https://doi.org/10.2352/ISSN.2470-1173.2017.7.MWSF-338

PCB Surface Fingerprints Based Counterfeit Detection of Electronic Devices

Taswar Iqbal; Kai-Dietrich Wolf, Institute for Security Systems, University of Wuppertal, Velbert Germany

Abstract

Nowadays counterfeit electronic devices are in wide circulation and cause huge financial losses to the industry. In this work, visually imperceptible random patterns on a printed circuit board (PCB) surface resulting from the PCB manufacturing process are investigated as the potential fingerprints for counterfeit detection of electronic devices. For device authentication, surface fingerprints are matched by computing the normalized cross-correlation. The experimental results show that the variations (e.g. small marks of random size, shape, orientation, shape distortions, texture, etc.) encountered in the interlayer connecting vias resulting from the PCB manufacturing process imperfections can be used as surface fingerprints for device authentication. For performance evaluation PCB surfaces with specially designed test patterns produced by industrial grade PCB manufacturing facilities are considered. Appropriate measures are suggested to address the challenges that are not yet addressed in this research work.

Introduction

Nowadays counterfeit products are in wide circulation and cause huge security threats and financial losses to the industry. The spectrum of counterfeit products, previously limited mainly to valuable documents (currency notes, identity verification documents, bank checks etc.), now covers all kind of products (e.g. electronics devices, mechanical parts, medicine, cosmetics). This sets new challenges for the research community involved in the area of security, particularly digital watermarking, whose main target is the intellectual property rights protection. Suitable measures for counterfeit components detection in the supply chain are being taken at governmental as well as industry levels.

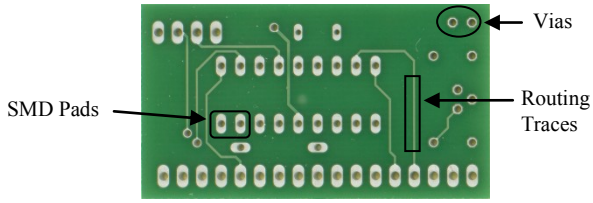
While considering counterfeit detection of electronic devices, the main focus has been on electronic payment systems, mobile phones or other applications involving security or money transactions. However, there are new application areas to be addressed as well. An example could be a building fire alarm or some other device for future modern buildings that has to be authenticated after an accident in order to ensure that the building authorities have been using authentic devices and not low-price counterfeit devices. If the device under test is found authentic, building insurance company would pay for the damage, otherwise the damage claim can be refused. This also applies for electronic components that are being used in the modern automotive industry from globally distributed suppliers.

Nowadays RFIDs are being integrated into PCBs for counterfeit detection and in order to trace and track the product. However, RFIDs have been forged. Recently, in [11] electronic device authentication based on surface data hiding while employing routing traces for signal and power tracks in PCB surface is considered for device authentication. This is the first attempt focusing on the extension of digital watermarking to physical surfaces (e.g. PCBs) of electronic devices. Also, in our unpublished results it is demonstrated that the imperceptible changes resulting from data hiding in PCBs that are enclosed in a plastic cover can be detected while considering industrial X-ray computed tomography (CT) imaging technique. This scenario corresponds to *electronic device authentication* based on PCB counterfeit detection while considering PCB surface data hiding technique and is not addressed in published research. [8] Trojan attacks aim at device failure under certain conditions and at getting some useful information from the device by leakage or by adding hardware components on PCB while modifying the original PCB design during the manufacturing process. In [18] counterfeit detection of PCBs is focused upon while employing the unavoidable tolerances encountered in the routing traces during the PCB manufacturing process. Impedance measurements for different traces are used for the PCB fingerprints computation. This technique is limited to the PCB counterfeit detection and cannot be applied to *a finished electronic device within a plastic cover*. Furthermore, while proposing design for security (DfS), carefully crafted *additional wire traces are inserted* into the original PCB design to ease the impedance measurement for signatures generation. [9] Counterfeit detection of ICs on PCB surfaces focus on infrared (IR) dissection while applying independent component analysis (ICA). Here, again the focus has been put on counterfeit detection of individual components rather than on electronic devices within a packaging cover. However, *thermal fingerprints* of authentic ICs resulting from IR analysis are employed for counterfeit detection of ICs at PCB level. In the present work a new approach is followed that is based on PCB surface fingerprints and *it does not require changes in the PCB design*, unlike PCB surface data hiding [11].

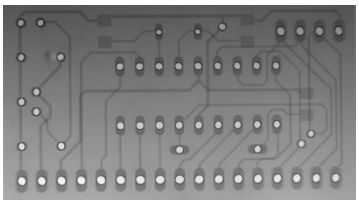
The idea of using surface fingerprints was used in the past for counterfeit detection of security documents. In [2] paper surface has been probed by a laser scanner and the surface roughness is employed to generate digital signatures for counterfeit detection. Even the initial idea was proposed in [16] long time before by employing tolerance on the surface from the manufacturing or inherent surface characteristics (roughness) for authentication purpose. In [19] superposed isolated dots suffering from dot gain effects from the laser printing process are employed to detect counterfeit paper surfaces (e.g. security documents). In [10, Ch. 4] multi-purpose high-capacity datastrip is proposed that allows surface data coding and counterfeit detection. In [15] noise like pattern called copy detection pattern (CDP) based on noise from the print-scan process is used for counterfeit document detection. In [4] random print variations are employed for the counterfeit detection of banknotes. In [7] dust and scratch marks on the scanner surface are employed as fingerprints for scanning device source recognition. Mikkilineni et al. in [14] have investigated the laser print process artifacts for printing device recognition to trace the source of counterfeit documents.

PCB Surface Fingerprints

While considering surface fingerprints for counterfeit detection, a visual surface pattern should have the following characteristics in order to qualify as a fingerprint, 1) randomness, means it is unpredictable, 2) copy-resistant, means cannot be copied from one surface to another surface, and 3) measureable, means can be captured reliably under the same conditions as well as slightly varying conditions. In order to meet the requirements 1-2, variations in PCB visual surface patterns resulting from the imperfections in the PCB manufacturing process are considered. Different visual surface patterns such as interlayer connecting vias, routing and power traces, surface mount devices (SMD) pads on a PCB can be seen in Fig. 1.



a) PCB surface



b) X-ray CT image of PCB surface

Figure 1: *a) Image of a PCB surface (bottom side view) with interlayer connecting vias, routing and power traces, SMD pads.b) X-ray CT image of PCB surface.*

Fingerprints of Interlayer Connecting Vias

Interlayer connecting vias [3] are very small plated holes in PCBs that are used for many purposes but their key function is to connect two different PCB layers, usually top and bottom layers. They are integral part of the PCB layout for all modern electronic devices and cannot be easily seen on a PCB surface. Their quality has a crucial role in the PCB quality. When considering the vias for surface fingerprinting there are contributions from 1) via surface finishing process, 2) variation in drilled hole, 3) distance between edges of the solder mask and via edges, 4) angle of the via hole (only visible in a 3D view).

The PCB surface finishing process results in small lines of varying size, shape and orientation on the via surface. This can be observed in the microscopic image of via shown in Fig. 2. In Fig. 3 marks of random shape/size, resulting from another PCB manufacturing process are shown and the existence of random noise like patterns can be seen. The edge to edge distance in the layout design is constant, that means the via-hole is located as center of the solder mask. However, in the actual manufacturing process, via alignment is a very difficult task and there exists always some misalignment (a well-known challenge in PCB manufacturing process). The different PCB manufacturing techniques are characterized based on this parameter. This can be noticed in Fig. 4 showing the same via on the top and bottom PCB surfaces. These changes in the visual surface pattern are completely unpredictable as well as uncontrollable. Please note that due to small via size and metallic surface, it is expected that via based surface fingerprints should be robust to survive in a fire accident, allowing counterfeit detection of fire alarm. Furthermore, please note that via surface patterns remain unused in an electronic device as no component is to be soldered. Also they are directly visible on PCB surface and these points make them an attractive choice for the PCB surface fingerprints.

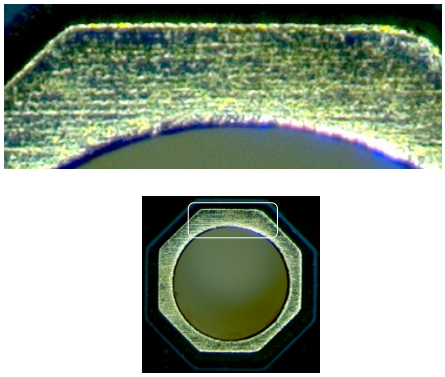


Figure 2: *Interlayer connecting via and its magnified view (on top) of microscopic image are shown in which presence of texture can be noticed.*

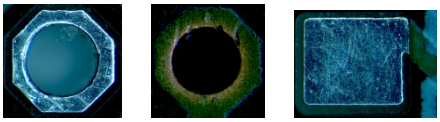


Figure 3: *Interlayer connecting vias and SMD pad from other manufacturing process. Magnified images are given in appendix A.*

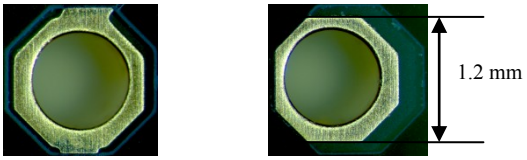


Figure 4: *Top and bottom view of the same misaligned via from the test PCB surface ordered using industry PCB manufacturing facilities.*

In the appendix some more images of the real PCB are shown to further highlight the random patterns on the PCB surface. By looking at the patterns in the appendix it can be easily seen that those surface patterns can be employed as fingerprints for device authentication.

PCB Via Surface Fingerprints Recognition

The next question to be answered is how to employ via surface patterns for PCB surface authentication. In general, this process is same as for any other surface (e.g. paper) fingerprints recognition system. However, here each step with its individual

impact on performance is to be investigated from beginning as in the present scenario a novel application is to be investigated that is completely different from the existing applications. An abstract view of a fingerprints based counterfeit detection process is given in Fig. 5. It starts with digitization of the PCB surface using an appropriate imaging technique. The preprocessing step deals with noise encountered in the analog-to-digital conversion process. The segmentation step deals with detection of the target regions (e.g. via patterns) in the PCB image. The PCB surface fingerprints step is the key step that computes the similarity between the test and the reference fingerprints assigned to a particular device. Finally, in the counterfeit detection step, a given test image is recognized as a counterfeit or authentic. In the following subsections each of these steps will be described in more detail.

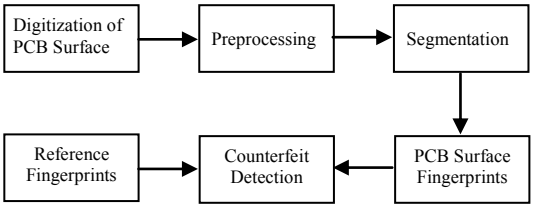


Figure 5: *Fingerprint based PCB surface authentication process.*

is not part of the original PCB layout design as it might *result in violation of functional transparency*.

Most importantly, when considering visual surface patterns on the PCB surface for counterfeit detection, segmentation problem becomes more complicated due to the unpredictable nature of components, traces, and components of varying size. This challenge has been encountered in [11] while investigating PCB surface for data hiding. In conventional image analysis based PCB quality control this challenge is not encountered as the target patterns are compared with an high quality reference image (gold standard) in a non-blind mode for defect detection. Finally, when there are more than one visual surface patterns (e.g. interlayer connecting vias) on the PCB surface that are employed in surface authentication process, then each one is to be processed in a certain order (as shown in Fig.6) for synchronization recovery.

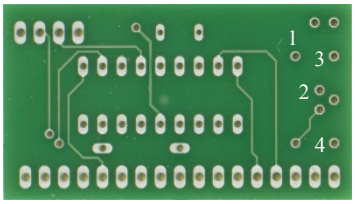


Figure 6: *Processing order of selected vias on PCB surface for counterfeit detection while considering only four vias.*

Digitization of PCB Surface

This step has crucial impact on the performance of the fingerprints recognition system. Here, the fundamental requirement is that it should be able to capture minor surface details that are necessary for surface fingerprints. That means, the target is to capture small variations (e.g. marks, texture, size, shape distortion, etc.) on PCB visual surface patterns (SMD pads, vias, routing traces, etc.). This goal can be achieved by imaging the surface with high resolution and good quality optics. The resolution must be at least two times higher than the target feature size. The microscopic images of visual surface patterns shown in Fig. 2-3 can fulfill this requirement. While considering counterfeit detection of electronic devices within a plastic cover then X-ray computed tomography (CT) based digitization technique has a key role. The modern industrial CT systems allow capture minor details at one micron resolution. A CT image of a PCB surface is shown in Fig.1b.

Preprocessing

The preprocessing step tackles any geometrical distortions encountered in image capturing process due to surface misalignment. Also, noise encountered in captured image from surface illumination process is tackled in preprocessing step. Ideally, the target surface area should be evenly illuminated for good quality visual surface patterns. Conventionally, averaging of many images and median filtering are employed to improve the image quality against noise.

Segmentation

Segmentation is a crucial step in the automatic counterfeit detection process. In [2] using laser scanner based paper surface, fingerprints registration has been considered a key challenge. In [5, 6, 15, 19] special registration marks are added around the target visual patterns to assist in the detection process (or synchronization recovery). Please note that in PCBs it is not suitable to add a new pattern (e.g. registration marks for synchronization recovery) that

In this work *regularity in the visual surface patterns* (as shown in Fig 3.) such as hexagonal, or circular shape of the vias is to be utilized by template matching technique for automatic detection of the target regions (e.g. via surface patterns). A template also known as region of interest (ROI) of via surface is to be stored in advance along with the fingerprints in the database. Here, a low quality grayscale image with maximum compression can be considered as a template to reduce data size. Template based segmentation technique is also robust against occlusion and varying lighting conditions.

PCB Surface Fingerprints

While considering PCB via surface patterns (see Fig. 2-4) for PCB surface fingerprints representation, a set of extracted features such as center of gravity (CG) of different vias, subpixel distance between CG of different vias, distance from CG to inner edges of the vias, distance from CG to outer edges of the vias [19]. Then, using feature vectors of test and reference surfaces, Hamming distance (HD), or Mohalanobis distance can be computed for device classification as authentic or counterfeit. However, in present research we have decided to investigate a technique that is independent of feature extraction while keeping feature extraction based technique for performance comparison in the future.

In order to differentiate between the authentic and the counterfeit surface image patterns, in the existing work [1, 7, 15] normalized cross-correlation (NCC) has been used as a similarity measure. Please note that in [12] this technique has been applied for human fingerprints recognition and found that it results in superior performance as compared with the Minutiae method. NCC based technique allows matching complex patterns that are difficult to characterize with a feature extraction based approach. It is also observed in our work that the surface fingerprints resulting from PCB manufacturing process imperfections vary from process to process, so NCC choice seems more appropriate. Also, NCC based technique is robust against varying lighting conditions. On

the other hand the drawback is that the template/fingerprints size is large as compared with the feature extraction based fingerprints representation. The large fingerprints size is computationally more expensive.

Formally, NCC based technique works as follows: It starts by selecting a template also called region of interest (ROI) that represents the surface fingerprints. Then, a test image (or test surface fingerprints image) is matched with the template by computing two dimensional NCC denoted by r at point (u,v) using [13],

$$r(u,v) = \frac{\sum_{x,y}\left[f(x,y) - \bar{f}_{u,v}\right]\cdot}{\sqrt{\sum_{x,y}\left[f(x,y) - \bar{f}_{u,v}\right]^2}\cdot}$$

$$\frac{\left[t(x-u,y-v) - \bar{t}\right]}{\sum_{x,y}\left[t(x-u,y-v) - \bar{t}\right]^2}. \qquad (1)$$

where, f and t represent the test and template images of the fingerprints, respectively. $\bar{t}$ is the mean of the template image. The test image f has a size larger than template image. $\bar{f}u,v$ is the mean of $f(x,y)$ in the region under the template. The template image is shifted pixel by pixel over the whole test image and at each position value of r is computed. Finally, the highest value of r denoted by $r_{\max}$ is taken and test surface image is considered authentic as follow,

$$\begin{aligned} &If \quad r_{\max} \geq \lambda \quad Authentic \\ &elseif \quad r_{\max} < \lambda \quad Counterfeit \end{aligned} \qquad (2)$$

where λ is the threshold level to be found experimentally. To ensure that the decision made is correct, the ID of the template resulting in $r_{\max}$ should match with that of test device or the surface being interrogated. There are N surface fingerprint templates for authentic surfaces that are registered in advance in database. In one-to-one verification mode template, threshold level, and device ID can be stored in an authentic device or in a database.

Here, scalability can be improved by increasing the number of vias (e.g. 7-9) (as shown in Fig.6) for counterfeit detection. In this case a vector of via surface patterns for each authentic electronic device will be stored in the database. In segmentation step all those vias will be detected by applying the template matching technique repeatedly in a predetermined order. Also, instead of using eq.(2), the decision will be made on majority basis. This would also result in improved performance in terms of error rate while considering robustness against noise.

While considering template size, initially whole region of the via surface pattern is to be considered as this would result in maximum entropy by taking into account all minor details resulting from PCB manufacturing process for a given via surface. Please note that in practical application scenario all (or many) vias present on a given PCB surface can be analyzed and those resulting in the best performance (i.e. highest NCC value) for different imaging systems can be employed for authenticity verification. In this case position of via surface on a given PCB will also be stored in a database.

Results

In order to evaluate performance of the proposed technique a PCB surface (see Fig.1) of a real device is investigated. In another scenario a custom designed PCB surface (shown in Fig.7) with only target patterns consisting of interlayer connecting vias is considered. For the image capturing process, a digital microscope (Stereo Discovery8.0), equipped with a digital camera (model MRf Rev.3) and AxioVision software is used. Suitable measures for image enhancement are not required as such noise is not encountered in our experimental setup. In Fig. 8 the NCC plots are shown for an authentic (top) and a counterfeit (bottom) surface considering an interlayer connecting via. In this work *template images are selected manually* and one such image is shown Fig. 9. Considering the PCB surface shown in Fig.1 for ten real PCB test surfaces taking same via on all surfaces, this scenario has been successfully demonstrated for counterfeit detection. Also, the experiment is repeated for different vias on the PCB surface to account variability in the PCB test surface. However, due to the small number of test surfaces the results are not reported here.

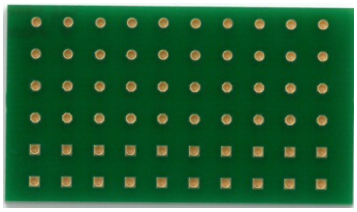


Figure 7: *Custom designed Test PCB with only interlayer connecting vias.*

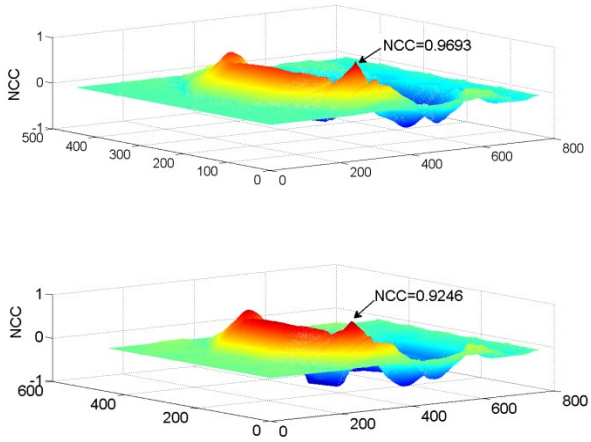


Figure 8: *Normalized cross-correlation (NCC) of matched surface images (top), two different surfaces (bottom).*

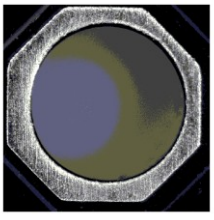


Figure 9: *Via surface pattern used as the template.*

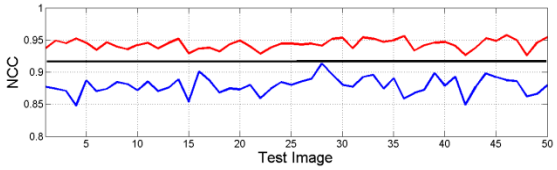


Figure 10: *Normalized cross-correlation (NCC) for authentic (red curve, top), counterfeit (blue curve, down) surfaces and threshold level (constant line).*

In Fig.10 the experimental results are shown while considering 60 PCB test surfaces designed with only interlayer via surface patterns. There are 60 via patterns (see Fig.7) on each test surface. The templates of the 50 out of 60 vias are stored in advance. Then the images of these via patterns are taken and used as test image for via recognition. As it can be seen in Fig.10, test images can be differentiated correctly. Here, counterfeit means a surface that has not been registered in the database. Please note that the highest values for the counterfeit surface among 50 registered templates against the authentic surfaces are shown in Fig.10. However, when a given test via surface is checked against a randomly selected counterfeit surface, normally NCC value is much less. In Fig.11 the results are shown while considering 500 via surface images. Here, five images are taken for each via surface on five different days while considering total 100 via surfaces. Out of these 500 images 100 images are used as the templates and the remaining 400 images are used as test images. About 30-40 errors are found while considering threshold levels in the range 0.935-0.945. This results in an error rate of ~10%, including both the false positive and true negative rates.

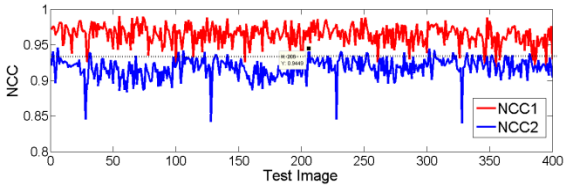


Figure 11: *Normalized cross-correlation for 400 authentic (NCC1, red curve, top) and 400 counterfeit surfaces (NCC2, blue curve, bottom).*

In Fig.12 the results are shown while considering 360 via patterns. Here, 360 via surface patterns from 60 PCB surfaces (6 vias from each PCB surface) are considered. Images are taken in different sessions on different daytimes and days. The templates (same used in Fig.10) and the test via surfaces have been different. The vias have similar size, shape and manufacturing conditions. As it can be seen the behavior while considering only counterfeit surfaces (i.e. always different test and template images) is same as in Fig.11. While considering a threshold level at 0.935 some false positives will be encountered.

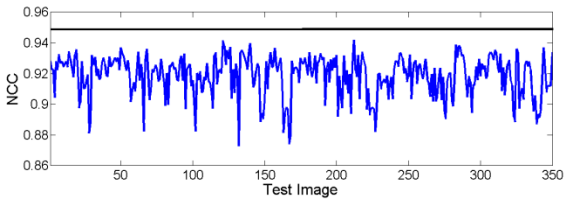


Figure 12: *Normalized cross-correlation (NCC) for 360 test images.*

In this research work the performance of individual via surfaces while considering vias from many different PCBs is investigated and it is found that the via surface patterns can successfully be employed for counterfeit detection of electronic devices. Furthermore, in practical applications while considering many vias on an entire PCB surface (see Fig. 6) it would certainly result in superior performance in terms of scalability as compared with single via based counterfeit detection. Considering more vias should not pose serious challenge. The impact of surface rotation/re-rotation is also investigated initially for small number of PCB test surfaces and no difference in performance is found. Also, template and test images size is reduced by applying principal component analysis (PCA) for small number of test surfaces and performance is not degraded. However, for down sampling of test and reference images the performance is degraded.

There have been produced 100 test PCB surfaces shown in Fig. 1 but the results at this stage are not ready. Also, in order to evaluate the performance experimentally 80 PCB surfaces (see Fig.7) consisting of only via surface patterns are produced, offering 9600 via patterns considering both top and bottom sides of PCBs. This is task of the next research phase. As a performance measure, confusion matrix and ROC curve [17] will be considered.

Conclusions

In this work an important novel area, dealing with counterfeit detection of electronic devices based on PCB surface fingerprints, is focused upon. For counterfeit detection, the PCB via surface imperfections resulting from the PCB manufacturing process, are investigated as the potential PCB surface fingerprints. The experimental results show that the PCBs can be authenticated based on the PCB via surface fingerprints while employing normalized cross-correlation as a similarity measure. For performance evaluation, real-PCB surfaces are considered with no assembled components. To capture the fine-details on via surface digital micro-scope is considered for image capturing purpose. The results for the experiments are presented while highlighting foreseen challenges along with the potential countermeasures to tackle them. Our key focus has been to investigate the idea of PCB surface fingerprinting under controlled conditions to demonstrate the proof-of-the-concept.

In the future work different imaging devices for template registration and counterfeit detection and large number (9600) of via surface patterns from 80 custom designed test PCB surfaces with only PCB vias will be investigated. A novel application of industrial CT in area of security dealing with counterfeit detection of *electronic devices within the device cover* based on PCB surface fingerprints is identified and investigated. To simplify the task at hand initially optical imaging technique is considered to demonstrate proof-of-concept and CT images will be considered in the future work. An accurate automatic image registration and segmentation for fingerprints computation while considering CT images is expected to pose serious challenge in this regard.

References

[1] A. Baecker, “Embadometrie - Qualitative Vermessung mikroskopischer Strukturen mittels eines optischen Sensors mit linienförmiger Apertur,” Ph.D. dissertation (in German), University of Wuppertal, 2012.

[2] J. Buchanan, R. Cowburn, A. Jausovev, and et al., “Fingerprinting' documents and packaging,” Nature, vol. 436, p. 475, 2005.

[3] C. Coombs, “Printed Circuits Handbook,” Pub. McGraw Hill, 6th Edition, 2007.

[4] T. Dewaele, M. Diephuis, T. Holotyak, and et al, "Forensic authentication of banknotes on mobile phones," in Proc. Proceedings of SPIE Photonics West, Electronic Imaging, Media Forensics and Security V, San Francisco, USA, 2016.

[5] M. Diephuis, F. Beekhof, S. Voloshynovskiy, and et al., "A framework for fast and secure packaging identification on mobile phones," in Proc. Proceedings of SPIE Photonics West, Electronic Imaging, Media Forensics and Security V, San Francisco, USA, 2014.

[6] M. Diephuis, S. Voloshynovskiy, and F. Beekhof, "Physical object identification based on FAMOS microstructure fingerprinting: comparison of templates versus invariant features," in Proc. 8th International Symposium on Image and Signal Processing and Analysis, Trieste, Italy, 2013.

[7] A.E. Dirik, H.T. Sencar, and N.A. Memon, “Flatbed Scanner Identification Based On Dust and Scratches Over Scanner Platen,” Proc. IEEE International Conference on Acoustics, Speech and Signal Processing, Taipei, Taiwan, 1385-1388, 2009.

[8] S. Ghosh, A. Basak, and S. Bhunia, "How Secure Are Printed Circuit Boards Against Trojan Attacks?", IEEE Design & Test, vol. 32, no. 2, pp. 7-16, 2015.

[9] E. T. Gilmore, P. D. Frazier, I. J. Collins, and et al., "Infrared analysis for counterfeit electronic parts detection and supply chain validation," Springer Environment Systems and Decisions, Volume 33, Issue 4, pp 477–485, Dec. 2013.

[10] T. Iqbal, “High-Capacity Analog Channels for Smart Documents,” Ph.D. dissertation, University Duisburg-Essen, April, 2006.

[11] T. Iqbal, K. D. Wolf, and D. Lichte, “Authentication of Printed Circuit Boards Based on Surface Data Coding,” IASTED Conference on Signal and Image Processing (SIP2012), Honolulu, USA, Sep. 2012.

[12] D. K. Karna, S. Agarwal, and S. Nikam, “ Normalized Cross-correlation based Fingerprint Matching,” IEEE Int. Conf. on Computer Graphics. Imaging and Visualization, 2008.

[13] J. P. Lewis, "Fast Normalized Cross-Correlation," in Proc. of Vision Interface 1995.

[14] A. Mikkilineni, G. Ali, P. Chiang, G. Chiu, J. Allebach, and E. Delp, “Signature-embedding in printed documents for security and forensic applications,” in Proc. SPIE: Security, Steganography, and Watermarking of Multimedia Contents VI, vol. 5306, pp. 455–466, Jan. 2004.

[15] J. Picard, “Copy Detectable Images: from theory to practice,” Proc. of Optical Document Security, San Francisco, 23-25 January 2009.

[16] N. R. Wagner, “Fingerprinting,” IEEE Sympoium on Security and Privacy, pp. 18-22, 1983.

[17] A. Webb, K. Copsey, and G. Cawley, “Statistical Pattern Recognition,” Book, Pub. John Wiley & Sons, 2nd Edition, 2011.

[18] F. Zhang, A. Henessy, and S. Bhunia, "Robust Counterfeit PCB Detection Exploiting Intrinsic Trace Impedance Variations," 33rd IEEE VLSI Test Symposium, 2015.

[19] B. Zhu, J. Wu, and M.S. Kankanhalli, “Print signature for document authentication,” ACM CCS, 2003, 145-154.

Appendix

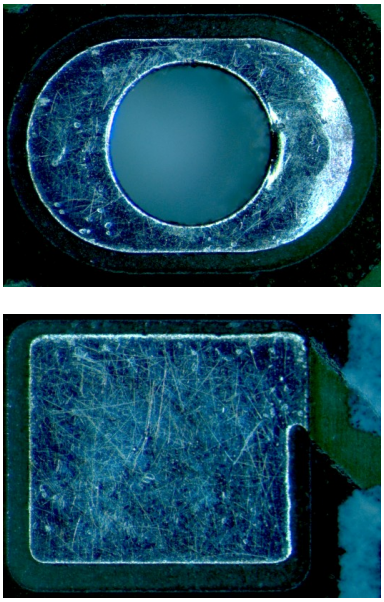


Figure A1: Random marks from manufacturing process on SMD pad surface (through-hole, top, surface mount, bottom).

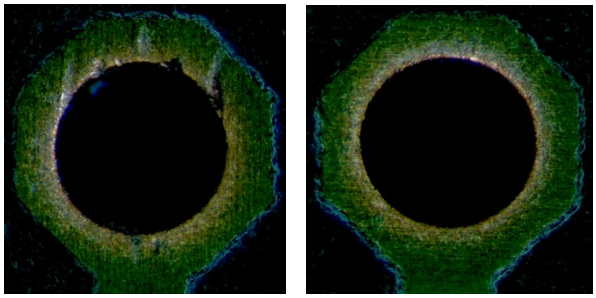


Figure A2: Random shape/size marks on via surface resulting from the PCB manufacturing process. (magnified view)

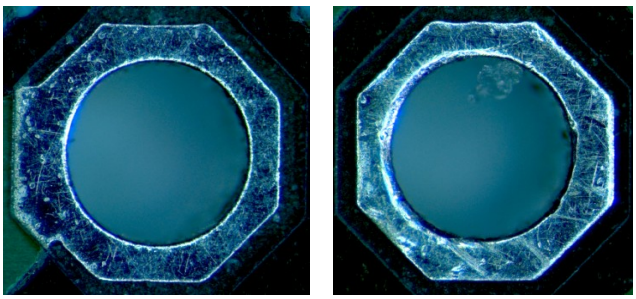


Figure A3: Random shape/size marks, dots on via surface resulting from the manufacturing process. (magnified view).