4-25-2017

Lithography, Spectroscopy, and Super Resolution Terahertz Imaging for Quality Assurance and Authentication

Kiarash Ahi
kiarash.ahi@uconn.edu

Lithography, Spectroscopy, and Super Resolution Terahertz Imaging for Quality Assurance and Authentication

Kiarash Ahi, PhD

University of Connecticut, 2017

The supply chain today spreads all around the globe. For assembling a system, several components, each of which may be produced in a different country and by a different manufacturer, need to travel the globe to get to the assembly sites. In such a global supply chain, tracing the components could be a great challenge and counterfeiters can find open doors to infiltrate the markets. Several billions of dollars of counterfeit integrated circuits (IC)s are sold each year. Low-quality authentic ICs might also pass the quality control sections and enter the supply chain occasionally. The endurance and reliability of the counterfeit and low-quality ICs are less than those of their authentic counterparts, and besides economical damage, unexpected system failures as a result of the failure of a counterfeit component can lead to loss of lives. As a result, quality management, authentication and counterfeit prevention in today`s electronic industry play a crucial role. The semiconductor business is constantly expanding and as a result, more counterfeiters become attracted to the semiconductor device manufacturing. Moreover, counterfeiters are constantly trying more complicated techniques to avoid being exposed. As a result, the counter-counterfeit industry needs to constantly develop new techniques for revealing the counterfeiters. From the quality management point of view, as the technology becomes more advanced, more advanced techniques are needed to control the quality of the ICs before entering the supply chain and prior to being selected in the assembly sites. In this work, we develop innovative techniques for quality management, authentication, and counterfeit detection.

In the first part of this work, encrypted micro-signatures are designed and fabricated by electron beam lithography (EBL) on the ICs. These signatures travel on the ICs through the global supply chain. Once the component is received at the assembly site, the signature is decrypted and authenticity is proved.

In the second part of this work, we developed advanced innovative techniques for physical inspection of the ICs by the use of terahertz (THz) spectroscopy and imaging. Recycled, blacktopped, and reverse engineered ICs are all detected by our THz authentication system.

In the third part, we realized a resolution enhancement technique (RET) for developing super-resolution THz images. This RET enhances the resolution of the THz images by more than 10 times, enabling the THz imaging systems to image and measure the dimensions of the features by accuracies beyond Abbe`s diffraction limit.

Lithography, Spectroscopy, and Super Resolution Terahertz Imaging for Quality Assurance and Authentication

Kiarash Ahi, PhD

University of Connecticut, 2017

A Dissertation

Submitted in Partial Fulfillment of the

Requirements for the Degree of

Doctor of Philosophy

at the

University of Connecticut

2017

APPROVAL PAGE

Doctor of Philosophy Dissertation

Lithography, Spectroscopy, and Super Resolution Terahertz Imaging for Quality Assurance and Authentication

Presented by

Kiarash Ahi

Major Advisor _____
Rajeev Bansal

Associate Advisor _____
Marten van Dijk

Associate Advisor _____
Sina Shahbazmohamadi

University of Connecticut
2017

Acknowledgements

I thank God who gave me the opportunity of keeping an open mind for stepping out of my comfort zone for traveling the world, doing research to find the answers to my curiosities and discovering the beautiful new horizons. I am grateful that I chose to keep a strong will toward using my time, intellectual power and resources for pushing my limits, using my capabilities to the full extent, making my dreams come true, and making changes in my life and others for the better.

I am grateful for the endless opportunities that the University of Connecticut and this great nation provided me toward pursuing my education, gaining the experience of teaching, earning an independent life, and doing research in the fields of science and engineering. I recognize the brave efforts of the men and women who came here before me, established this system and paved the roads for the successors. I am also grateful for the hard work of all the scientists from four corners of the world who developed the physical and mathematical theories during the history. Thanks to their great work, we could develop our theories and make advancements toward continuing their direction.

I would like to thank my parents, who raised me by making me believe in my physical and intellectual capabilities, valuing hard work, respecting science and research, and dreams of achieving academic excellence. Having such busy parents with research in academia imposed a huge distance between me and them, but also made me familiar with the great value of knowledge and learning, and made me determined to overcome the hardships of achieving academic excellence.

I would like to thank Dr. Rajeev Bansal, Professor & Head of the Department of Electrical & Computer Engineering at the University of Connecticut. He brought me hope by just a few sentences of kind advice when I wanted to withdraw from my Ph.D. program back in 2014.

I would like to thank Dr. Marten van Dijk, who opened new horizons about the philosophy of research and science, during the course “Natural Computation”, and supported me during different levels of my career and personal life.

I would like to thank my associate advisor Dr. Sina Shahbazmohamadi, who provided me with knowledge, samples, and facilities that I needed for performing my research, and supported throughout my education and finding my place in the semiconductor industry.

I would like to thank Drs. Sung-Yeul Park and Ali Bazzi, who gave me my initial admission to UConn, although I couldn`t have a chance to work with their groups.

I also would like to thank Dr. Mehdi Anwar who assigned me to do research in the new fields and helped me to discover new horizons of research.

I am also very grateful to my professors, Drs. Geoff W. Taylor, Faquir Jain, Helena Silva, John Ayers, Quing Zhu, Steven Schoenecker, and Ali Gokirmak, who have been great mentors to me and taught me the knowledge that leads to achieving the models and results of this dissertation.

Finally, I would like to thank my wife Kaalyn, who always inspired me to work hard toward achieving academic excellence. She never complained about my busy schedule of research.

Table of Contents

List of Figures

1

Fabrication of robust micro-signatures for identification of authentic electronic components and counterfeit avoidance

1.1 Abstract

In this chapter, a novel approach for marking integrated circuits capsulations with authentication micro-signatures is introduced. The signature patterns are fabricated using electron beam lithography. Moreover, the robustness of these signatures against aging and humidity is investigated. A technique comprising image processing and measuring similarity indices has been developed. These signatures are proposed to be fabricated in the manufacturer side of the supply chain. Then, they are decoded at the customer end. Thus, robustness against ambient environment and aging is a requirement for them to survive in the supply chain. Calculated Mean Square Error and Structural SIMilarity Index confirms that the reflected patterns of the signatures remain unchanged against aging and humidity.

1.2 Introduction

Since the early civilizations, counterfeiting of customers` goods has been always a great hindrance in front of innovation and protection of intellectual property. As the technology becomes more sophisticated, concerns about the early failure of the critical equipment grow. These critical systems consist of thousands of electronic and mechanical components. Consequently, having one counterfeit component may result in the failure of the entire system. Such failures are responsible for many deaths each year [1].

Electronics components travel all around the world before they are assembled into different systems. Each component is made in a different part of the world. It is more economical for the

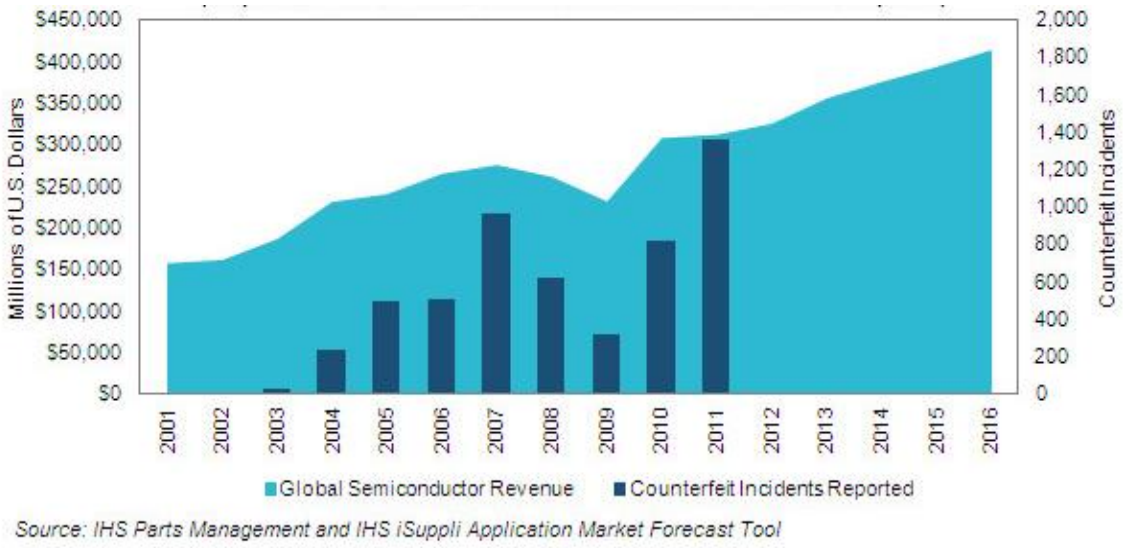


Figure 1.1. Global semiconductor revenue correlated with reports of counterfeit parts [3]

companies to obtain their needed components from various foundries. However, tracking all the components in such global market is not possible. Thus, counterfeiters have more freedom to inject their products in the supply chain nowadays [2]–[4].

The financial loss of supply chains due to counterfeit electronic components is reported to be higher than $10 billion per year in 2010 [1]. This loss would be more serious when one considers equipment failures because of malfunctions of counterfeit electronic components. More broadly, the counterfeiting and pirated products have imposed substantial damages on the economies worldwide. The total value of counterfeit and pirated products in case of G20 countries is reported to be up to $650 billion in 2008 and it is predicted to rise to $1,770 billion in 2015 [2]. As the electronic industry is growing fast, counterfeit electronic components bring more revenue to the counterfeiters and thus, more electronic counterfeit components are injected into the market. As Figure 1.1 indicates, the counterfeit electronic component incident reports have closely followed the global semiconductor revenue so far. Consequently, since a sharp rise in electronic components

market is predicted, a similar rise in counterfeit components is expected. As customers and suppliers are developing more advanced methods for detecting counterfeit components, the counterfeiters also make their techniques more sophisticated [3]. Consequently, innovative approaches for detecting counterfeit components are needed to be continually devised.

Most of the methods for detection of counterfeit ICs have been based on physical inspections and electric tests [4]–[7]. As counterfeiters are making their approaches more advanced, the need for incorporating signatures on the electronic components is arising. Such signatures are not only needed to be invisible to counterfeiters but they also should not be replicable by counterfeiters. Towards this aim, engineered microstructures (EMS) have been implemented on the surfaces of integrated circuits (ICs) and approaches to detect them without the need for sophisticated costly machines are developed [8], [9].

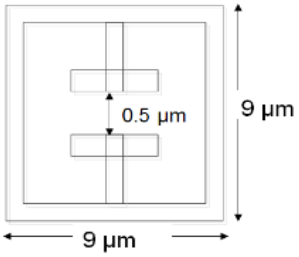
This chapter introduces a novel approach for implementation and detection of EMS for identification of authentic electronics components and any other products in general. It is believed that the proposed technology offers a tool (1) which allows identification of good ICs, and (2) which makes it impossible to resurface and re-introduce in the market since sanding of the surface destroys the EMS [10].

The application of these signatures implies that they need to be robust against aging and ambient environment effects. These signatures are required to survive the long journey in the supply chain from the manufacturers to the customers. In this chapter, a technique comprising image processing and measuring similarity indices is developed to investigate the endurance of the fabricated micro-signatures as they are exposed to the high humidity and aging process. Calculated Mean Square Error (MSE) and Structural SIMilarity Index (SSIM) proved that the reflected patterns of the signatures remain unchanged against aging and humidity.

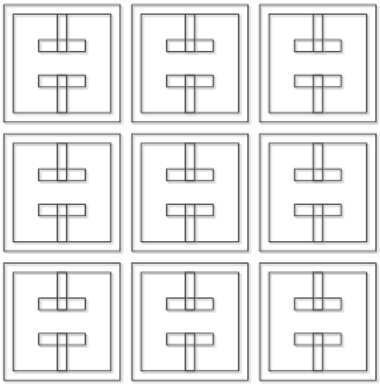
This chapter is organized as follows: Section 3 introduces the procedures for the fabrication of EMS using electron beam lithography and the concepts of matrix patterns that can carry coded signatures. Section 4 provides a technique for the investigation of the robustness of EMS against effects of aging and the ambient environment. The results provided in this section prove that the reflected patterns of the signatures remain unchanged against aging and humidity.

1.3 Engineered Microstructures

The incorporation of EMS may either be carried out by transferring the pattern to a thin metallic layer on the IC capping material or can be a direct write on micro-imprint. Engineered patterns ranging in size from micrometers to submicron dimensions are incorporated on the IC capping material as a tool for the identification of authentic ICs. Figure 1.2 shows a cell and a 3 × 3 array of an engineered microstructure that should be recognized as a standard micro-signature structure imparting the properties of an encrypted signature matrix. As this Figure also indicates, the structure is fabricated on the surface of a commercially available IC using Electron Beam Lithography (EBL) followed by Au sputtering.



(a)



(b)

(c)

Figure 1.2. (a) An EMS cell, (b) A 3 × 3 array of EMS, (c) The EBL system in UConn used for fabrication of the EMS

The EMS is invisible to the naked eyes but is detectable by using inexpensive and fast optical probing such as shining a laser pointer on the surface of the IC as shown in Figure 1.3. The Figure shows the experimental setup that includes a laser pointer, a focusing lens, the device under test and the reflections.

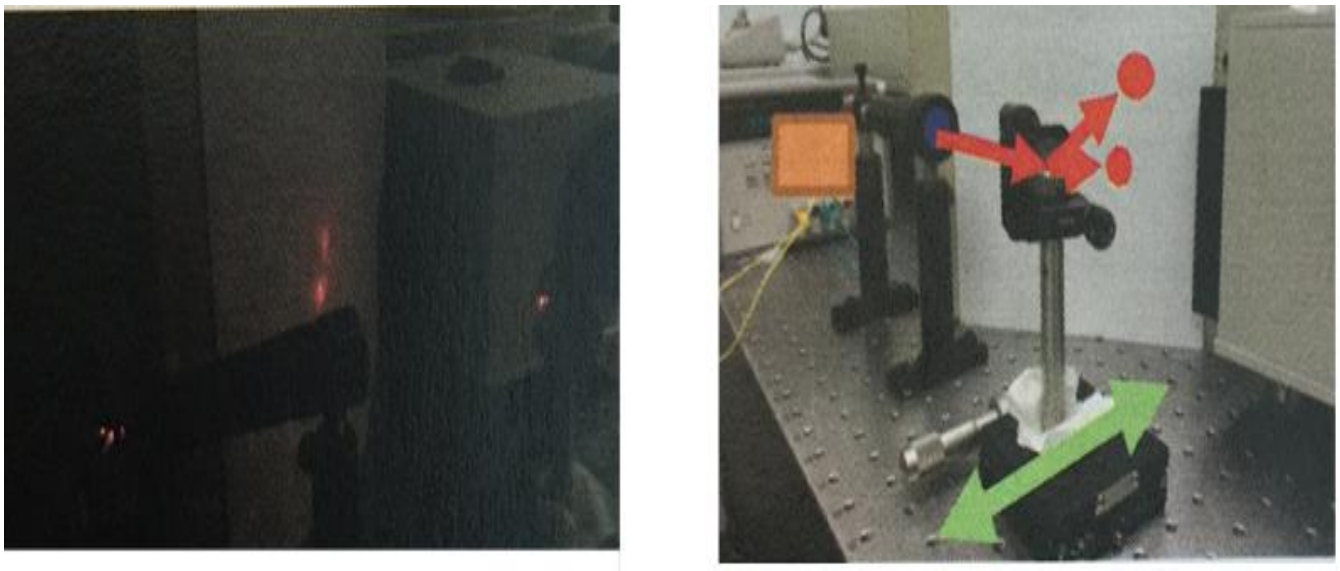


Figure 1. 3. The experimental setup and the presence of a second reflection introduced by the encrypted signature matrix

1.4 **Robustness of the EMS against Aging and Ambient Effects**

An electronic component travels all around the world in the supply chain until being assembled in a system. The component is exposed to the different ambient environment until it is received by the customer. This journey also takes time and the EMS is aged. Consequently, the application of the proposed technology requires the structures to remain robust against aging. Moreover, the second optical reflection that is correlated to the signature matrix must remain invariant during all the changes in ambient over time. Figure 1.4 depicts the journey of the EMS in the supply chain, between the manufacturer and the customer.

To investigate the robustness of the fabricated structures, the EMS is exposed to different ambient environment and aging. After these exposures, different similarity indices are computed. Figure 1.5-(a) depicts the EMS reflection under different ambient effects. For the case of the determination of the effects of the ambient environment on the EMS, the images of the laser reflections from the EMS (1) after the EMS has been exposed to high moisture and (2) once the EMS has been stored for three months in the room environment, are obtained. The obtained images

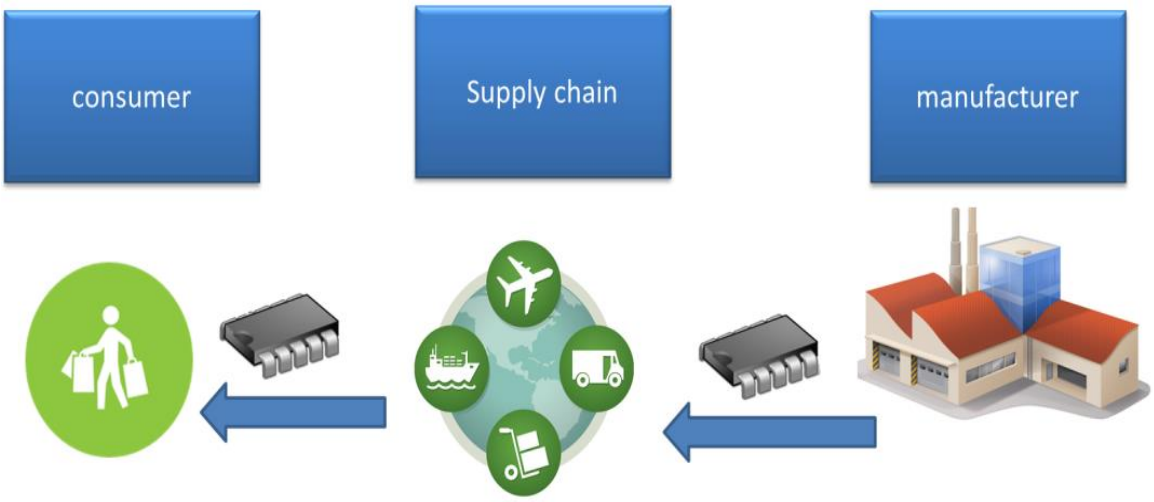


Figure 1. 4. The journey of a component in the supply chain

are then compared to the image of the laser reflection from the fresh EMS by SSIM, MSE and Euclidean distance (ED). Also, an image processing technique is developed to make the images prepared for applying the mentioned similarity metrics.

As the first step of this technique, since the colors of the obtained images are not playing a role, the colors are filtered. Then, in the second step, before analyzing the images with SSIM, MSE, and ED, since the reflection from the EMS is brighter than the background, for suppressing the background noise, pixels with the luminance of lower than 0.2 are filtered. The resulting images and corresponding histograms after these two filtrations are illustrated in Figure 1.5. Then the overall similarities of the images in Figure 1.5-(d) are computed by using different metrics, namely SSIM, ED, and MSE. The reason that SSIM is chosen as a measure in this work is the fact that this metric has been developed as an index to determine the quality of a distorted image compared with its original counterpart [11], [12]. Here the quality of the exposed EMS to the ambient effects and aging is to be compared with the fresh EMS and thus SSIM can provide a good measure for this purpose. The algorithm for the calculation of this metric is developed based on the principles of human visual systems. The human visual system is mainly focused on detection of structures. Two

other parameters which are effective in the human visual perception of image fidelity and quality are luminance and contrast. Eq (1) indicates that SSIM index takes the three mentioned parameters into account, namely luminance, contrast, and structure.

$$SSIM(x,y) = [l(x,y)]^{\alpha} .[c(x,y)]^{\beta} .[s(x,y)]^{\gamma} \quad (1)$$

Where l, c and s are representing similarities in terms of luminance, contrast, and structure between two images respectively. $\alpha > 0$, $\beta > 0$ and $\gamma > 0$ determine the relative importance of these three components. Values between 0 and 1 are assigned to l, c and s, the higher the value, the higher the similarity of the corresponding parameter between the two compared images. The output is a value between 0 to 1. For this work, only the structural shape of the EMS determines the authentication of the product. Consequently, structural similarity is to be measured. For this purpose, the effect of the contrast and luminance are to be eliminated from Eq (1). By substituting $\alpha = \beta = 0$, we can extract the structural similarity from the SSIM index as:

$$SSIM(x,y) = s(x,y) = \frac{\sigma_{xy} + C}{\sigma_x \sigma_y + C} \quad (2)$$

In a more general SSIM index is a promising measure for determining the structural similarity. The results of measurement of the degradation of EMS by the above index are shown in Table 1.1. The high values of SSIM confirm the robustness of the EMS. As the EMS is aged its similarity to the fresh EMS decreases: the few days aged EMS is more similar to the fresh EMS than the 3-month aged EMS is. Also, the two aged ones are more similar to each other than to the fresh one. It is desirable to observe degradation in the EMS as a measure of aging. The object is exposed to

the high humidity in the supply chain and it must remain unchanged. However, for detecting the recycled aged components, observing the degradation in the EMS is an advantage.

For confirming the result with a completely different metric, MSE which has been one of the most well-known metrics to measure differences between two signals is also used [13]. The MSE between two arbitrary finite length discrete signals (which can represent two visual images) $x = \{x_i \mid i = 1, 2, \cdots, N\}$ and $y = \{y_i \mid i = 1, 2, \cdots, N\}$ is defined by Eq. (3).

$$\mathrm{MSE}(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i - y_i)^2 \tag{3}$$

Euclidean distance (ED) can be considered as the ordinary distance between two points and it is given by the Pythagorean formula. Consequently, for the two arbitrary finite length discrete signals *x* and *y*, ED can be calculated by Eq. (4).

$$\mathrm{ED}(x,y)=\sqrt{\sum_{i=1}^{N}(x_i - y_i)^2} \tag{4}$$

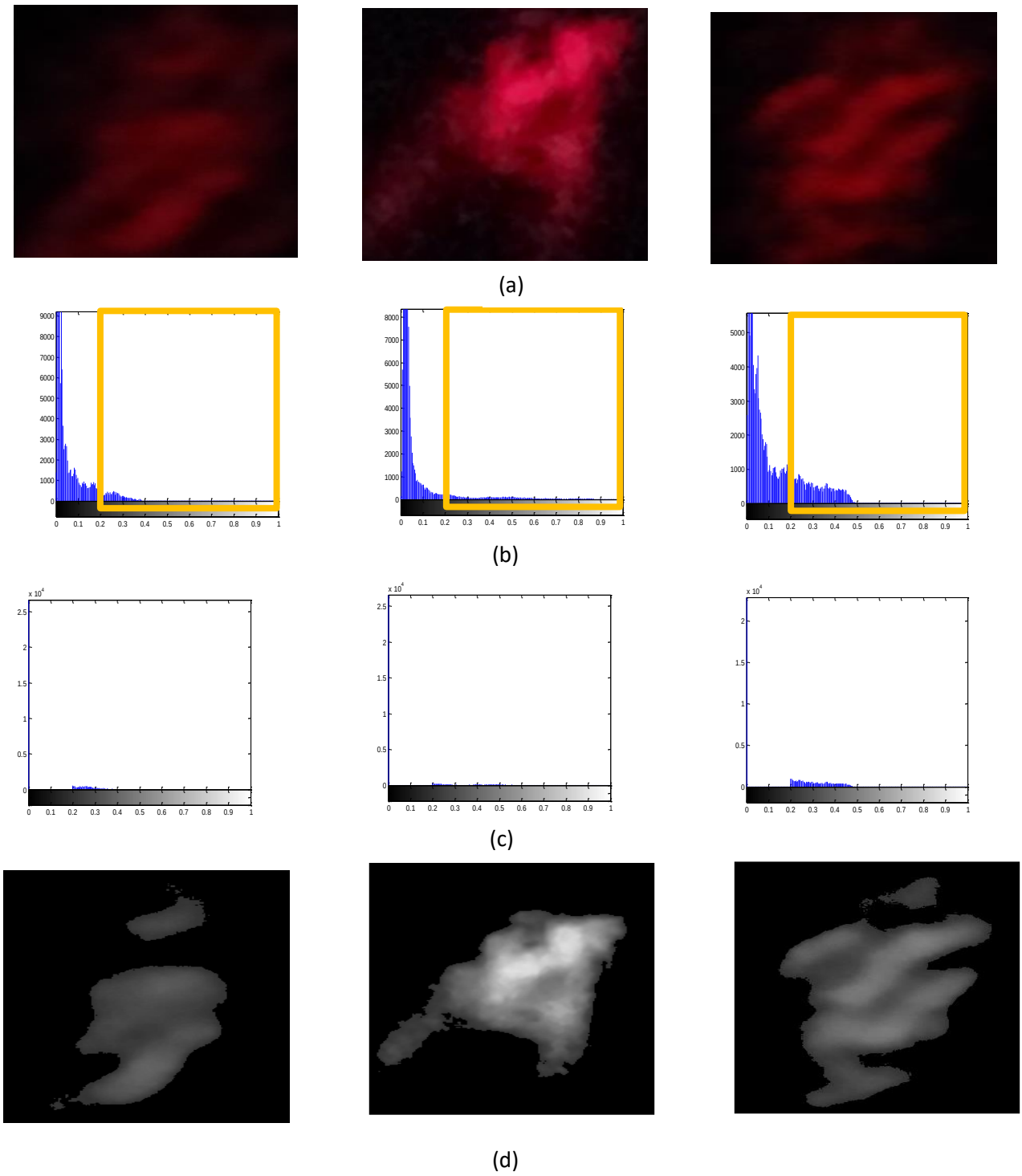


Figure 1.5. (a) Original images of the reflections of EMS (from left to right): without being exposed to ambient environment effects, after three months and after being exposed to high moisture. (b) Histogram of the original images in (a); the yellow windows show the filter window. (c) Histograms of the images after being filtered. (d) Images after filtering and removing colors.

Table1.1 Results of similarity measurements with SSIM, MSE and ED

Row #	The two images which are being compared to each other and the number of figure in with their corresponding fft2 is depicted		SSIM	MSE	ED
	First image	Second image			
1	High moisture	Original	0.9988	0.0077	18.3457
2	After a few days	High moisture	0.9969	0.0198	29.4204
3	After a few days	Original	0.9963	0.0237	32.1955
4	After a few days	3 months old	0.9802	0.1264	74.4005
5	3 months old	Original	0.9791	0.1333	76.4078
6	High moisture	3 months old	0.9779	0.1408	78.5268

The results of the degradation measurements using MSE and ED are also given by Table 1.1. Interestingly, the results from the SSIM are the same as the results from the MSE and ED, although the SSIM is based on a completely different logic to determine the similarities. This consistency between SSIM and MSE confirms the accuracy of the proposed approach. It is observed that calculated SSIM indices are very high, and MSEs are very small. It translates to the fact that the EMS are robust against aging and ambient effects.

1.5 Conclusion

In this chapter, a method for the fabrication of engineered micro-signatures was developed. Concepts of encoded matrices which can carry coded signatures were adopted to realize these signatures. The application of the proposed technology requires the structures to remain robust over time and under different ambient conditions. The fabricated structures were exposed to the different ambient environment and aging processes. Similarity indices were computed and it was observed that the EMS has not been degraded. In this way, the robustness of the engineered microstructures against effects of ambient environment is proved.

2

Encrypted electron beam lithography fabricated micro-signatures for authentication

2.1 Abstract

In this chapter, engineered microstructures (EMS) have been fabricated on the packed integrated circuits. Coding lookup tables were developed to assign different digits in numerical matrices to different fabricated micro-signatures. The numerical matrices are encrypted according to advanced encryption standard (AES). The encrypted numerical matrix is ink printed on the components, and the micro- signatures are fabricated on the packages of the chips via electron beam lithography (EBL). This process is to be done on the manufacturer side of the supply chain. The numerical matrix and the micro-signature accompany the product in its long journey in the global supply chain. The global supply chain is proved to be susceptible to counterfeiters. For keeping counterfeiters` hands out of the process, the cipher key and the coding lookup tables are provided to the consumer using a secure direct line between the authentic manufacturer and the consumer. On the consumer side, the printed numerical matrix is decrypted. Having the decrypted numerical matrix makes it possible to extract the micro-signature from the laser speckle pattern shined on the packaged product. In this chapter, an algorithm is developed to extract the micro-signature by having the decrypted matrix and reflected laser speckle patterns as inputs. Confirming the existence of the nan-signature confirms the authenticity of the component. Imitating the micro-signatures by the counterfeiters is not possible because there is no way for them to observe the shape of these signatures without having access to the cipher key.

2.2 Introduction

In this chapter, engineered microstructures (EMS) have been fabricated on the surfaces of integrated circuits. A method using image processing and pattern recognition was developed to

read the physical patterns of the micro-signatures. Encryption methods are adopted to keep the micro-signatures hidden from the counterfeiters.

The financial loss of supply chains due to counterfeit electronic components is reported to be higher than $10 billion per year [1]. This loss would be much more serious when one considers the equipment failures resulting from the malfunctions of counterfeit electronic components. The loss of lives due to these failures is beyond financial measures. The total value of counterfeit and pirated products in for G20 countries were reported to be up to $650 billion in 2008 and it was predicted to rise to $1,770 billion in 2015 [2]. As the electronic industry is growing fast, counterfeit electronic components bring more revenue to the counterfeiters and thus, more electronic counterfeit components are injected into the market. The counterfeit electronic component incident reports have closely followed the global semiconductor revenue so far. Consequently, since a sharp rise in electronic components market is predicted, a high rise in counterfeit components is expected. Most of the methods for detection of counterfeit ICs have been based on physical inspections and electric tests [14]–[17], [5], [4], [3], [6], [7]. As counterfeiters are making their approaches more advanced, the need for adding signatures on the electronic components is arising. Such signatures do not only need to be invisible from counterfeiters, but also not to be replicable by counterfeiters. These signatures are proposed as essential authentication means for industrial and healthcare electronics components.

In this work, complex matrix patterns were realized by putting different sizes of microstructures as entries in a matrix. These signature matrices which entries are EMS were formed to embed passcodes on the surfaces of the ICs. A novel method is developed for translating random patterns of EMS to the encrypted numerical matrices. The numerical matrices are encrypted using advanced encryption standard (AES) and then the encrypted matrices are translated to the EMS matrices

patterns using the developed EMS lookup table. EMS matrices are not visible unless the observer knows the assigned patterns in advance. Image matching between the translated EMS pattern from decryption of numerical matrix and the EMS pattern extracted from speckle laser pattern of the surface of the object proves the authentication of the object. The encrypted numerical matrix is printed in ink on the packages of the objects and is obvious to everyone. The EMS pattern, however, is fabricated using electron beam lithography (EBL) and is invisible.

The numerical matrix cannot be translated to the EMS pattern unless the cipher key and the dedicated EMS lookup table are both known. The fabricated EMS matrix cannot be extracted unless its pattern is known from the decrypted numerical matrix. Thus, counterfeiters cannot extract the EMS pattern shape from the surface of the object while customers can obtain the key from the authentic manufacturer. In this way, counterfeiters cannot replicate the EMS by reverse engineering. The flexibility of making random signatures, encryption with AES together with the possibility of dedicating a unique EMS lookup table for each series of the product makes it impossible for the counterfeiters to broke into the process and replicate it.

This chapter is organized as follows. In Section 2.3, the concepts of the micro-signatures, encryption and physical fabrication via EBL are discussed. In Section 2.4, the image processing approach for extraction of the EMS patterns from the laser speckle patterns based on matching concepts is developed. In Section 2.5, the theory is implemented in practice and is confirmed by practical results.

2.3 Concepts, encryption, and fabrication of the micro-signatures

The micro-signature matrix which consists of EMS entries is fabricated on the surface of the IC. Metamaterials with negative refractive indices are used for fabrication of the EMS matrix. The fabrication process and reliability of the process is discussed in [9], [10], [18], [8]. This matrix is

too small to be seen by an optical microscope and since the surface of the IC is not conductive, it is invisible to electron microscopes. Thus, counterfeiters cannot have access to the shape of the matrix to replicate it. An algorithm is developed to extract the pattern of this matrix from the speckle pattern. This algorithm is discussed in the next section. However, for the extraction of this matrix from the speckle pattern, the EMS pattern should be known in advance. In fact, the algorithm matches the known EMS pattern with the speckle pattern. If a match occurs, the authentication is done, otherwise, the object is determined to be counterfeit. The whole process of the authentication is depicted in Figure-2.1. The EMS is fabricated in the manufacturer on the surface of the packaged ICs. A numerical matrix is also printed on the package of the IC. This numerical matrix which is visible to everyone is encrypted using advanced encryption standard (AES) [19]. A lookup table is also provided to convert the decrypted numerical matrix to the EMS pattern. Once this matrix is decrypted and converted to the EMS matrix pattern, authentication of the product is proved. An example of the EMS lookup table is brought by Table-2.1. An EMS element and the conversion (coding) of the numerical matrix to the EMS pattern together with the AES encryption of the numerical matrix are shown in Figure-2.2 and Figure-2.3 respectively.

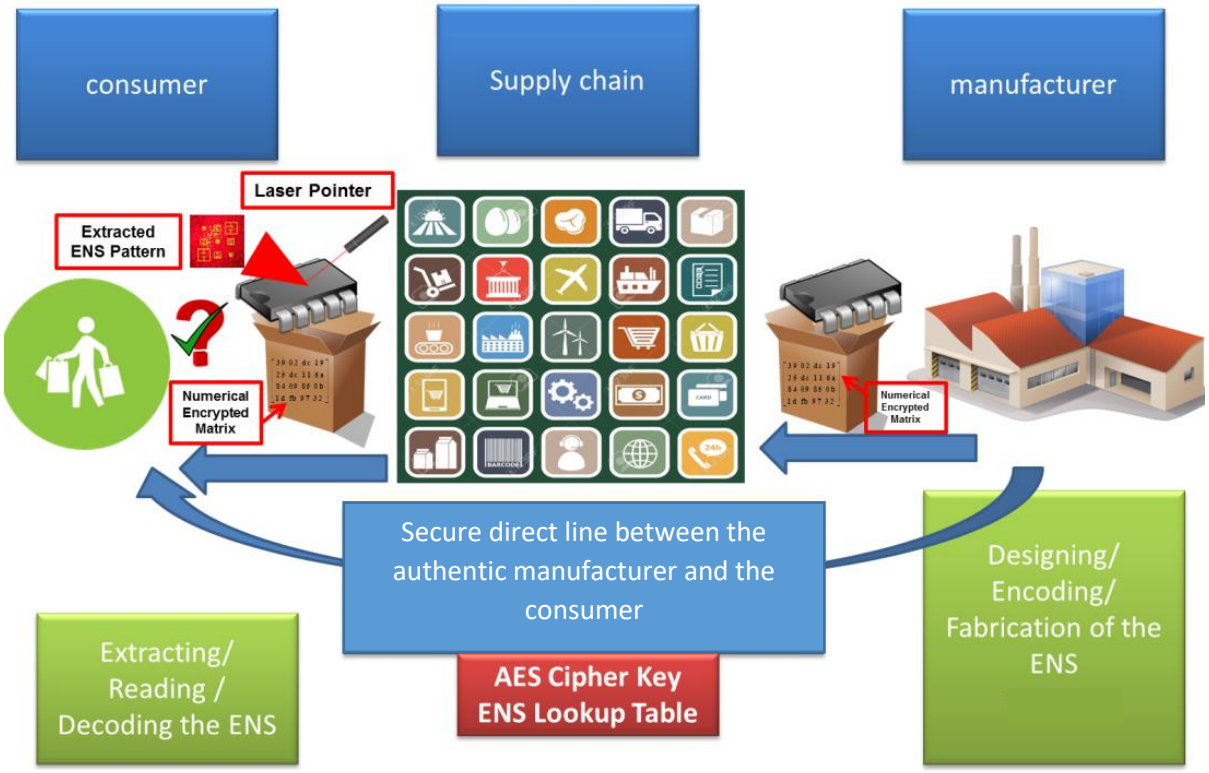


Figure 2.1. The process of identification of authentic components by micro-signatures

Table-2.1 An example of the EMS lookup table

ENS Location / Sizes	5 µm	10µm	15 µm	20 µm
1x1	32	55	3e	ec
1x2	80	a8	90	e5
1x3	79	6c	31	82
1x4	6b	7f	4f	e0
2x1	c8	12	43	06
2x2	5a	8e	2b	f3
...	...	...	...	...
4x4	34	e6	52	4d

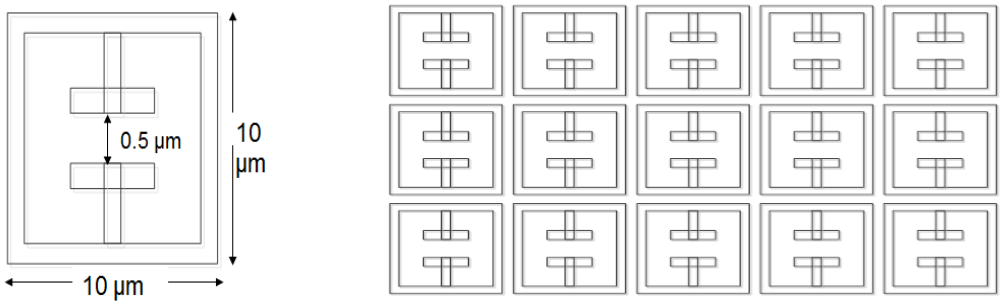


Figure 2.2. (a) A 10 µm EMS. (b) A 3 × 5 matrix of EMS.

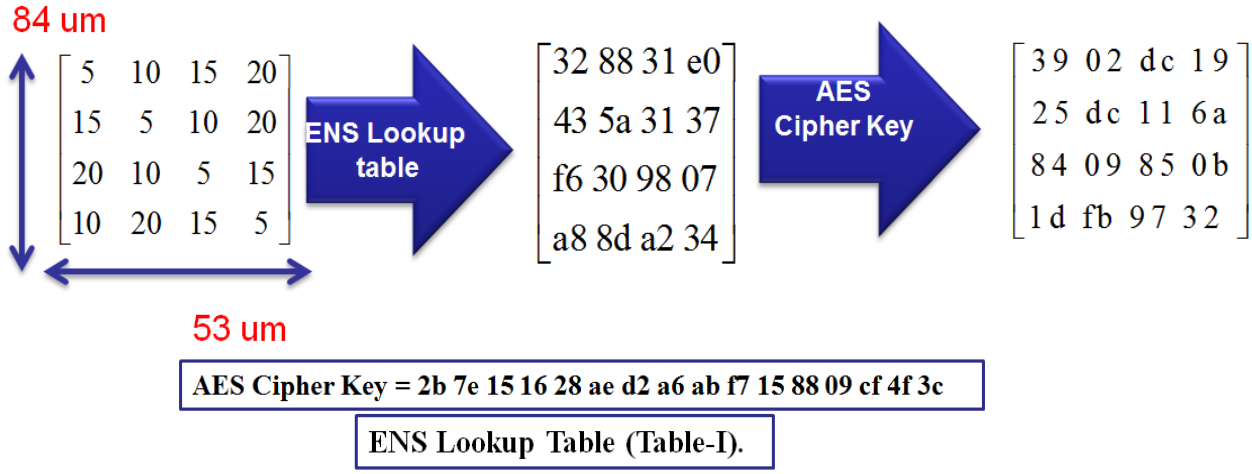


Figure 2.3. Left to right: Converting the EMS pattern to a numerical matrix using the EMS lookup table (Table 2.1), and then encrypting the numerical matrix using AES. The right-hand matrix is ink printed on the product while the left-hand side matrix is converted to a signature-shaped pattern and fabricated via EBL

2.4 **Extraction of the fabricated EMS to match the signature matrix**

The EMS array can be tailored to provide unique signatures for each and every piece of product. This random signature either unique to a family if ICs or an individual IC may be entered into an IC identifier register for future reference and cross-verification. This will allow the detection of over-produced or counterfeit ICs as the counterfeiters will not be able to regenerate the random EMS unique to an individual IC even if they are able to imprint one particular EMS. Once the numerical matrix is converted to the EMS pattern matrix using the AES cipher key and EMS

lookup table, in a reversed process of that of the Figure-2.3, the developed algorithm in this section can match the fabricated pattern with the decrypted matrix to prove the authentication. Without having the knowledge of the EMS pattern, this algorithm cannot adjust the similarity window precisely and thus even if the counterfeiters break into this algorithm, they cannot extract the fabricated EMS without having access to the EMS lookup table and the cipher key.

For the extraction of the fabricated EMS from the laser speckle pattern, the SSIM algorithm is modified as follows [12]. SSIM takes three parameters into account, namely, luminance, contrast, and structure. The algorithm takes a window of $n \times m$ pixels, with the upper left corner located at $x \times y$, and calculates the $SSIM(x, y)$ for that window. Consequently, when two $w \times l$-pixel images are given to the SSIM algorithm, $(w-n+1)\times(l-m+1)$ values are calculated as $SSIM(x, y)$ for each pixel pairs. Eventually, the algorithm gives the average of all the calculated $SSIM(x, y)$ as the SSIM index of the two images.

For detecting EMS in an obtained image from laser reflection from the surface of an IC, SSIM index can be employed. In this application, in $SSIM(x, y)$ formula which is represented by equation (1), luminance, $l(x, y)$ would not be effective in the detection of the EMS since in general it is desired to have a luminance independent detection system. From the formulation point of view, luminance is dependent only on the mean values of the pixel sets which occurs inside the mentioned window; since the mean value would be highly determined by the background noise in case of the images of this work, it`s desired to eliminate the effect of the luminance in the overall calculations. Contrast, $c(x, y)$ is not as important as the structure $s(x, y)$ factor as well. So α which indicates the weight of luminance is set to zero for this work, and β , the weight of contrast

is set much lower than γ the weight of $c(x,y)$. Then, the resulting formula for detecting EMS would be equal to $s(x,y)$ which is indicated by Eq (1).

$$SSIM(x,y) = s(x,y) = \frac{\sigma_{xy} + C}{\sigma_x \sigma_y + C} \tag{1}$$

Where σ_x and σ_y are the standard deviations of the two-pixel sets held inside the mentioned window from the two images, one image is indicated by x and the other one by y. C is a constant and σ_{xy} is the sample cross-correlation of x and y after removing their means [13], [20].

$$\sigma_{xy} = \frac{1}{N-1} \sum_{i=1}^{N} (x_i - \mu_x)(y_i - \mu_y) \tag{2}$$

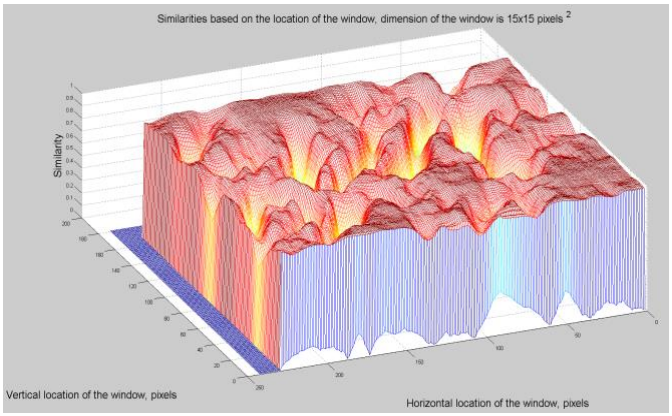
2.5 **Detecting the location of the EMS as the entries of the signature matrix**

The sizes and locations of the fine structural similarities caused by the reflection from EMS are not known within the image of the reflected laser beam from the surface of the IC. To detect the sizes and locations of the reflections of the EMS within the obtained images, the $SSIM(x,y)$ which is indicated in equation (1) is calculated inside the mentioned selection window. In each iteration, the size of the window varies from 2×2 pixels to the size of the image. For calculating the $SSIM(x,y)$ over the entire image, location of the windows moves from $(x,y) = (0,0)$ to $(x,y) = (w-n+1) \times (l-m+1)$. In another word, the $SSIM(x,y)$ is calculated for $(x,y) = (w-n+1),(l-m+1)$ in the windows of the sizes 2×2 to $w \times l$ where $0 \le x \le w-n+1$ and $0 \le y \le l-m+1$. Once the window cover a similar structure inside the two images, say at location $(x,y) = (x_1, y_1)$, a higher calculated $SSIM(x_1, y_1)$ is observed compared with $SSIM(x,y)$ in the

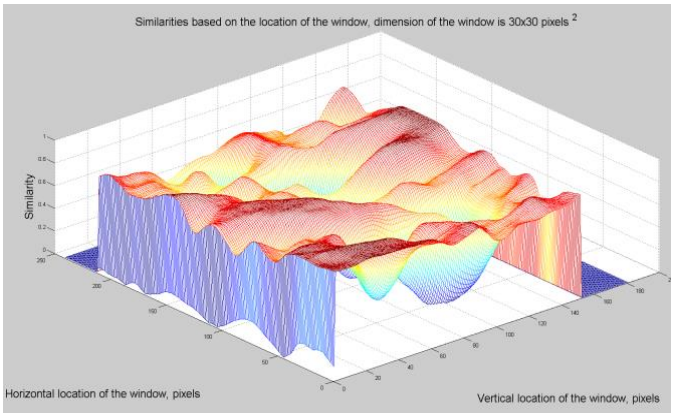
neighborhood of (x_1, y_1). Consequently, once a peak is observed in the results, the location of the corresponding EMS is detected to be $(x_1 + \frac{\mathrm{n}}{2}, y_1 + \frac{m}{2})$.

2.6 **Detection of the size of the EMS**

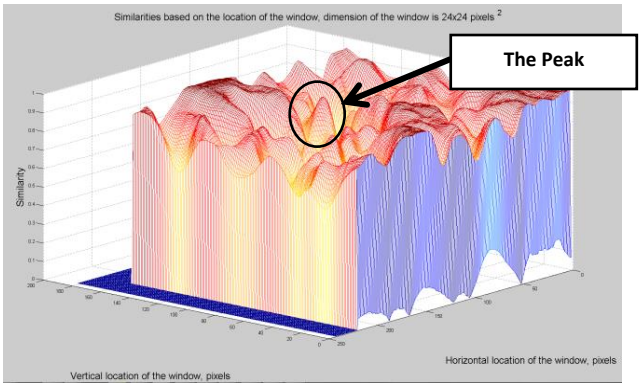
For obtaining the size of the reflected EMS it should be taken into account that as the window reaches the EMS, a peak is going to be shaped in the resulting set of SSIM as it is illustrated in Figure-2.4. Where the size of the window is larger than the EMS reflection, the peak will not be



(a)



(b)



(c)

Figure 2.4. (a) By applying windows of the dimensions less than 24×24 pixels almost no local peak is distinguishable in the mesh grids. (b) By applying windows of the dimensions larger than 24×24 pixels almost all the local peaks are smoothed in the mesh grid. (c) By applying windows of the dimensions 24×24 pixels local peaks are distinguishable in the mesh grids; this refers to the fact that the window fit the fine structures.

sharp, because the window includes the EMS reflection during several iterative movements. Where the window is smaller, sharp peaks will not be observed as the window cannot cover the whole EMS reflection and in another word the EMS occurs inside the window during several iterative movements. Consequently, where a well-shaped peak is observed, the size of the respective window refers to the size of the reflection of the EMS. One can consider the moving window as a square signal which is convolved to another square signal (which is the EMS reflection), thus in practice, half of the width of the peak represents the size of the EMS.

2.7 **Practical results**

A pattern consisting of different sizes of EMS is written on the surface of an IC. This pattern is shown in Figur-2.5. Each element in the matrix refers to the size of each of the EMS, for example the second diagonal element refers to a $5\mu m \times 5\mu m$ EMS which is surrounded by eight other EMS neighbors with sizes $15\mu m \times 15\mu m$, $5\mu m \times 5\mu m$, $10\mu m \times 10\mu m$, $15\mu m \times 15\mu m$, $10\mu m \times 10\mu m$,

$5\mu m \times 5\mu m, 10\mu m \times 10\mu m$ and $20\mu m \times 20\mu m$ clockwise. The IC is setup horizontally and thus the ratio (horizontal/vertical) of dimensions in this work is 0.63.

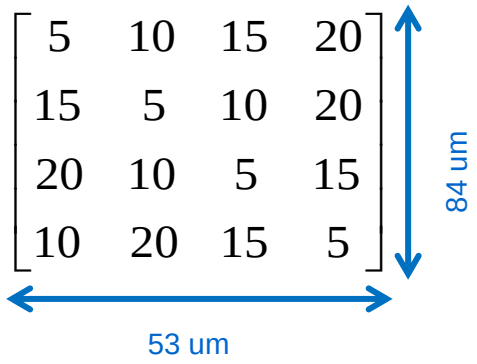


Figure 2.5. The fabricated EMS pattern: the entries of the matrix indicate the sizes of the

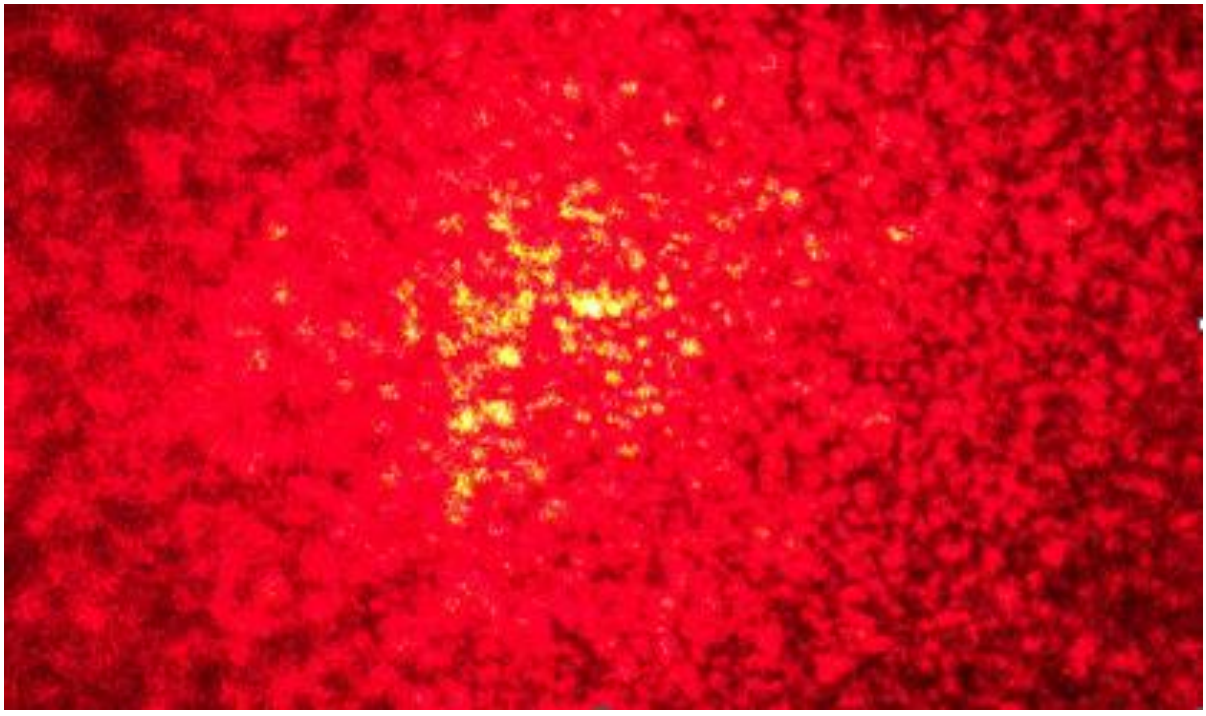


Figure 2.6. The speckle pattern from reflection of the laser beam from the surface of the IC.

The speckle pattern shown in Figure-2.6 is obtained from reflection of the laser beam from the surface of the IC. The aspect ratio of the speckle pattern used in the calculation of this section is 531×841-pixel.

For detecting EMS, the method described in Section 2.4 is applied to the speckle pattern. The speckle pattern is rotated 180 degrees for obtaining the second image to be employed by the algorithm. It is observed that as the size of the comparison window increases, some peaks appear. The peaks become sharper and sharper until the window reaches some certain size then again the peaks become smoother and smoother as the size of the window increases until the new sets of

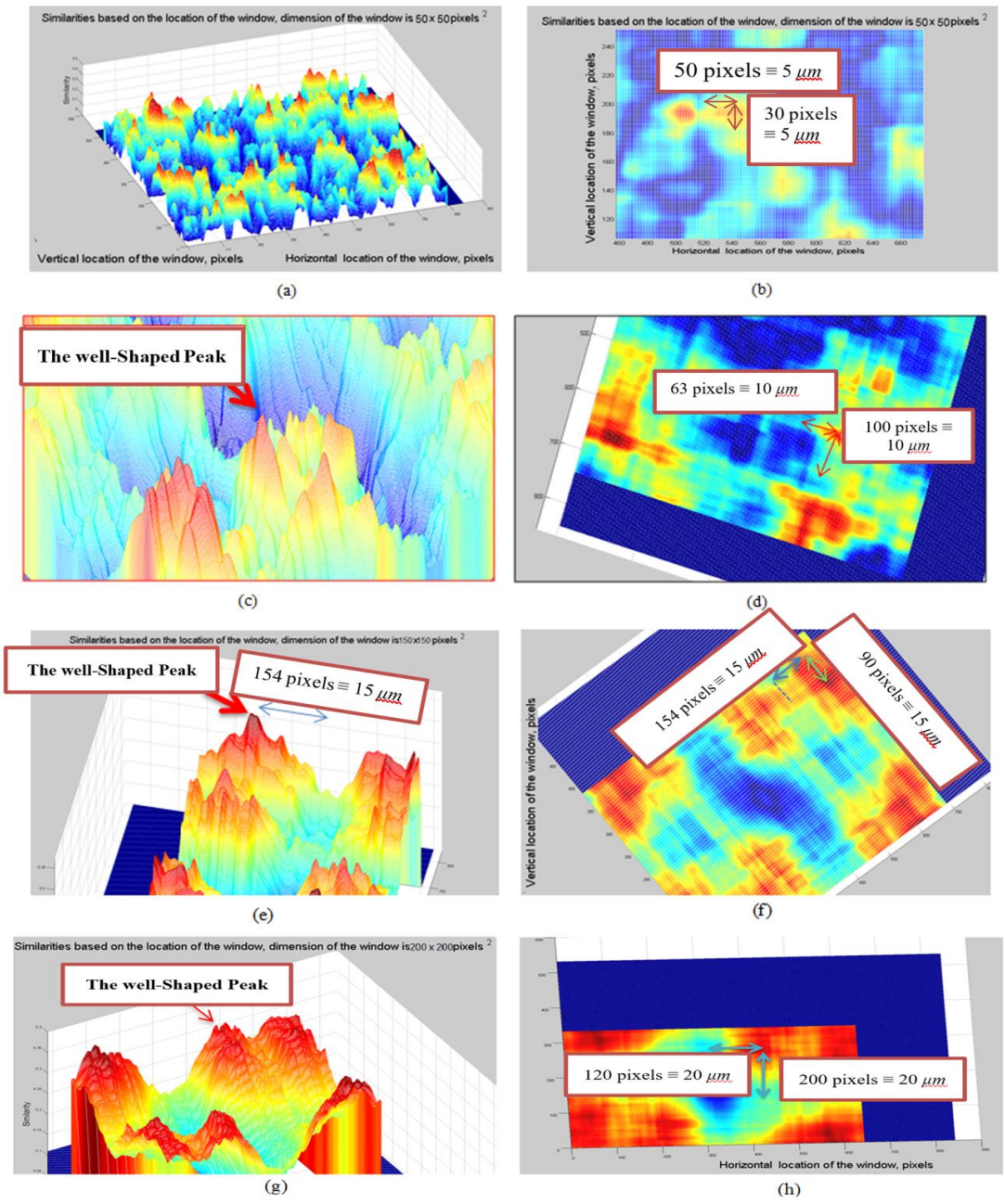


Figure 2.7. (a) The appeared peaks where the size of the window reaches 50×50 pixel. (b) The horizontal location of the peaks for the window 50×50 pixel. (c) The appeared peaks where the size of the window reaches 100×100 pixel. (d) The horizontal location of the peaks for the window 100×100 pixel. (e) The appeared peaks where the size of the window reaches 150×150 pixel. (f) The horizontal location of the peaks for the 150×150 pixel window. (g) The appeared peaks where the size of the window reaches 200×200 pixel. (h) The horizontal location of the peaks for the 200×200 pixel window.

peaks appear in higher sizes. In this work, the first set of peaks appears when the size of the window reaches 50×50 pixels as it is shown in Figure-2.7-(a). According to Section 2.4, it is possible to obtain the size of the EMS by measuring the size of the corresponding peak. Towards this goal, the size of the peak is measured in the mesh grid of Figure-2.7-(a) perpendicular to the *xy* plane as it is shown in Figure-2.7-(b). The horizontal location of the peak is placed at pixel 593 and its hillside continues to 593 as it is indicated by the black arrow on Figure-2.7-(b), thus the length of the horizontal hillside is $(593-563)=30 pixels$. Similarly, the total length of the vertical hillside of this peak is $100 pixels$. By incorporating the aspect ratio, the size of the corresponding EMS is obtaining as follows.

$$\begin{aligned} Vertical &= (100/2\,pixels)\times 84um/(840\,pixels) = 5\ um \\ Horizontal &= (30\ pixels)\times 53um/(531 pixels\times 0.63) = 4.8\ um \end{aligned} \quad (3)$$

As the size of window increases from 50×50 the mentioned set of peaks become smoother and then again a new set of peaks appears at 100×100, as shown in Figure 2.4-(c). By the same procedures and calculations, as presented in Eq. (4), it is revealed that these peaks are corresponding to EMS which size is $10 \mu m$.

$$\begin{aligned} Vertical &= (100\,pixels)\times 84um/(840\,pixels) = 10\ um \\ Horizontal &= (63\ pixels)\times 53um/(531 pixels\times 0.63) = 10\ um \end{aligned} \quad (4)$$

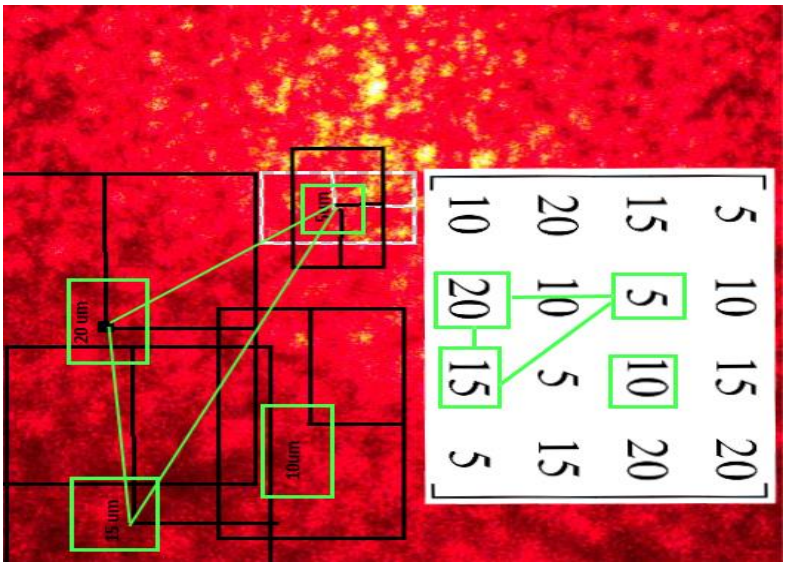


Figure 2.8 Collection of the detected peaks on the same plane (the original image)

As the size of window increases, two other sets of sharp peaks appear where the window is 150×150 and 200×200 pixels. By The same calculations as EQ. (4), it is obtained that these peaks are revealing the $15\mu m$ and $20\mu m$ EMS respectively.

Collecting the locations of all of the detected peaks on the same plane results in Figur-2.8. Figure-2.A in the Appendix-I illustrates the detailed process of collecting the locations of the peaks. It was expected that the only symmetric elements of the matrix of Figure-2.2 are detectable since the 180 degrees' rotation of the main image is employed as the second image for the procedure. As Figure-2.5 indicates, only symmetrical elements of the matrix are revealed by this procedure. It is also observed that the detected locations are inconsistent with the location of the fabricated EMS.

2.8 **Conclusions**

In this chapter, an innovative method for authentication of the electronic components has been represented. Engineered micro-signatures have been used for this purpose. These signatures are invisible to counterfeiters, and thus counterfeiters cannot clone them. In addition, since these

signatures are fabricated on the packages of the components, sanding and blacktopping of the components by counterfeiters destroy them. The micro-signatures are encoded to numerical matrices by developing lookup tables. The numerical matrices are then encrypted using the advanced encryption standard algorithm. An image processing algorithm has been developed to extract the micro-signature from the reflected laser speckle pattern. This algorithm confirms if the correct micro-signature, which matches the decrypted numerical matrices, exists on the object. The numerical matrix needs to be decrypted before giving to the matching algorithm. The cipher key is transferred via a secure direct line between the consumer and the manufacturer. Consequently, counterfeit components which might have been injected to the supply chain are identified at the consumer end.

Appendix-I

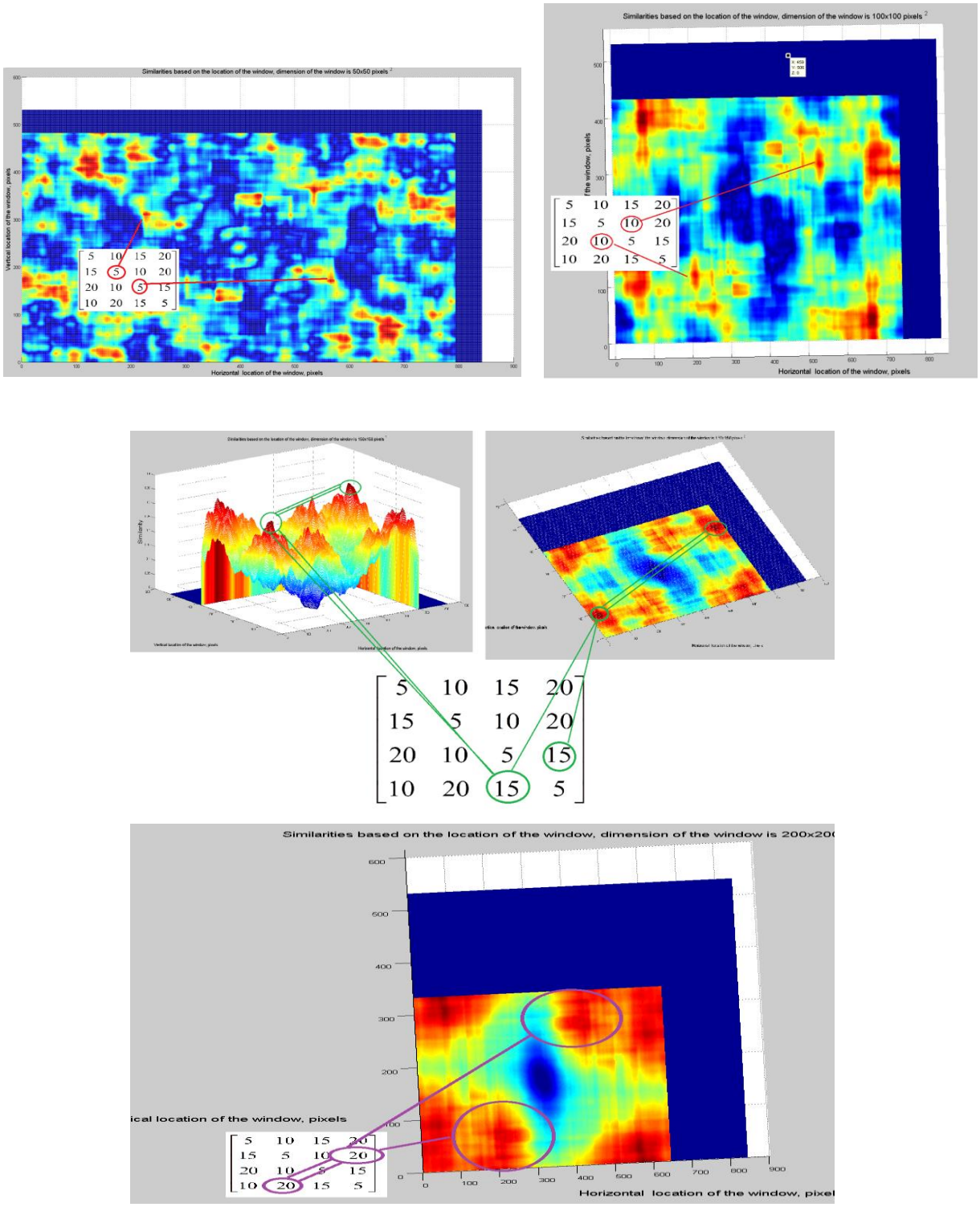


Figure 2. A. Assigning the detected peaks to the fabricated EMS pattern

3

Terahertz Time Domain Spectroscopy for Noninvasive Authentication and Quality Inspection of Packaged Integrated Circuits

3.1 Abstract

In this chapter, the capabilities of terahertz time-domain spectroscopy systems for authentication of packaged integrated circuits are introduced. Generating and detecting the electromagnetic waves in terahertz frequency range has become possible as of only a few decades ago. Capabilities of terahertz beams for traversing through most of the nonconductive materials make them promising tools for noninvasive inspections. Thanks to terahertz time-domain spectroscopy systems, digital recording of the phase of the beams has become possible. Having access to the phase of the beams makes it possible to inspect the hidden layers inside packaged items. Having access to the phase of the beam has also enabled the realization of novel resolution enhancement techniques to generate super resolution terahertz images. Where ionizing imaging needs to be avoided terahertz imaging is introduced as a promising alternative to X-Ray imaging. Moreover, terahertz imaging systems are portable, robust and economical. Since terahertz is a newly commercialized technology, most of its capabilities in different fields of applications are undiscovered. In this chapter, novel techniques for noninvasive quality inspection and authentication of packaged integrated circuits are proposed.

3.2 Introduction

Electromagnetic beams in terahertz (THz) frequency range can traverse through the majority of nonconductive materials. Moreover, THz time-domain spectroscopy (TDS) systems can digitally record the phase of the THz beams. Consequently, noninvasive material spectroscopy, layer

inspection and super resolution transmission imaging of packaged objects have become possible using THz-TDS systems. In this chapter, we report the capabilities of THz-TDS systems for quality inspection and authentication of the packaged integrated circuits (IC). Nowadays, ICs are used in wide varieties of appliances, equipment and machines. An early failure of an IC can lead to the total shout down of a system. These unpredicted failures can happen in critical systems such as power, aerospace and healthcare systems and thus are great threats to economies and human lives. Besides reliability aspects, ICs need to be immune against cyber-attacks and surveillance. Malicious counterfeit ICs have been used as Trojan horses for taking control of critical systems and information. In summary, reliability and authenticity of ICs are two critical factors that are to be determined before using an IC in a system.

In terms of the systematic realization and mass production of EMS, the costs of lead time and money could be optimized. However, because the economy is very competitive, even slight impacts of this process on the final cost cannot be ignored. As a result, we propose this active authentication technique for critical components, such as the components that are used in aerospace and healthcare industries. On the other hand, the proposed passive THz techniques can be used for every type of products without any impact on the production throughput and lead time. Although, THz techniques can detect all types of counterfeit ICs and it can reveal the material characteristics of the packaging of the ICs which is considered same as fingerprints, there are the hypothesis about the possibility of missing very accurate by the reverse engineered components (which may be introduced by foreign governments) by solely using physical inspection techniques.

Several different counterfeit detection approaches based on physical and chemical inspections have been proposed and realized in the industry. X-ray tomography, scanning electron microscopy

(SEM), Energy Dispersive X-ray Spectroscopy (EDS), chemical analysis and using different solvents on the ICs, optical inspections using high-resolution microscopes and analyzing the results using artificial intelligence have been employed for detection of counterfeit ICs. However, THz-TDS systems provide a very promising set of tools which can be used for noninvasive quality inspection and authentication of the packaged ICs. Since THz beams can traverse through nonmetallic materials and due to the fact that THz-TDS systems can record the phase of the THz beams, layer inspection, material analysis and super resolution transmission imaging of the packaged items are possible by THz-TDS systems. These systems are nonionizing, economical and portable. A set of innovative techniques that we developed for quality inspection and authentication of ICs by utilizing THz-TDS systems are reported in this chapter.

This chapter is organized as follows: In Section-3.3 authentication and quality inspection of ICs are realized by utilizing the material analysis capabilities of THz-TDS systems. Section-3.4 presents layer inspection capabilities of THz-TDS systems and their applications in quality inspection and authentication of ICs. In Section-3.5 transmission images of ICs are developed and used for authentication of ICs. In Section-3.6, resolution enhancement techniques for THz-TDS systems have been developed. Thanks to the achieved super-resolution images, accurate measurements of the size of the dies and bond wires are realized, which enables THz-TDS systems to be introduced as promising tools for quality inspection and authentication of ICs. Section-3.7 summarizes and concludes the chapter.

3.3 Material analysis capabilities of THz-TDS for quality inspection and authentication of packaged ICs

3.3.1 Analyzing the transmitted beam

Different materials have unique absorption coefficients and refractive indexes. The packaging materials of the ICs are a composition of different materials and thus it is neither practical nor economical for the counterfeiters to fabricate the exact same blend of materials of authentic ICs in order to obtain certain refractive index and absorption coefficient. Due to the fact that THz beams can traverse through the packaging of the ICs, the absorption coefficient of the packaging materials can be easily measured. In addition, THz-TDS systems record the phase of the beams and thus refractive indexes are measurable by using these systems. Figure 3.1-(a) illustrates two flash memory ICs, one of them is from a set of authentic ICs and another is from a set of detected reversed engineered counterfeit ICs. In Figure 3.1-(b), the traversed THz pulses from two of the authentic flash memory ICs and two of the counterfeit flash memory ICs are illustrated. The traversed pulses from the tested counterfeit ICs show more time delays and attenuations. Thus, the refractive index and the absorption coefficient of the packaging material of the counterfeit ICs are higher than those of the authentic ones. Observing unexpected material characteristic is sufficient to determine that an IC is counterfeit. By using the following equations, the refractive indexes and absorption coefficients of the authentic ICs and counterfeit ICs are calculated and tabulated in Table-3.1.

$$n = \frac{c\Delta t}{T} + 1 \tag{1}$$

$$\alpha = 20(\log_{10}^{e})\mu_a \simeq 8.7\mu_a \tag{2}$$

$$\mu_a = -\frac{1}{T}\ln\frac{A_T}{A_0} \quad (3)$$

Where c is the velocity of light, Δt is the measured time delay and T is the thickness of the IC, α is the attenuation coefficient in dB/cm, μ_a is the amplitude attenuation factor in cm^{-1}, A_0 is the amplitude of the reference traveling THz pulse and A_T is the amplitude of the traversed THz pulse trough the sample.

Since the pulse profile versus time is recorded by THZ-TDS systems, the spectrum of the traversed beam can be computed by using Fast Fourier Transform. The spectra of the authentic and counterfeit ICs are compared in Figure 3.2. The presence of different dips in the spectrums refers to the presence of different elements in the composition of the packaging materials of the counterfeit and authentic ICs. Thorough THz databases are under development and the constituent materials can be analyzed by using these databases [21]–[23].

(a)

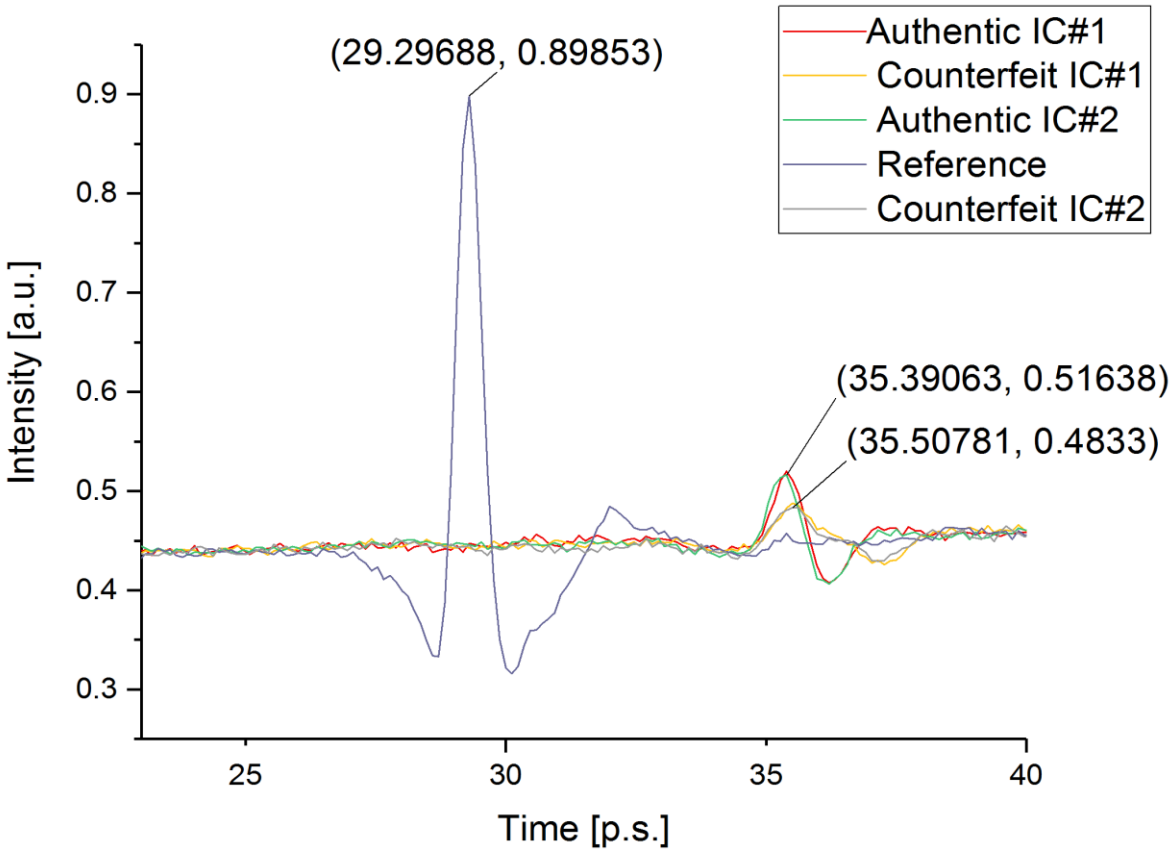


Figure 3.1. (a) left: a counterfeit flash memory IC, right: an authentic Intel flash memory IC (b) reference, and traversed THz pulses from a set of counterfeit and authentic the flash memory ICs

Table 1 Calculated refractive indices and absorption coefficients for three ICs; two authentic and one counterfeit

	Refractive Index	Absorption Coefficient
Authentic ICs	1.7807	0.2062 cm^{-1}
Counterfeit ICs	1.7957	0.2305 cm^{-1}

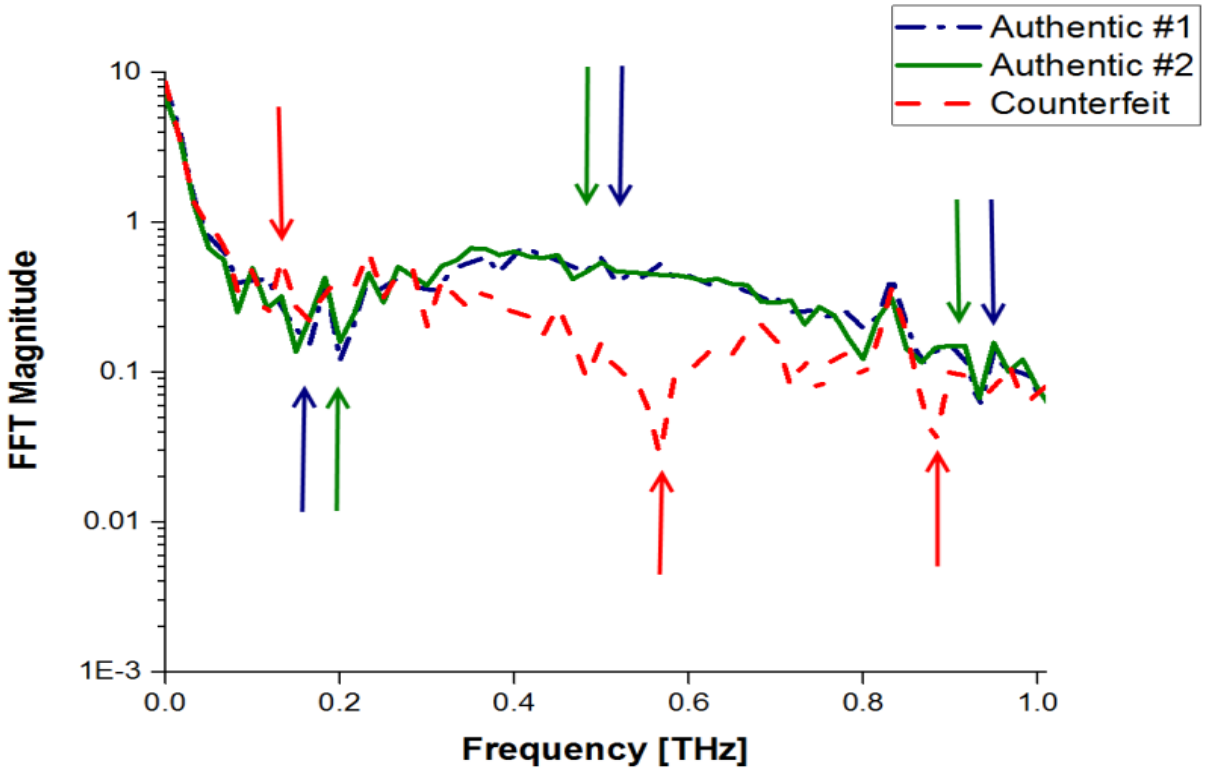


Figure 3.2. Spectrum of the traversed THz pulses from counterfeit and authentic Ics

3.4 **Analyzing the reflected beam**

3.4.1 Material inspection through analyzing of the reflected beam

As different materials have different absorption coefficients and certain dips in the THz frequency range, the reflected THz beams from different materials show different profiles. As a result, the inspection of the surfaces of the ICs is possible by analyzing the reflected THz beams. In addition, THz-TDS systems can record the beam intensity in every 0.1 picoseconds, and in the vacuumed the beam traverses 30 μm every 0.1 picoseconds. As a result, in a THz-TDS system where the beam angle is 45^0, hills and valleys on the surfaces of the ICs as small as 21 μm can be revealed. Figure 3.3-(b) illustrates the time delay from an IC which is thinned as a result of sanding. As it is observed under an optical microscope, The IC is thinned by 181 μm. This distance is equal to 8.5 picoseconds time delay. As indicated in the Figure, the exact same amount of time delay is observed in the beam profile. In Figure 3.3-(c) a contaminated spot is detected by observing a different reflection profile. Under a high-resolution optical microscope, this contaminating is distinguished as flux which can cause corrosion and fire hazard if the IC is overheated.

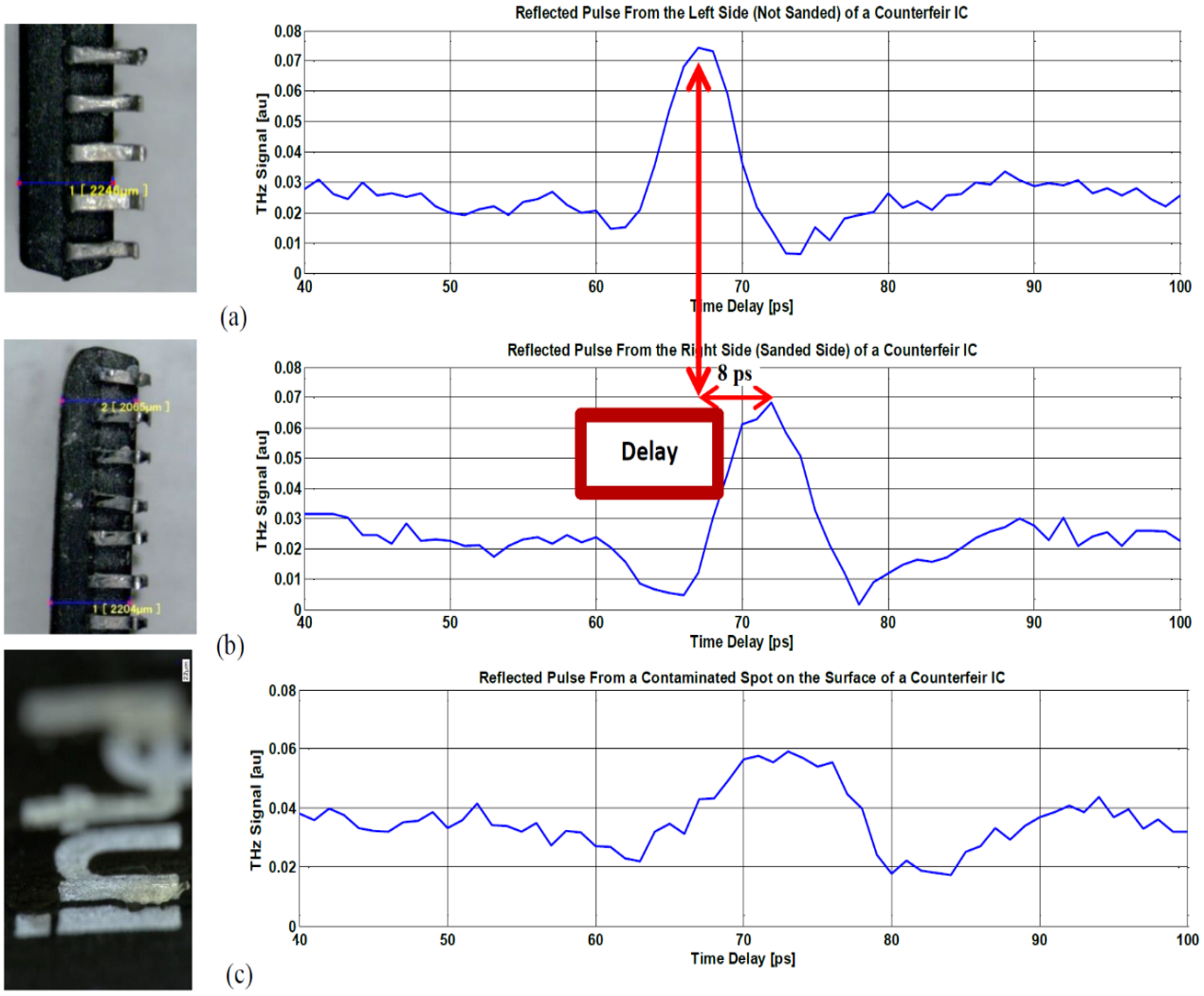


Figure 3.3. (a) Reflected THz pulse from the left side of the surface of a counterfeit sanded recycled IC and vertical image of the IC under an optical microscope (b) Reflected THz pulse from the right side of surface of a counterfeit sanded recycled IC the and vertical image IC under an optical microscope; this side is thinner as a result of being sanded. (c)) Reflected THz pulse from the contaminated spot of a recycled couterfeit IC.

According to the law of reflection, part of the incident beam is reflected upon passing the interfacing of the two mediums with different refraction indexes. Thanks to this property of the rays, and due to the fact that THz-TDS systems record the phase of the beams, we can observe and measure the thickness of the hidden layers in the packaged ICs. In Figure 3.4 reflected THz beam

from an IC is shown and attributed to the top surface, die and bond wires of the IC on lateral X-ray image. The thickness of the layers can be calculated by the following equation [24].

$$d_i = \frac{\Delta t_{i(i+1)}}{2n_i} \tag{4}$$

Where d_i is the thickness of the layer i, $\Delta t_{i(i+1)}$ is the time separations expressed as optical delay in mm and n_i is the refractive index of the layer i. Since in THz-TDS setup the THz beam is not perpendicular to the sample, the reflection angle needs to be taken into account. If the THz pulse reaches the surface of the sample by the angle of θ, the thickness of the first layer can be calculated by the following equation.

$$d_1 = \frac{\Delta t_{12}}{2n_1}\cos\theta \tag{5}$$

Where θ is calculated by utilizing the Snell`s law [5]:

$$\theta = \sin^{-1}\left(\frac{n_1 \sin\theta_1}{n_2}\right) \tag{6}$$

In this experiment $\theta_1 = 45^o$ and thus $\theta = 23^o$. Substituting $\theta = 23^o$ and the refractive index from Table-3.1 into (5) gives the thickness of the layer between the surface and the die as 7.3 mm which is confirmed by the lateral X-ray image.

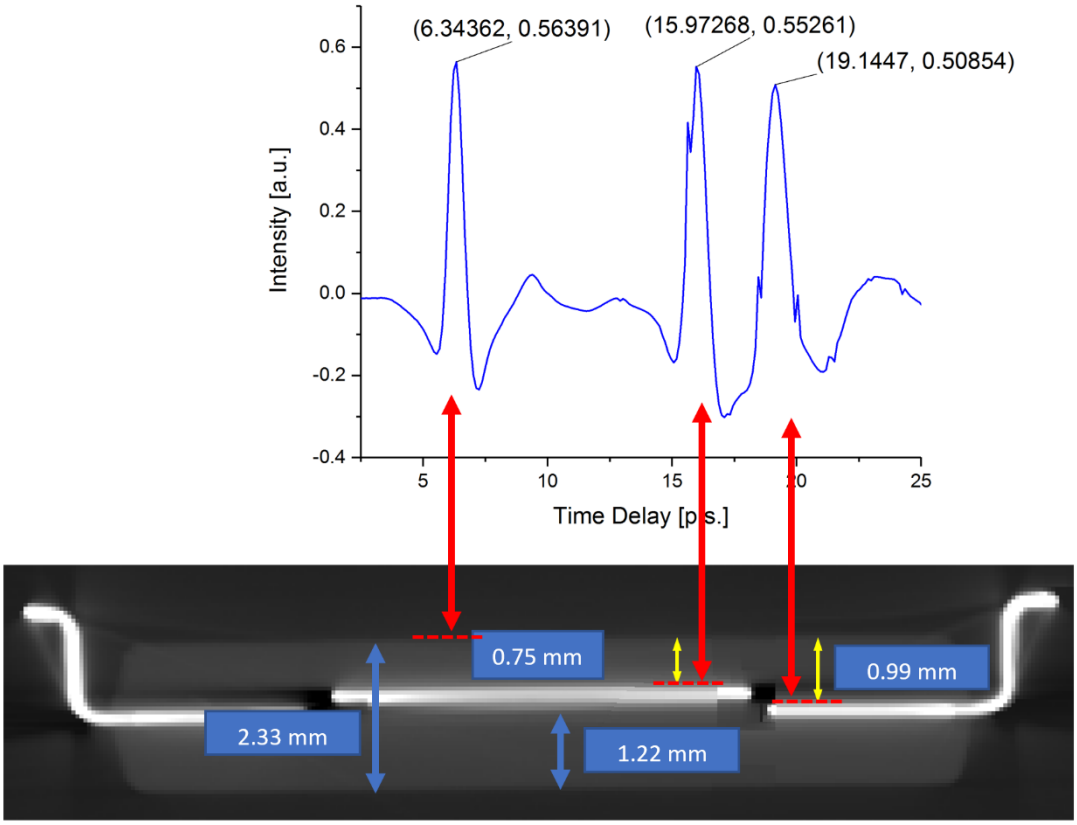
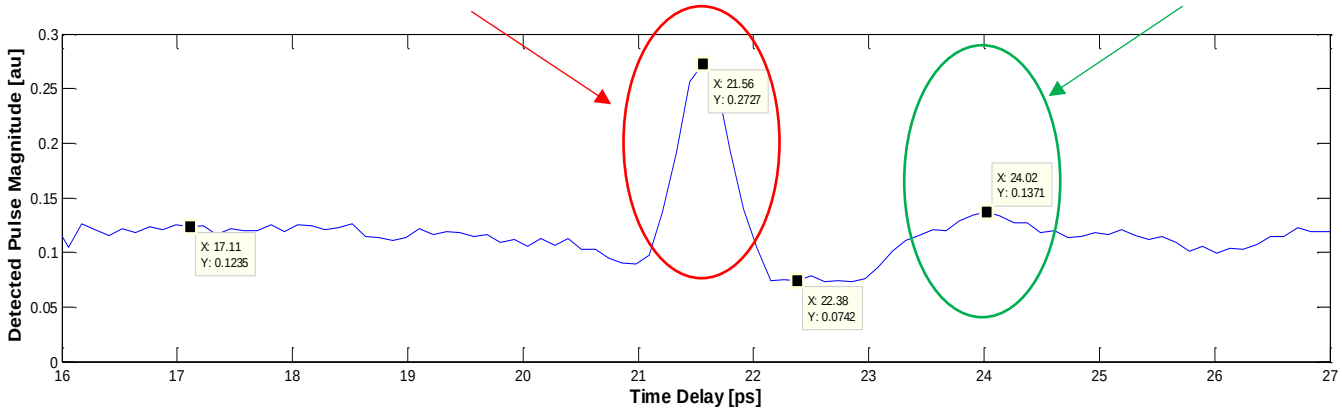


Figure 3.4. Inspection of the layers by THz-TDS systems: correlation of the reflected beams and the layers inside the IC.

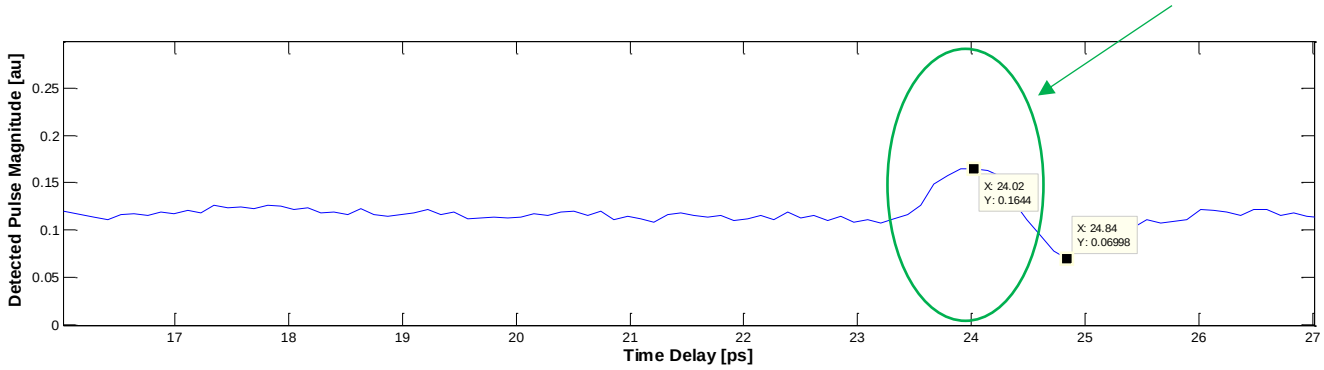
If a contaminating or blacktopping layer is covering the entire surface of the IC, this layer can be detected by comparing the reflected profile from the top and back of the IC. As Figure 3.5 illustrates, a blacktopped IC is discovered in this manner. Also, as shown in Figure 3.6, observing two layers back to back on the top surface reveals the existence of blacktopping and contaminating layers.

Unauthorized recycled ICs with sanded, contaminated and blacktopped surfaces stand for the greatest portion of the injected counterfeit ICs into the supply chain. Besides quality inspection

applications, the techniques which are developed in this section offer a promising role for detection and avoidance of the recycled counterfeit ICs.



(a)



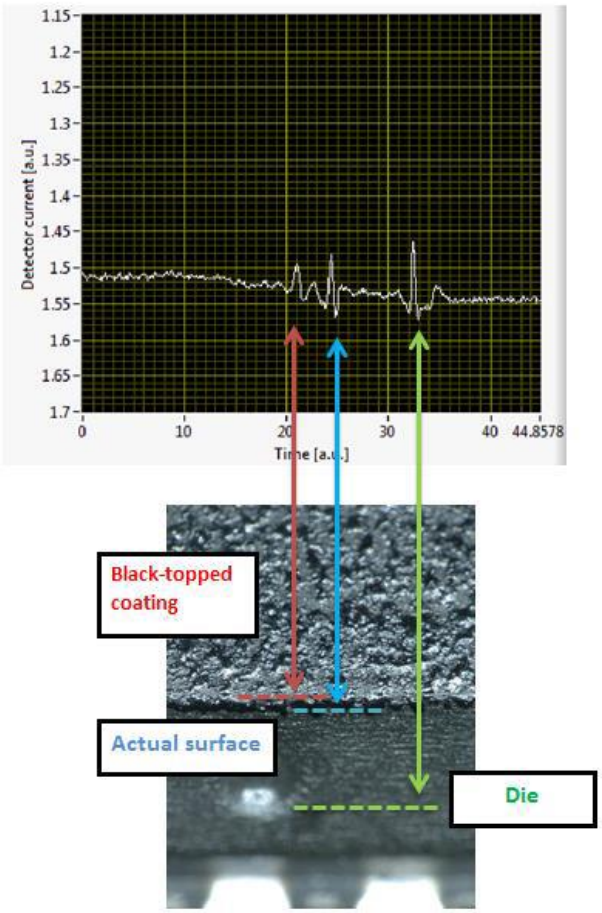
(b)

Figure 3.5. (a) reflected beam profile from top surface of a blacktopped IC, (b) reflected beam profile from back surface of the same IC. The pulse at 24.04 ps is reflected from the actual surface while the pulse at 21.56 is reflected from the blacktopping layer which covers only the top surface.

3.4.2 Developing THz reflection images

By recording the reflected beams in certain step intervals and mapping the reflected beams on a two-dimensional plane, analyzing an entire layer is possible on one graph. For this aim, as shown

(a)



(b)

Figure 3.6. (a) a blacktopped counterfeit IC. (b) detection of the blacktopping layer by analyzing the reflected THz beam. The bottom image is the IC under a high resolution optical microscope from the side.

in Figure 3.7, two stepper motors are utilized to move the object in a two-dimensional plane in certain step intervals and a data accusation software is developed to record the beams in each step. By mapping the reflected beams from the surfaces of the ICs, THz images in Figure 3.8 are developed. Contaminated and sanded spots in these images are revealed. In Figure 3.9, reflected beams from different layers of the IC are mapped in different graphs and THz tomography images of the inside layers of the beams are developed.

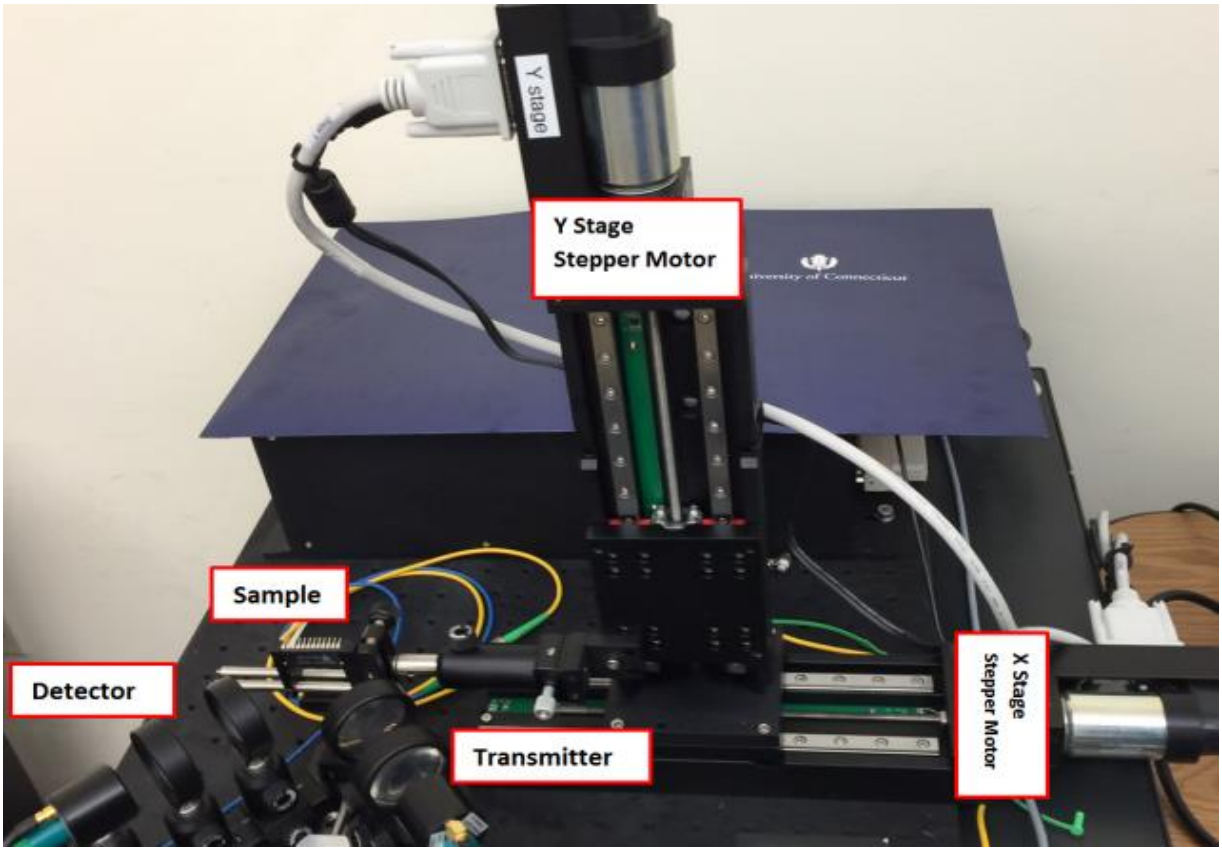
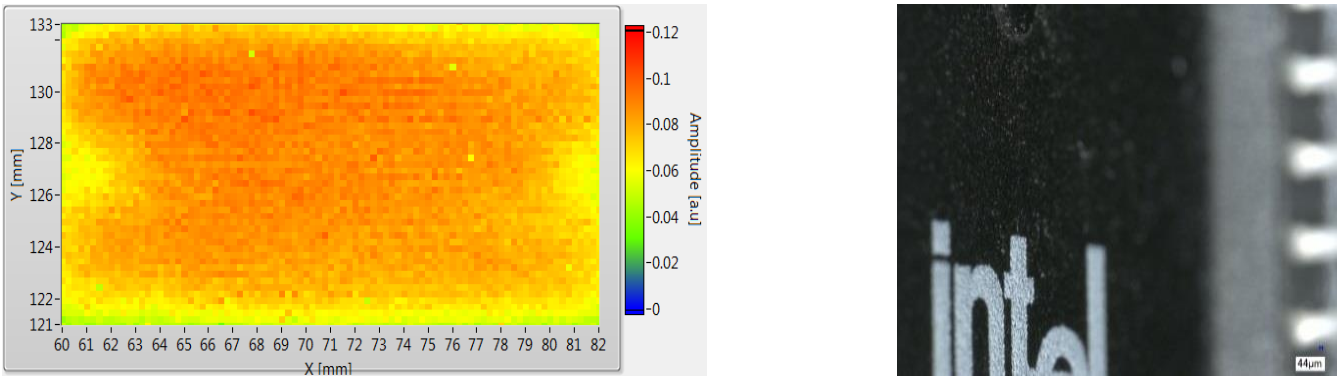
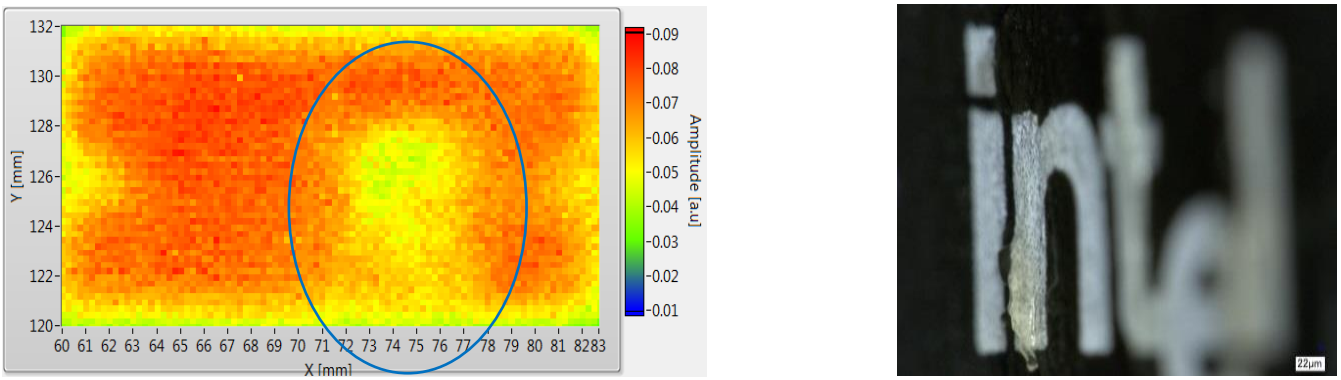


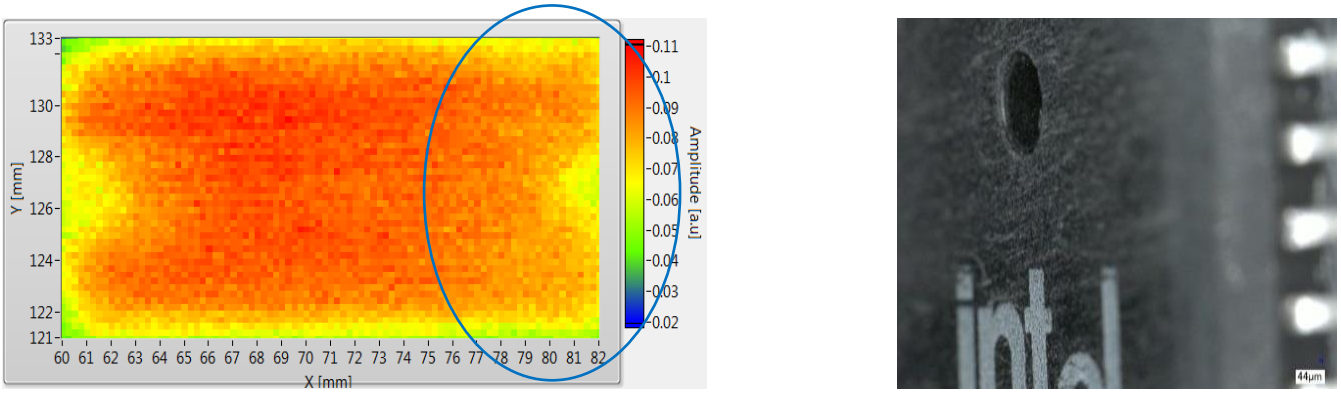
Figure 3.7. The THz-TDS system in reflection mode, the location of the sample and the stepper motors



(a)

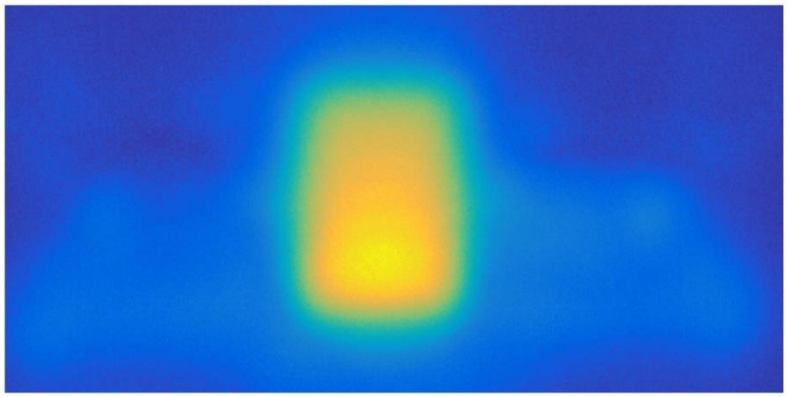


(b)

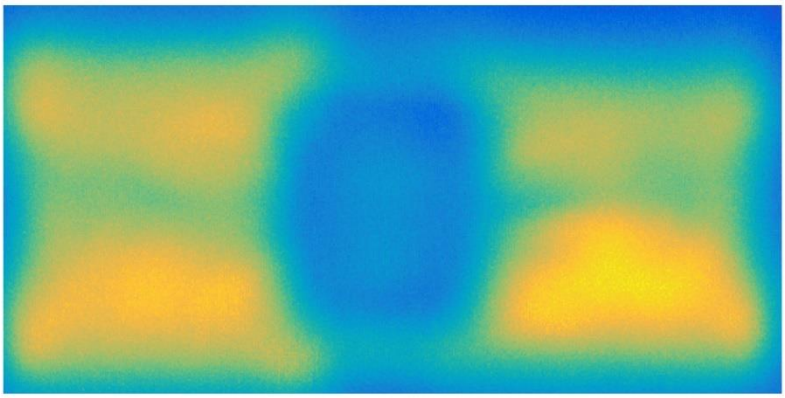


(c)

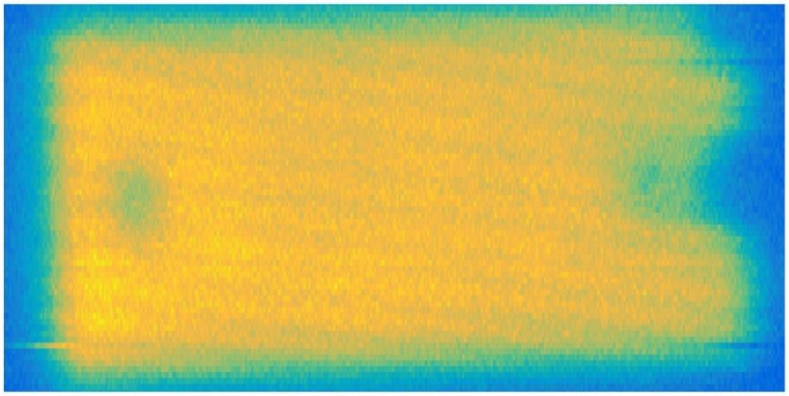
Figure 3.8. THz reflection images on the left and optical images using a high-resolution microscope on the right. (a) Images of an authentic IC. (b) Images of a counterfeit recycled IC: the contaminated spot is obvious in the THz image. This contamination is flux which likely is used by counterfeiters during the recycling process of the IC from its old circuit board. (c) Image of an IC which is sanded on one side. The difference of the reflected THz pulse magnitude is obvious in the THz image.



(a)



(b)



(c)

Figure 3.9. Reflection THz images of the layers of the authentic flash memory IC: (a) die, (b) bond-wires, (c) surface (shadows of the sample holder are observed on the right side).

3.5 Transmission imaging for authentication

In this section, the sample is raster scanned at the focal plane between the transmitter and the receiver. Since the conductive material absorbs the beam, mapping the transmitted beam in a two-dimensional graph provides the map of the conductive parts inside the packaged IC. In Figure 3.10, the transmission THz images of an authentic flash memory IC and its reversed engineered clone. Although, THz transmission imaging is capable of providing us with sufficient input to determine the counterfeit IC, but the resolution of the image is not sufficient to measure the size of the features. In the next section, a resolution enhancement technique is proposed for enabling THz-TDS systems to measure the size of the leads and dies of the packaged ICs.

3.6 Resolution enhancement of THz-TDS systems for enabling them toward quality inspection applications

The two-dimensional raster scan of the object against THz beam is mathematically modeled by a 2D convolution of the PSF and the object function*[17]*.

$$i(x,y,z) = PSF(x,y,z) * o(x,y,z) \tag{7}$$

Where *PSF(x,y,z)* is the point spread function of the THz beam, *i(x,y,z)* is the image of the object and *o(x,y,z)* is the object function at on the corresponding *z-plane*, located at distance *z* from the focal point. Consequently, the object function which is the super resolution representation of the object is obtained as:

$$o(x,y,z) = i(x,y,z) *^{-1} PSF(x,y,z) \tag{8}$$

The PSF is obtained by the following equation [25]:

$$PSF(\rho, z) = \sum_{f} I(0,0,f)\exp(-z\alpha(z,f) - 2\rho^2 / (\frac{1}{\sqrt{2\ln 2}}\frac{k}{NA}\frac{c}{f}\sqrt{1+(\frac{2\ln 2}{c\pi}(\frac{NA}{k})^2 fz)^2})^2) \quad (9)$$

Where *k-factor* depends on the truncation ratio and the level of the irradiance and *NA* is the numerical aperture of the THZ-TDS system, *n* is the refractive index of the packaged object, α is the absorption coefficient, *f* is the frequency of the beam, *c* is the speed of light and ρ is the radial position from the center of the beam:

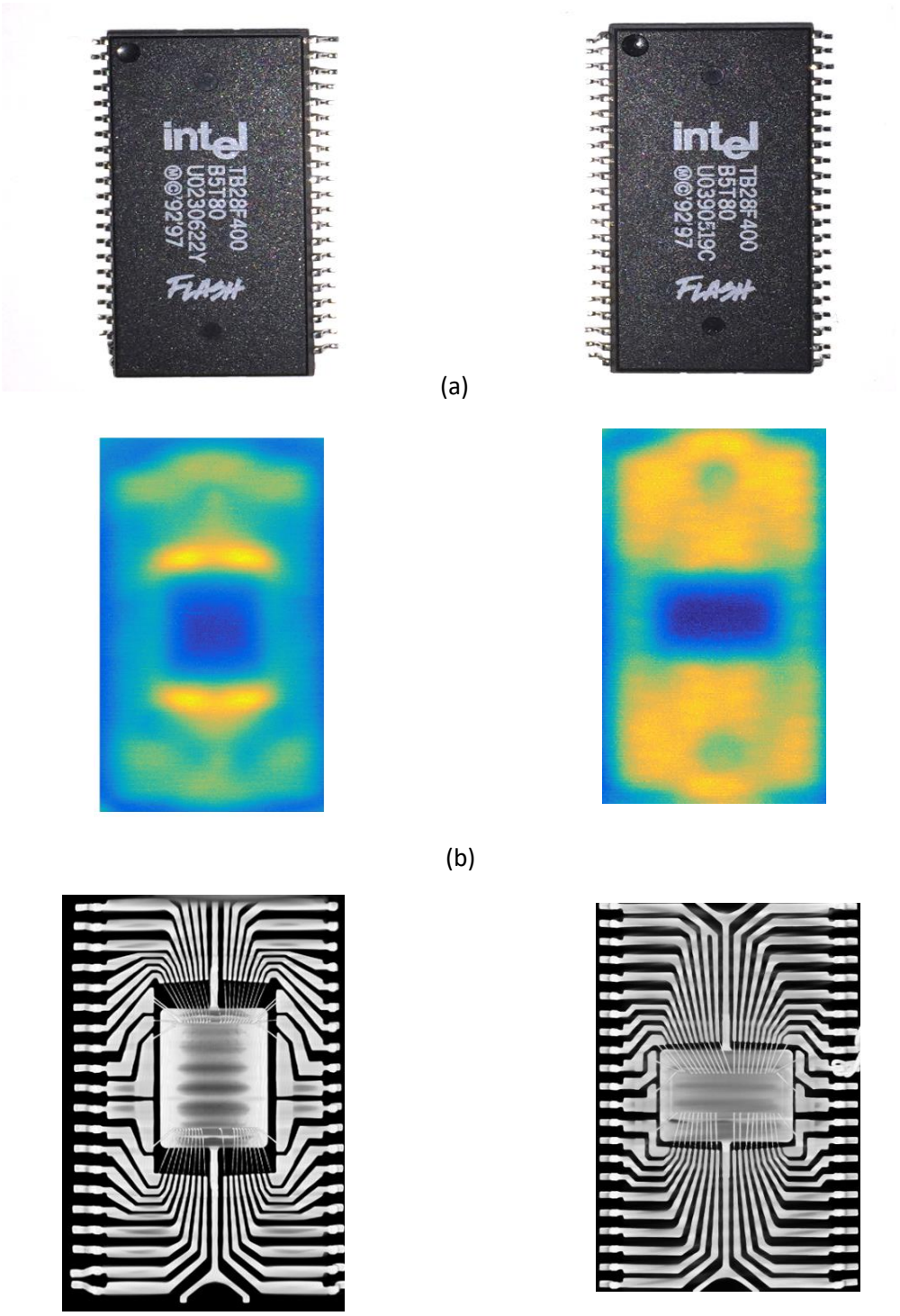


Figure 3.10. (a) Two electronic chips one counterfeit and another authentic. (b) THz transmission images of these ICs; the die geometry of the counterfeit IC (left image) differs from the authentic one (right image). (c) X-ray images of the same ICs are shown to confirm the obtained THz images

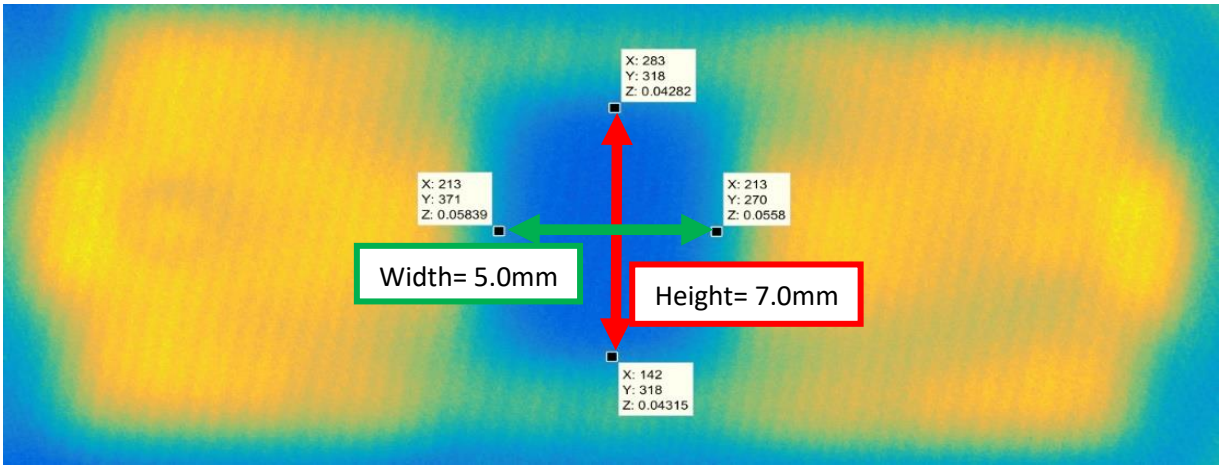
$$\rho^2 = x^2 + y^2 \tag{10}$$

By substituting Eq. (9) into Eq. (8) the super-resolution representations of the THz images are achieved.

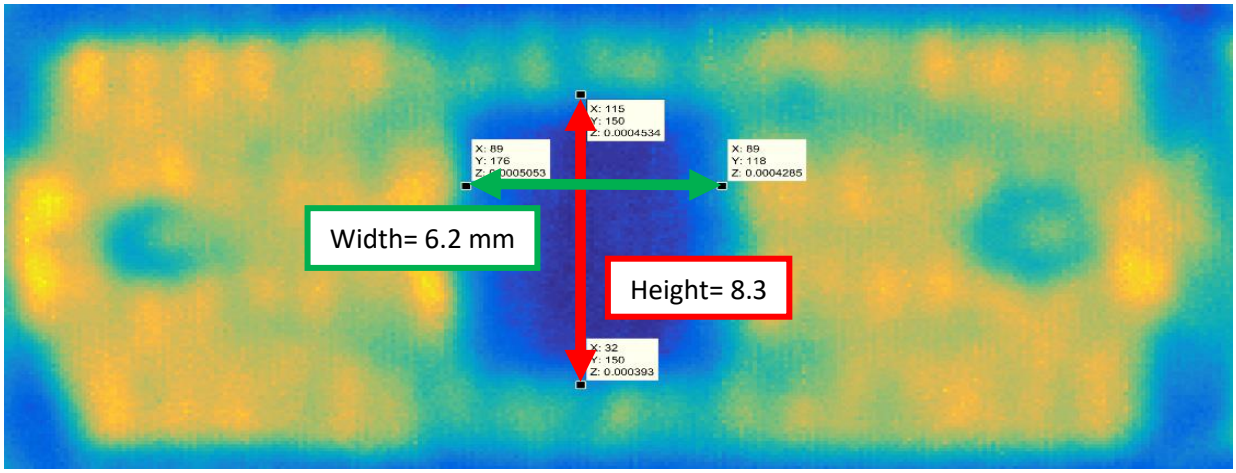
Figure 3.11 illustrates the resulted super-resolution image. In the super-resolution image, not only the dimension of the die is corrected but also traces of the bond wires are revealed.

3.7 **Conclusion**

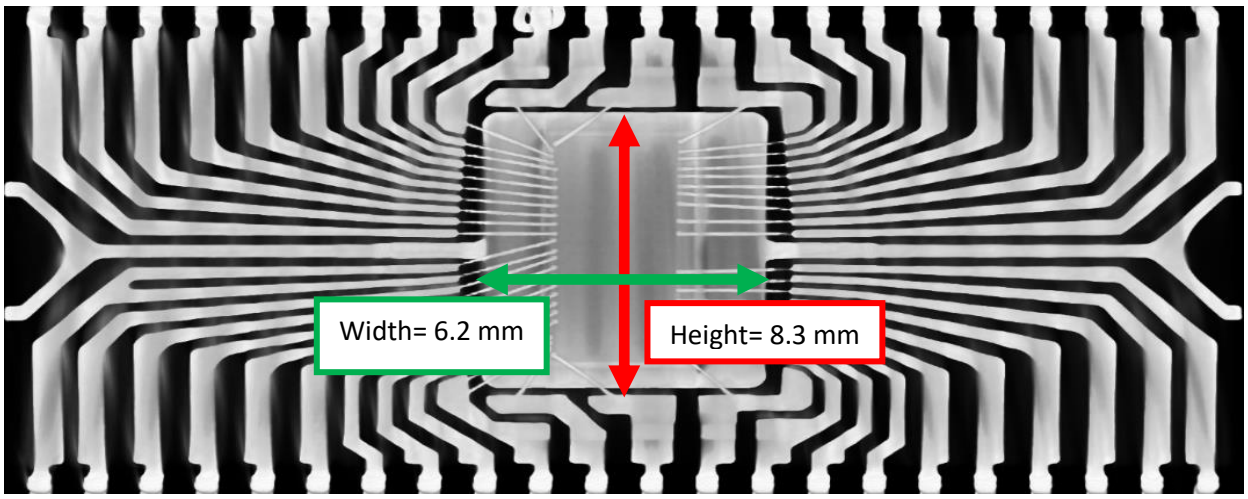
In this work capabilities of THz for quality inspection and authentication of the packaged ICs were discussed. Novel techniques for authentication of the packaged ICs were proposed. Thanks to these techniques, ICs with contaminated and sanded surfaces, misshaped dies and bond wires, blacktopping layers, reversed engineered with layer thickness and constituent material mismatched are detectable. Automated systems can be developed for realization of these techniques in order to inspect large quantities of ICs in quality control and authentication sections.



(a)



(b)



(c)

Figure 3.11. (a) THz image before resolution enhancement, (b) the same image after resolution enhancement, (c) the size of the die is confirmed by X-ray image. [1 pixel=0.1 mm]

References

[1] J. M. Radman and D. D. Phillips, "Novel Approaches for the Detection of Counterfeit Electronic Components," *IN Compliance Magazine*, no. October, 2010.

[2] Frontier Economics Ltd., "Estimating the global economic and social impact of counterfeiting and piracy," 2011.

[3] IHS, "Counterfeit-Part Risk Expected to Rise as Semiconductor Market Shifts into Higher Gear," EL SEGUNDO, Calif., 2012.

[4] K. Ahi and M. Anwar, "A Novel Approach for Enhancement of the Resolution of Terahertz Measurements for Quality Control and Counterfeit Detection," in *Diminishing Manufacturing Sources and Material Shortages (DMSMS)*, 2015.

[5] K. Ahi, N. Asadizanjani, S. Shahbazmohamadi, M. Tehranipoor, and M. Anwar, "Terahertz characterization of electronic components and comparison of terahertz imaging with x-ray imaging techniques," in *Proc. SPIE 9483, Terahertz Physics, Devices, and Systems IX: Advanced Applications in Industry and Defense, 94830K*, 2015, p. 94830K.

[6] K. Ahi, N. Asadizanjani, M. Tehranipoor, and M. Anwar, "Authentication of electronic components by time domain THz Techniques," in *Connecticut Symposium on Microelectronics & Optoelectronics*, 2015.

[7] K. Ahi, N. Asadizanjani, S. Shahbazmohamadi, M. Tehranipoor, and M. Anwar, "THZ Techniques: A Promising Platform for Authentication of Electronic Components," in *CHASE Conference on Trustworthy Systems and Supply Chain Assurance*, 2015.

[8] K. Ahi, A. Rivera, A. Mazady, and M. Anwar, "Embedding Complex Nano-Signatures for Counterfeit Prevention in Electronic Components," in *CHASE Conference on Trustworthy Systems and Supply Chain Assurance*, 2015.

[9] K. Ahi, A. Rivera, A. Mazady, and M. Anwar, "Authentication of electronic components using embedded nano-signatures," in *Connecticut Symposium on Microelectronics & Optoelectronics*, 2015.

[10] K. Ahi, A. Mazady, A. Rivera, M. Tehranipoor, and M. Anwar, "Multi-level Authentication Platform Using Electronic Nano-Signatures," in *2nd International Conference and Exhibition on Lasers, Optics & Photonics*, 2014.

[11] W. Zhou and a C. Bovik, "A universal image quality index," *Signal Process. Lett. IEEE*, vol. 9, no. 3, pp. 81–84, 2002.

[12] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," *IEEE Trans. Image Process.*, vol. 13, no. 4, pp. 600–612, 2004.

[13] Z. Wang and A. C. Bovik, "Mean Squared Error: Love It or Leave It ?," *IEEE Signal Process. Mag.*, vol. 26, no. January, pp. 98–117, 2009.

[14] K. Ahi and M. Anwar, "Modeling of terahertz images based on x-ray images: a novel approach for verification of terahertz images and identification of objects with fine details beyond terahertz

resolution," in *Proc. SPIE 9856, Terahertz Physics, Devices, and Systems X: Advanced Applications in Industry and Defense, 985610*, 2016, p. 985610.

[15] K. Ahi and M. Anwar, "Advanced terahertz techniques for quality control and counterfeit detection," in *Proc. SPIE 9856, Terahertz Physics, Devices, and Systems X: Advanced Applications in Industry and Defense, 98560G*, 2016, p. 98560G.

[16] A. Rivera, A. Mazady, K. Ahi, and M. Anwar, "Growth dependent optical properties of ZnMgO at THz frequencies," in *Proc. SPIE 9483, Terahertz Physics, Devices, and Systems IX: Advanced Applications in Industry and Defense, 94830X*, 2015, vol. 9483, p. 94830X.

[17] K. Ahi and M. Anwar, "Developing terahertz imaging equation and enhancement of the resolution of terahertz images using deconvolution," in *Proc. SPIE 9856, Terahertz Physics, Devices, and Systems X: Advanced Applications in Industry and Defense, 98560N*, 2016, p. 98560N.

[18] K. Ahi, A. Rivera, A. Mazady, and M. Anwar, "Fabrication of robust nano-signatures for identification of authentic electronic components and counterfeit avoidance," *Int. J. High Speed Electron. Syst.*, 2017.

[19] C. Cid, S. Murphy, and M. Robshaw, *Algebraic aspects of the advanced encryption standard*. 2006.

[20] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "The SSIM Index for Image Quality Assessment." [Online]. Available: https://ece.uwaterloo.ca/~z70wang/research/ssim/.

[21] "No TNIST THz Spectral Databaseitle." [Online]. Available: http://webbook.nist.gov/chemistry/thz-ir/.

[22] "THz database." [Online]. Available: http://thzdb.org/.

[23] "RIKEN THz Spectral Database." [Online]. Available: http://www.riken.jp/THzdatabase/.

[24] K. Su, Y.-C. Shen, and J. A. Zeitler, "Terahertz Sensor for Non-Contact Thickness and Quality Measurement of Automobile Paints of Varying Complexity," *IEEE Trans. Terahertz Sci. Technol.*, vol. 4, no. 4, pp. 432–439, Jul. 2014.

[25] K. Ahi, "Scanning Using Super Resolution Terahertz Imaging," 62/402,478, 2016.