Reverse Engineering of CMOS Integrated Circuits

G. Masalskis, R. Navickas

Vilnius Gediminas Technical University, Department of Computer Engineering,
Naugarduko str. 41, LT-03227, Vilnius, phone: +370 684 23229, e-mail: giedrius.masalskis@el.vgtu.lt

Introduction

Reverse engineering is defined as „the process of analyzing a subject system to identify the system's components and their interrelationships and create representations of the system in another form or a higher level of abstraction". In the field of integrated circuits this process is usually used to verify product design correctness by taking their mask data and extracting transistor level netlist. This netlist is then abstracted to gate level and to functional level. Obtained functional level model is verified against initial chip design. [1-6]. Reverse engineering is also used to recover unavailable specifications of integrated circuits (Fig. 1) and to design new ICs using recovered data.

In this publication we propose methods of chip physical level reverse engineering using visual data of IC metal layer interconnects, called *vias*. We also provide experimental test result data of proposed methods. Brief overview of currently known reverse engineering methods is also presented.

Reverse engineering problems

Reverse engineering process may be divided to two independent stages (Fig. 1):
1. Physical level analysis.
2. Functional level analysis.

Each of these stages requires solving very different problems. When analyzing physical level, objective is to reconstruct the topology of all manufacturing process layers of the chip as accurately as possible. This stage is required if original data of photolithographic masks is not available. It is also employed when searching for errors in chip manufacturing process. Analysis process is performed on the actual physical integrated circuit when original design data is not available. Many technological steps are involved in such case: chip decapsulation, chemical or plasma etching, polishing, etc. Final goal of these steps is precise uncovering of each of technological layers of the chip. After uncovering, each of the layers is photographed using optical or electron microscopy. Digital image data is stored for further processing and analysis.

Functional analysis stage is performed when chip photolithographic mask data is available. This data may be researched using physical level analysis techniques or may be taken from original chip design, if it is available. Using automated software tools, transistor level netlist is extracted from mask data. Then transistor level netlist is abstracted to gate level and further to functional level chip representation. Model, which was obtained using abstraction, is simulated in comparison with original design model to find possible mask layout level or manufacturing process errors.
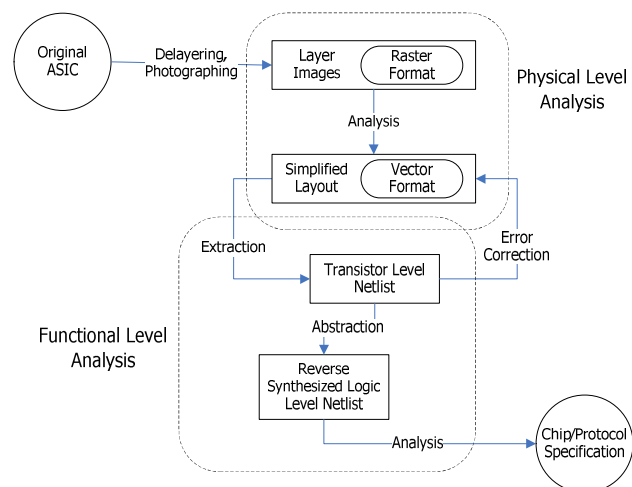

Fig. 1. Reverse engineering procedure

Most of existing scientific publications of reverse engineering field are focused on functional analysis. There are two categories of these publications. Publications in first category analyze methods of functional structure recognition (e.g.: transistors) from integrated circuit mask data [1-3]. Publications in second category analyze various functional abstraction methods using existing transistor level netlists [4-7]. Many of the described methods are implemented in various computer software programs and are applied in practice.

Publications analyzing the first stage (physical level) of reverse engineering are almost nonexistent in scientific literature. Physical level analysis of integrated circuit is however described in some of USA patents [8-10].

An automated reverse engineering system which integrates optical photography device and computer software is described in [8]. This system has significant drawbacks: it operates using predefined library of integrated circuit structural units. Unit structures are stored in digital raster image format and recognition is performed by visually searching for similar units. Using a predefined library of structures limits system abilities.

Methods for accelerating reverse engineering process which includes both physical and functional level stages are described in [9]. Most of the paper is dedicated to physical level analysis but there are no details on methods used for extracting layout data from photographic images. This paper emphasizes the problem of superposition of different layer images. System described in this paper is tool to help during manual reverse engineering process and it is not an automated system.

Reverse engineering assistant software is depicted in [10]. Algorithms characterized in the paper are suitable for integrated circuit functional level analysis only.

Considering information state in previous publications of reverse engineering field, we chose to perform our research in the physical layout level of integrated circuits. In this publication we will present methods, which enable restoration of photolithographic mask data by applying digital image processing and analysis algorithms on images of layers of integrated circuits. Such methods are required to restore mask data for further analysis using existing functional level (Fig. 1) methods and tools.

Components of integrated circuits may be recognized in digital photo images using various mathematical, morphological and statistical image processing and analysis algorithms. These algorithms are widely used in digital devices for image processing [11].

We propose methods based on these recognized digital raster image processing and analysis algorithms with specific application for IC image layer analysis. Such specialisation is possible because every layer in IC is designed and manufactured following special *design rules*.
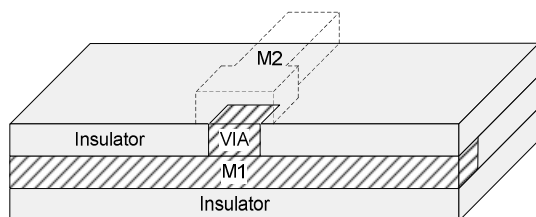
General algorithm and analysis object

Fig. 2. Simplified drawing of via and its surrounding layers

In this paper we present analysis of 2 methods suitable for recognition of IC metal layer interconnects, called *vias*. Fig. 2 displays simplified structure of via and its surrounding layers. *VIA* connects wires from first metal layer *M1* to second metal layer *M2*.

Each of two presented methods are based on general algorithm which consists of three main steps:
1. Input image processing.
2. Processed image analysis and vector data extraction.

3. Vector data analysis and processing.

Implementation of steps 1 and 2 is differs for each proposed method. To measure which method is generally most suitable for via layer data extraction, they were be put to trial using fixed batch of test images and precision of each method was calculated and compared.

Test images

Before moving on to describe the methods we must first introduce their input data. We have selected sample image sets with varying characteristics for more objective method evaluation. Four different test image sets of integrated circuit dies were used. They were taken using optical microscope. Sample images from each of the sets are shown in Fig. 3. Three of pictured ICs were manufactured using 0.35µm technology and one was manufactured using 0.25µm technology.

Technology rules define vias as fixed size squares. In test images their diameter is approximately 0.40-0.60µm and metal wire diameter is approximately 0.60-1.00µm. Image resolution is approximately 15 pixels per micrometer.
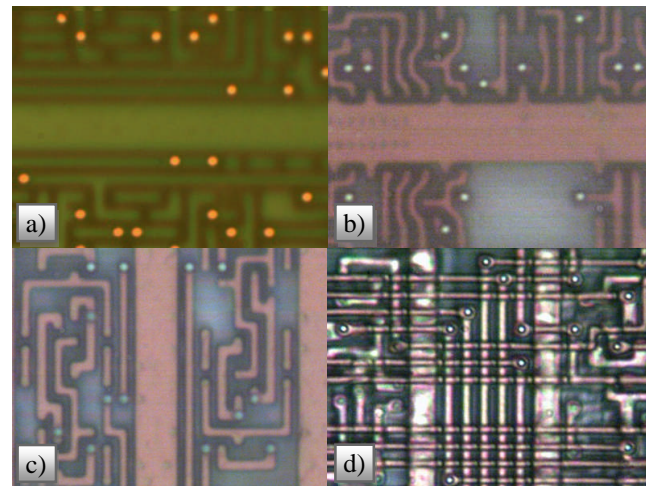

Fig. 3. Test image fragments of four different IC dies

Test samples were selected to have special properties with purpose to accurately assess efficiency of proposed via detection methods. Sample type fragment in Fig. 3a is an example of microscope image which is very suitable for via detection. Insulating layer masks metal structures very efficiently and via intensity is higher than other parts. Sample type in Fig. 3b has the most common characteristics observed when examining via layer photographs. It contains some noise, via intensity is higher than most of the remaining areas and it contains spaces without underlying metal wires. These spaces usually exhibit colour and intensity properties similar to those of vias, except their area size is much larger than via size. Sample type in Fig. 3c is similar to Fig. 3b but vias in it have intensity similar to the remaining areas. Sample type in Fig. 3d represents an extreme case. It illustrates difficult conditions for via detection: metal wires are clearly visible because of particularity of IC manufacturing process and metal wire pixel intensity and colour is equal to intensity

and colour of via pixels. This makes it very difficult to separate vias from other objects in the image.

Before performing method-specific processing, initial images must be pre-filtered to remove noise and other unnecessary details. This is done by applying median [12] filter with window size of 3x3 or 5x5, depending on the size of undesirable particles. After this step, processing steps specific for each of our proposed algorithms are applied.

Blob selection method

This is a simpler and faster of two proposed via detection methods. It is based on simple threshold filter and binary image blob feature analysis.

After noise reduction, threshold filter is applied to the image. Threshold value is constant, defined by highest intensity pixel values in via regions of image. Such approach assumes that pixels in via areas are always of higher intensity compared to their surrounding areas. Vias have lower intensity edges which separate them from other areas. This is generally true for via photographs because insulating oxide layer between two metal layers has lower light reflectivity than via regions.

After threshold filtering, resulting binary image is processed with simple blob reject filter. This step requires predefined approximate dimensions of via objects in pixels. Via size must be calculated in advance and provided to this method as input parameter.

Size-based blob filtering removes binary objects which size does not fall into size range specified by filter parameter. Remaining objects are identified as vias.

Cross correlation method

Second method is based on statistical similarity search principle. Image regions which correlate with a provided via sample image are marked as via locations.

After noise reduction, reference via search pattern is selected from the image. This pattern must be an image of single, very good quality generic via sample taken from original image. The search pattern must contain via and it must include some surrounding background edge pixels. Correct pattern selection is very important step for this algorithm. Best quality via pattern image can be derived by averaging a few well formed via image samples.

Fundamental idea of this algorithm is to calculate correlation of search pattern at every point in test image [13]. This produces cross correlation map which is stored as image with equal dimensions as input. Fig. 4 shows cross correlation result of sample image in Fig. 3d. Correlation peak points are denoted by white ovals.

Cross correlation image is threshold-filtered to isolate correlation peak points. Peak points form blobs in binary image. These blobs indicate via locations in the original image. If via size is unknown prior to detecting via locations, it is calculated afterwards. After identifying via locations, a part of original image (after noise filtering) is selected for further analysis. The selected part is threshold filtered and feature sizes at previously found via locations are measured. Collected via dimension set is used to

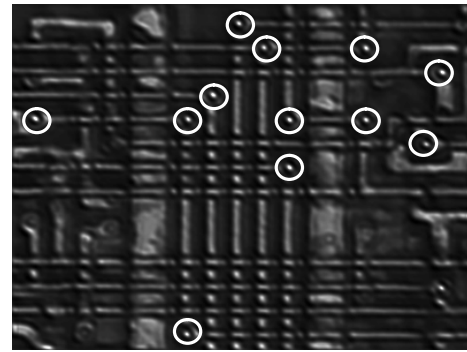calculate median value. Calculated value is the most accurate measurement of the actual via diameter.

Fig. 4. Cross correlation result of via layer image

Extracted data processing

After extracting via location and size data using two described methods, it is processed to confirm with via design rules. They define restrictions for via size and spacing. Design rules are input parameters for this processing stage.

Usually via size must be rounded to 0.1µm precision and via shape must be square.

Spacing design rule processing is used to discard some of recognition false positive matches. This is possible because they define the minimum distance between two vias. False positive via match can be identified by analyzing location data. It's indicated when location does not fall into spacing grid of nearby vias.

Results

Custom software application was designed and implemented to perform the method testing. Test results are presented in Table 1.

Table 1. Method test results

Method	Cross correlation				Blob selection			
Sample type	a	b	c	d	a	b	c	d
Total	147	16	89	99	147	16	89	99
Found	147	15	61	72	147	16	70	78
Missed	0	1	28	27	0	0	19	21
Wrong	0	0	4	8	0	0	1	185
Precision (~%)	100	94	66	67	100	100	78	27

Shaded cells in Table 1 indicate best performance cases. "Sample types" were described earlier and are shown in Fig. 3. "Total" is total count of vias in test image set. "Found" indicates how many vias were correctly identified using specific method. "Missed" tells the difference between "Total" and "Found". Values in "Wrong" row indicate how many locations in test image set were erroneously identified as vias. "Precision" row contains precision percentage values rounded to nearest integer.

On three out of four test image sets higher extraction precision was achieved using simpler method. However these image sets contain the highest quality images (Fig. 3, a, b, c). When input image quality decreases below certain level, cross correlation search method gains precision advantage over blob selection method, because latter one is

not able to distinguish vias in abundant noise patterns. Cross correlation search takes over precision lead because it actually performs recognition of predefined via patterns in noisy image in contrast to blob selection which only depends on via size information.

Conclusion

Two methods suitable for extraction of integrated circuit metal layer interconnect data from microscope images were proposed and experimentally verified.

Custom software application was developed to verify and tune proposed method algorithms.

Test results show that in most cases blob selection method is the most suitable method for via identification in image. However both proposed methods are highly dependent on the quality of input image data. Cross correlation search method is highly preferable to blob selection when input image data quality degrades.

References

1. **Bourbakis N. G., Mogzadeh A., Mertoguno S.** A knowledge-based expert system for automatic visual VLSI reverse-engineering: VLSI layout version // IEEE Transactions on Systems, Man and Cybernetics. – 2002. – Part A, Vol. 32. – P. 428–436.
2. **Li T. and Sung-Mo K.** Layout Extraction and Verification Methodology for CMOS I/O Circuits // Proceedings of the 35th Design Automation Conference. – San Francisco, USA. – 1998. – P. 291–296.
3. **Kostelijk T., De Loore B.** Automatic verification of library-based IC designs // IEEE Journal of Solid-State Circuits. – 1991. – Vol. 26. – P. 394–403.
4. **Alexander K. M., Kirk R. S., Lathrop R. H.** Automatic generation of behavioral simulation models using functional abstraction // Proceedings of the Custom Integrated Circuits Conference. – 1988. – P. 3.3/1–3.3/4.
5. **Blaauw D. T., Saab D. G., Banerjee P.** Functional abstraction of logic gates for switch-level simulation // Proceedings of European Conference on Design Automation. – 1991. – P. 329–333.
6. **Blaauw D. T., Saab D. G., Banerjee P.** SNEL: a switch-level simulator using multiple levels of functional abstraction // Proceeding of the IEEE International Conference on Computer-Aided Design. – 1990. – P. 66–69.
7. **Lester A., Bazargan-Sabet P., Greiner, A.** YAGLE, a second generation functional abstractor for CMOS VLSI circuits // Proceeding of the Tenth International Conference on Microelectronics. – 1998. – P. 265–268.
8. **Yu K. K., Berglund C. N.** Automated system for extracting design and layout information from an integrated circuit // Patent #5,086,477. – USA. – 1992. Northwest Technology Corp.
9. **Abt J., Kapler T. and Begg S.** Computer aided method of circuit extraction // Patent #6,907,583. – USA. – 2005. Semiconductor Insights, Inc.
10. **Chisholm G. H., Eckmann S. T., Lain C. M.** Reverse engineering of integrated circuits // Patent #6,536,018. – The University of Chicago, USA. – 2003.
11. **Acharya T., Ray A. K.** Image Processing Principles and Applications, Wiley-Interscience. – 2005.
12. **Tukey J.** Exploratory Data Analysis. Addison-Wesley Menlo Park, CA. – 1977.
13. **Duda R. O., Hart P. E.** Pattern Classification and Scene Analysis. – Wiley. – 1973.

G. Masalskis, R. Navickas. Reverse Engineering of CMOS Integrated Circuits // Electronics and Electrical Engineering. Kaunas: Technology, 2008. – No. 8(88). – P. 25–28.

New methods for automated visual recognition of metal interconnect technological layers of integrated circuits are presented. Image processing and analysis algorithms are used in these methods to extract interconnect structure locations and dimensions. Recognized structure data is used to recreate initial photolithographic mask data suitable for further analysis. Proposed methods were experimentaly tested and their precision was calculated from test results. To perform experimental testing, custom software was developed as a framework for this and future research. Methods proposed here are initial part of collection of methods suitable for complete chip topological structure extraction, including all layers. Ill. 4, bibl. 13 (in English; summaries in English, Russian and Lithuanian).

Г. Масалскис, Р. Навицкас. Обратное проектирование КМОП интегральных схем // Электроника и электротехника. – Каунас: Технология, 2008. – № 8(88) . – С. 25–28.

Предложена методика для обратного проектирования КМОП интегральных схем на основе автоматического визуального опознавания топологических слоев. Разработан метод для автоматического визуального опознавания слоя окон межслойных соединений и соответствующее программное обеспечение, основанное на операциях морфологического сужения и расширения. Метод использован на практике. В будущем по этой методике планируется опознавание всех топологических слоев ИС. Ил. 4, библ. 13 (на английском языке; рефераты на английском, русском и литовском яз.).

G. Masalskis, R. Navickas. KMOP integrinių grandynų lustų atvirkštinis projektavimas „iš apačios į viršų" // Elektronika ir elektrotechnika. – Kaunas: Technologija, 2008. – Nr. 8(88) – P. 25–28.

Aprašyti nauji integrinių grandynų metalo technologinių sluoksnių kontaktinių angų automatinio vizualinio atpažinimo metodai. Įprasti rastrinių vaizdų apdorojimo ir analizės atpažinimo algoritmai naudojami tarpsluoksninių sujungimų angoms ir jų dydžiams atpažinti. Šie duomenys toliau naudojami tarpsluoksninių angų fotošablono topologijai atkurti. Pasiūlytieji metodai buvo išbandyti, atliekant eksperimentus su praktiniais duomenimis, ir apskaičiuotas kiekvieno iš jų tikslumas. Eksperimentams atlikti buvo sukurta speciali bandomoji programinė įranga. Sukurtieji metodai yra dalis metodų visumos, ateityje įgalinsiančios atkurti visų integrinių grandynų sluoksnių fotošablono topologijas. Il. 4, bibl. 13 (anglų kalba; santraukos anglų, rusų ir lietuvių k.).