combating fake chips by controlling supply chain - EE Times." 2012. 28 Apr. 2013 <http://www.eetimes.com/design/military-aerospace-design/4399254/How-semiconductor-re-creation-reduces-counterfeit>
The supply chain of an integrated circuit has three major tiers in which a transaction can occur. The three tiers are: the Original Component Manufacturer, Authorized Distributors, and Independent Distributors or Brokers. If a company happens to be in a position of leverage they can place a large order with the OCM and almost ensure that they are getting a correctly built part for their device. As the order gets smaller, the company may not be in a position to deal with the manufacturer directly and would have to turn to one of the second or even third tier distributors. When this happens there are more chances for counterfeit chips to be “slipped” into the system and the ability of the company to guarantee receipt of an original diminishes. One way this happens is through IC recycling.

When an IC is recycled it is cleaned to appear as if it were new. A common practice is for the chip to have the markings on the top sanded off and then it is “black topped” or coated with a material or paint so it appears new. It is then remarked, repackaged and sold back to a supplier. We will work under the idea that when this new material is applied it changes the chemical makeup of the exterior. We can then test this top portion to determine its authenticity. We will do this in two ways: using a scanning electron microscope, and the widely used acetone test.

3 Theory

3.1 Applications

Detecting whether an IC has been recycled can sometimes be as simple as looking at the packaging that it arrives in. Damaged and reused packaging or an improperly sealed ESD bag could be potential signs of a recycled part. Once opened, the part could lack the proper pin protection (usually a piece of foam that protects the pins from abuse.) Depending on the size a shape of the chip, they may not arrive in a bag at all. Component suppliers also use ESD safe “tubes” in which to package their chips. These tubes are cheap, easy to source, and give the appearance of legitimacy. One can assume that over time the cost to package counterfeit chips will become so small that all counterfeits will arrive in new packaging making this simple identification process unreliable. What then do we have to look for to identify a counterfeit? That question again has a very complex answer since there are many different ways to approach this problem. For our project we focused on the counterfeiting method nicknamed “blacktopping.”

3.2 Blacktopping

Blacktopping, as stated earlier, is a process in which an IC has its exterior re-coated so as to appear new. When an original IC is made at the OCM it has certain codes applied to the chip.

---

These codes show the batch that the chip originates from, where it was made (country), and the
date it was manufactured. Since these codes can be used to identify a chip the counterfeitors
first need them removed. They do this by sanding or lightly scraping the markings off the chip. If
they were to stop here the chip would have obvious signs of tampering. To cover up the signs of
tampering the counterfeitors will then apply a solvent-soluble, non epoxy based coating to the
outer surface. This coating, when applied correctly, removes all signs of sanding/scraping and
gives the chip the appearance of being new. After the coating has dried the chip is then
remarked with new, fake codes. These codes appear to be legitimate but could not be used to
trace the chip back to its source correctly. This coating however is very different from the
packaging used during the manufacturing process and when tested correctly, can be easily
identified.

4 Proposed Solution

4.1 Image Processing (solution)
Sandblasting, the precursor step to blacktopping, causes counterfeit ICs to appear similar to
their genuine counterparts when examined via the naked eye. However, when closely examined,
there are clear differences between the textures of the two. To obtain these close-up views, or
“fingerprints,” a high magnification microscope is a necessity. This is why we propose the use of
a scanning electron microscope (SEM) to determine outlier images. By definition, an outlier is a
statistical anomaly in a set of similar values, and can be determined by establishing a distribution
function with these values. Basically, if a set of images can be processed in such a way that
they are reduced to single values, outlier analysis can be used to determine which of them are
different (and therefore, suspect).

The first step in this process is to obtain the images using an SEM. A scanning electron
microscope produces a high-resolution, high-magnification image, which is very useful for outlier
analysis. An SEM works by using electrons instead of light to form an image. A beam of
electrons is sent through electromagnetic fields and lenses, which focus it toward the sample.
Then, X-rays are released from the backscattering of electrons and are collected via a sampler
to form the image.³ By just looking at the fingerprints obtained from the SEM, one can tell the
difference between genuine and counterfeit chips. Figure 1 shows the comparison of some
package textures.

![Figure 1: Package texture images of a genuine chip (left) and a counterfeit chip (left) obtained from SEM](http://www.purdue.edu/ rem/rs/sem.htm)

³ Purdue University, dept. of Radiological and Environmental Management. “Scanning Electron Microscope.”
To allow for automated detection of outliers, the next step in this process is to convert these obtained images to a single value. This is very straightforward, as it merely requires us to convert the images from RGB values to grayscale, and then determine a threshold grayscale value. Because of the simplicity of its built-in functions, MATLAB was used in our project. However, any language with an image processing toolkit could be used. Specifically, the process works using the following steps… (1) Convert to grayscale so that only one value will represent each pixel, as opposed to three. (2) Enhance the image using an adjustment function, allowing each level of gray to be more distinct. (3) Calculate the average pixel grayscale value and turn set all pixels under that value equal to 1. (4) Finally, store all of the 1’s in an array for each image.

After a unique “whitespace” array, representing the amount of pixels under the threshold, has been established for each image, the final step is to plot a distribution graph and determine if there are any outliers. Because all fingerprints of a constant magnification look very similar (and therefore have similar whitespace arrays), the set of images should form a normal distribution. A normal, or Gaussian, distribution is a probability function where the median, mean, and mode are approximately equal.\textsuperscript{4} forming a bell curve. Equation 1 is the normal distribution function.

\[
\frac{1}{\sqrt{2\pi}\sigma^2} \exp \left\{ -\frac{(x - \mu)^2}{2\sigma^2} \right\}
\]

(1)

Once the array containing the whitespace value for each image is converted to its distribution, the bell curve can be plotted and any numbers far away from the median are considered outliers. In this project, outliers are points that are more than two standard deviations away from the median. By the three-sigma rule, 95\% of values should occur within the first two deviations.\textsuperscript{5} MATLAB then returns the corresponding outlier images to the user as outputs.


4.2 Physical Inspection

Physical examinations of chips is an easy way to detect blatant counterfeits and should be the first step in counterfeit detection. Physical inspections of the chips should include a low-power visual inspection along with some type of surface and marking permanency test. Both of these tests will involve a human interaction and require that tester to be trained to detect signs of counterfeiting.

During the visual inspection, the tester should be checking the chip’s package, pins, and markings. The package should be checked to make sure it is the correct type of packaging, that there are no blatant signs of wear, and that there is no evidence of blacktopping. If the tester notices scratches, scuffs or other marks on the chips packaging, it can be a sign that the chip has been used before. When checking the pins, the tester should make sure that there are the

---


correct number of pins that should be present for that type of chip, that the pins are not bent, and that there are not other signs of wear or discoloration on the pins. When checking for signs of blacktopping, the tester should make sure that the color and texture of the packaging is similar to known good chips. An easy test for blacktopping can also be done by trying to scratch the surface of the chip with the edge of a razor blade. This should typically not remove material from the package, but may remove material if the chip has been blacktopped. Finally, the tester should check to make sure that the markings resemble markings expected on the chip and that the markings are not faded, poorly lined, or blurry.

Another test that requires human interaction to complete is a marking permanency test. This test is used to detect the presence of a counterfeit chip by checking for evidence of blacktopping. During the blacktopping process, a material similar to the material used during manufacturing is used to resurface the chip and and remove old markings and signs of aging. After blacktopping, the chip also needs to be re-marked. Marking permanency tests hope to detect the use of blacktopping or re-marking by applying solvents to the surface of the chip. Two different solvents were used to implement the marking permanency tests. One solvent was one part denatured alcohol and three parts mineral spirits, and the other solvent was one-hundred percent acetone.

5 Results

5.1 Image Processing
The outlier detection process has promising results. Starting with 17 png images in a given directory, all were successfully converted to binary and compared using a Gaussian distribution through the use of MATLAB. Figure 2 shows the images in their directory. The top-left image, “g1.png”, is the outlier.

![Fig. 2: The 17 images that were compared using outlier detection. The top-left image is the outlier.](image)

After the images were converted to grayscale, the average pixel value was calculated. This allowed all images to be converted to binary, as shown in figure 3.
Finally, MATLAB was able to detect the outlier by plotting a Gaussian distribution curve. The program was able to identify the outlier by calculating it to be more than two standard deviations away from the median. Both the command window output and the Gaussian curve are shown in Figure 4. The blue vertical lines in fig. 4 represent standard deviations.

5.2 Physical Inspection
The physical inspection and tests did yield some results. For the physical inspection and marking permanency tests, we tested two known counterfeit Motorola microprocessors and one
known genuine version of the same microprocessor. The three chips we tested, and before and after marking permanency test images can be seen in the chart below. To summarize the results, the visual inspections and first marking permanency test did not show any difference between the genuine and counterfeit chips. However, when using the acetone in a marking permanency test we did get results. When using the acetone to test the known counterfeit chips, the surface of the counterfeits became inconsistent in color and texture. Also when testing the known counterfeits, the cotton ball that was used to apply the acetone had color transferred to it from the surface. Images of the cotton balls can be viewed below. When using the acetone on the known genuine chip, the chip’s surface did not change and there was no color transferred to the cotton ball.

<table>
<thead>
<tr>
<th>Chip Name</th>
<th>Chip Image</th>
<th>Pin Inspection</th>
<th>Capping Inspection</th>
<th>Inspection after Acetone Test</th>
<th>Inspection after Alcohol/Mineral Spirits Test</th>
<th>Image after Solvent use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Genuine</td>
<td><img src="image1.jpg" alt="Genuine Chip Image" /></td>
<td>Little to no wear/dark discoloration</td>
<td>Consistent color and texture. Clean markings</td>
<td>No effect</td>
<td>No color on cotton swab</td>
<td>No change in texture</td>
</tr>
<tr>
<td>Counterfeit 1</td>
<td><img src="image2.jpg" alt="Counterfeit 1 Chip Image" /></td>
<td>Little to no wear/dark discoloration</td>
<td>Markings do not match genuine, but clean markings. Consistent color and texture to cap</td>
<td>Color transfer to cotton swab (see fig 1)</td>
<td>Inconsistent color and texture around markings</td>
<td>No change from Acetone Test</td>
</tr>
<tr>
<td>Counterfeit 2</td>
<td><img src="image3.jpg" alt="Counterfeit 2 Chip Image" /></td>
<td>Little to no wear</td>
<td>Markings do not match genuine, but clean markings. Consistent color and texture to cap</td>
<td>Color transfer to cotton ball (see fig 1)</td>
<td>No noticeable change in texture or color of cap</td>
<td>No change from Acetone Test</td>
</tr>
</tbody>
</table>

**Figure 1.** Chart showing results of visual inspection and both marking permanency tests

**Figure 2.** Cotton ball showing color transfer from first counterfeit
6 Obstacles Encountered

6.1 Image Processing
The most problematic obstacle encountered in the image processing part of this project was computational inefficiency. The outlier detection process relies on each image being examined pixel by pixel. In the case where there are thousands of images being analyzed, this can be a very slow process. There are many solutions to the problem of algorithm speed, but those are a matter of mathematical analysis, and are essentially optimization issues. If this project were to be extended into a professional application, that would be one of the first issues to be worked on. Another problem with the outlier detection process is the ambiguity of the threshold detection step. This step is based on the mean value among all pixels in all images in the directory. In addition to the slow computation of this value, the fact that it is merely an average could prove to be arbitrary. In other words, no one knows for sure whether or not a strict average is the appropriate threshold- that is based on the type of image. This can be fixed through exhaustive testing.

7 Budget
We were given a $5000 dollar budget for this project. The only costs were $150 for a Dremel tool used in the first half of the semester, and $30 for the acetone to perform the physical inspection. The chips used were extras given to us from another project.

8 Conclusion
Trying to catch a counterfeit chip is a constant game of cat and mouse. As methods are developed to catch a counterfeit workarounds are created. Counterfeiters have already
developed a method of blacktopping that is resistant to solvents\(^6\). The material being used to blacktop could be coated with a thermal or UV cured epoxy\(^7\). This coating will not react to acetone and could give a false positive.

Preventing the purchase of counterfeit devices starts when the order is placed. Placing orders with the OCM or its authorized distributors is one recommended way of preventing counterfeit purchases\(^8\). As stated earlier, the ability to purchase all parts from the OCM or its authorized distributors may not be possible. What if only one chip is needed or the chip needed is no longer in production? Then the only place to purchase from may be a third tier distributor or broker. By purchasing from these distributors the buyer has removed some protection against counterfeiting.

Based on the research performed during this project we recommend the following guidelines to follow when purchasing devices. First, always try and purchase parts from the OCM or its authorized distributors. This alone will reduce your exposure to the black-market of counterfeiting. If this can’t be done and material must be sourced from a third tier distributor (non-authorized or broker) then all parts, upon receipt, must be considered counterfeit until proven otherwise. The acetone test should be performed and can quickly help to eliminate inexperienced counterfeiting techniques. If all chips pass the acetone test then a random chip should be scraped to check for an acetone resistant coating having been applied. If the first two tests do not uncover a counterfeit then the final test should be to use an SEM to image the device and have it compared using the image processing techniques outlined in this report.

---

\(^6\) "Bride of Blacktopping: microchip counterfeiters are getting smarter …" 2011. 22 Apr. 2013

\(^7\) "Counterfeit components avoidance program, certification." 2008. 28 Apr. 2013

\(^8\) "Counterfeit microcircuits - U.S. Senate Armed Services Committee." 28 Apr. 2013