Printer Watermark Obfuscation

Maya Embar
Illinois Institute of Technology
Rice Campus
201 East Loop Road
Wheaton, IL 60189
(630) 788-0841
membar@hawk.iit.edu

Louis McHugh
Illinois Institute of Technology
Rice Campus
201 East Loop Road
Wheaton, IL 60189
(630) 808-9464
lmchughi@iit.edu

William Wesselman
Illinois Institute of Technology
Rice Campus
201 East Loop Road
Wheaton, IL 60189
(630) 540-8957
wwesselm@hawk.iit.edu

ABSTRACT

Most color laser printers manufactured and sold today add "invisible" information to make it easier to determine when a particular document was printed and exactly which printer was used. Some manufacturers have acknowledged the existence of the tracking information in their documentation while others have not. None of them have explained exactly how it works or the scope of the information that is conveyed. There are no laws or regulations that require printer companies to track printer users this way, and none that prevent them from ceasing this practice or providing customers a means to opt out of being tracked.

The tracking information is coded by patterns of yellow dots that the printers add to every page they print. The details of the patterns vary by manufacturer and printer model.

In this document, our team will discuss several obfuscation methods and demonstrate a successful one.

Included in this document is an explanation of the firmware generated yellow dots matrix and answers to the following questions:

1. Which printers produce the dots?
2. How are the dots put on?
3. What is needed for testing?
4. What is the dot size and spacing?
5. Where are the dots located on the page?
6. How can the dots be rendered useless?

Categories and Subject Descriptors

K.6.5 [**Management of Computing and Information Systems**]: Security and Protection – *insurance**, physical security***

General Terms

Algorithms, Measurement, Documentation, Performance, Design, Reliability, Experimentation, Security, Standardization, Theory, Legal Aspects, Verification

Keywords

Yellow Dots; Obfuscation; Printer; Watermark; Steganography; Tracking; Template; Firmware

RIIT'14, October 15–18, 2014, Atlanta, Georgia, USA.
Copyright is held by the owner/author(s). Publication rights licensed to ACM.
ACM 978-1-4503-2711-4/14/10...$15.00.
http://dx.doi.org/10.1145/2656434.2656437

1. INTRODUCTION

For almost a decade [1] some color laser printer manufacturers have implemented a system where yellow dots are added to every page printed. These yellow dots are nearly impossible to see with the naked eye, but can be seen with the aid of a high lumen blue or ultraviolet LED light and either a specific background color or a microscope. These dots are not produced by black and white printers or color printers that are not laser. The Electronic Frontier Foundation (EFF) conducted tests to verify the absence of yellow dots on these types of printers. We conducted our own tests to confirm this.

In terms of confidentiality, the presence of yellow (tracking) dots raises the following key issues: What information is being tracked? How can the information be used? Is any personally identifiable information being revealed? We reviewed the findings of multiple sources of information and conducted our own research to address these questions.

2. YELLOW DOTS

2.1 EFF Findings

The Electronic Frontier Foundation (EFF) released this statement regarding printer tracking: "We've found that the dots from at least one line of printers encode the date and time your document was printed, as well as the serial number of the printer." [1]

Since this original statement on the issue, the EFF (with grass roots support) has compiled a list of printers that produce yellow dots. [2]. The EFF has even gone to the next logical step and decoded the yellow tracking dot system implemented on Xerox DocuColor printers.

"So far, we've only broken the code for Xerox DocuColor printers," said EFF Staff Technologist Seth David Schoen, "But we believe that other models from other manufacturers include the same personally identifiable information in their tracking dots." [1]

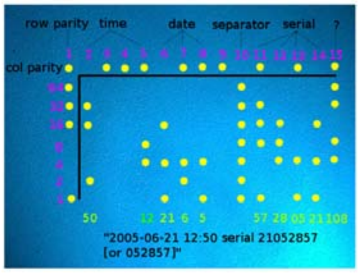

Figure 1. Xerox dot pattern explained

The EFF provided this schematic for decoding: [3]

> The topmost row and leftmost column are a parity row and column for error correction. They help verify that the forensic information has been read accurately (and, if a single dot has been read incorrectly, to identify the location of the error). The rows and columns all have odd parity: that is, every column contains an odd number of dots, and every row (except the topmost row) contains an odd number of dots. If any row or column appears to contain an even number of dots, it has been read incorrectly.
>
> Each column shown in Figure 1 is read top-to-bottom as a single byte of seven bits (omitting the first parity bit); the bytes are then read right-to-left. The columns (which we have chosen to number from left to right) have the following meanings:
>
> 15: **unknown** (often zero; constant for each individual printer; may convey some non-user-visible fact about the printer's model or configuration)
> 14, 13, 12, 11: printer **serial number** (in binary-coded-decimal, two digits per byte) (constant for each individual printer; see below)
> 10: **separator** (typically all ones; does not appear to code information)
> 9: **unused**
> 8: **year** that page was printed
> (without century; 2005 is coded as 5)
> 7: **month** that page was printed
> 6: **day** that page was printed
> 5: **hour** that page was printed (may be UTC time zone, or set inaccurately within printer)
> 4, 3: **unused**
> 2: **minute** that page was printed
> 1: **row parity bit** (set to guarantee an odd number of dots present per row)
>
> The printer serial number is a decimal number of six or eight digits; these digits are coded two at a time in columns 14, 13, 12, and 11 (or possibly 13, 12, and 11); for instance, the serial number 00654321 would be coded with column values 00, 65, 43, and 21.

The work by the EFF also raises another interesting and troubling thought: How many other technologies and devices have the government and private industries developed to limit or intrude upon our rights and freedoms?

2.2 Obfuscation Methods

One definition of Obfuscation we found was: “Obfuscation (or beclouding) is the hiding of intended meaning in communication, making communication confusing, willfully ambiguous, and harder to interpret.” [8] Our team utilized steganographic obfuscation to render the dots meaningless. We have not discovered any way to prevent the tracking dots from printing, and therefore believe this is a beneficial security technique most basic users can implement on their own computer(s).

Some considerations to ensure effective obfuscation:

Halos: Do halos exist, which distort the color around the watermark dots or content color?
Dot layer: Are the yellow dots placed in the foreground or background on the printed document?

The goal of this project was to render the forensic information contained in the yellow dots useless through one of the following obfuscation methodologies: Root Level Bypass, Yellow Block, or Steganographic Obfuscation. Following is a brief overview of each method, and an evaluation of implementation viability.

2.2.1 Root Level Bypass

Our research discovered that the yellow dots are generated at the printer firmware level. This approach involves modifying or overwriting the printer firmware to prevent generation of yellow dots by the printer.

We did not pursue this option due to the lack of available test printers for research and development. Root Level Bypass will void the manufacturer’s warranty, and any mistake will likely render the printer unusable.

2.2.2 Yellow Block

Yellow Block is a method that would either print small yellow blocks all over the page, or blanket the sheet with yellow ink.

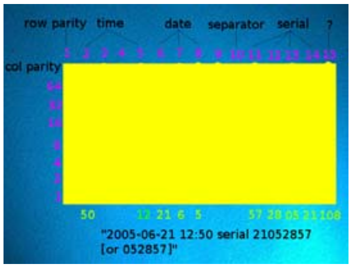

Figure 2. Modified EFF image of Yellow Block Obfuscation

From the outset, this solution seemed unreasonable due to its lack of professionalism, possible distortion of content and excessive consumption of yellow ink. The printers we tested either detected the yellow field and printed white instead of yellow dots, or printed white dots above and below the tracking dots to ensure their detectability in the yellow field (halos).

2.2.3 Steganographic Obfuscation

This method requires determination of the firmware generated yellow dot pattern (size, spacing, color, and distribution) and creation of a fill pattern that obfuscates the yellow dot information.

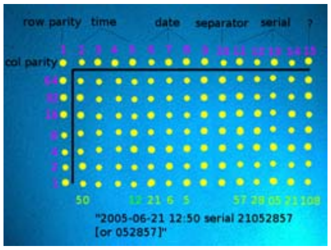

Figure 3. Modified image showing Steganographic Obfuscation

We determined Steganographic Obfuscation was the best choice for the following reasons:

- Yellow block will not work as desired; it is defeated by the printer firmware.
- It has no chance of rendering the printer useless - a distinct advantage over Root Level Bypass.
- It could be implemented simply, and with minimal impact to the appearance of documents.

2.3 Obfuscation Implementation

To implement this method, we created a template in Microsoft Word that blanketed the entire page with yellow dots that are slightly larger than the printer watermark dots. The image created for use in the template was a 600 dpi 8.5 x 11 inch transparent PNG with 1 pixel x 1 pixel yellow dots in a grid pattern. A magnified sample of that image is shown below.

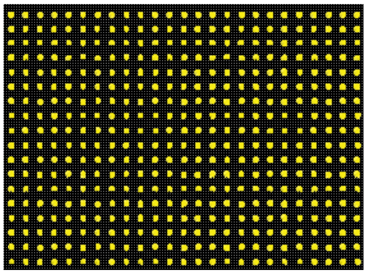

Figure 4. Section from Proof of Concept Template

Figure 4 shows the yellow dot obfuscation pattern on a black background to enhance visibility of the yellow dots. The actual image has a transparent background. We then created a new .dot template using this image as the background. We created a new document using this template, and found the firmware generated yellow dots were obfuscated.

Complete documentation of how to create the obfuscation image as well as how to use that image to create a .dot template can be found in the User Manual available for download. [6]

2.4 Obfuscation Results

2.4.1 Imaging

The following equipment was used by our team to produce the images contained in Appendix 7.1:

- Digital Blue QX7 Microscope: http://www.newegg.com
- Gorilla Glass slides: http://www.shop.gorillascientific.com
- Vinyl Microscope Slide Cover Slips (Figure 5)
- Blue Light: Handmade - parts purchased from Radio Shack
  - Battery Pack
  - Switch
  - Blue LED
  - Battery

Type of Printer	Model
Konica-Minolta bizhub	C452
HP LaserJet Pro Color	M251nw
HP LaserJet Pro Color	M451nw
HP LaserJet Pro Color	M451dn

Table 1. Tested Color Laser Printers

The printers listed in Table 1 were selected because of their availability for use and testing at our campus. The microscope was used to capture magnified images of the yellow dots produced by the tested color laser printers. We determined that a blue LED light and magnification of 10x or greater makes the yellow dots visible.

2.4.2 Image Refinement

Some of the images in Appendix 7.1 have been altered in either exposure or color to enhance the yellow dots produced by the printer. In no case were any dots added or deleted, and in all cases the type of modification that was made is included in the image caption.

2.4.3 Yellow Dot Template

The Yellow Dot .dot template is available for download. [6]

3. Research and Analysis

3.1 Research

3.1.1 EFF updates

The EFF has a list of printers that do or not display tracking dots [2]. There are different printers in the list now than when we began our research in 2013. The Konica-Minolta C452 printer used for testing in 2013 is no longer on the list of printers which have been verified as yellow-dot producing. The three HP LaserJet Pros that our campus recently acquired are not on the EFF list either. These omissions contradict our analyses, because all four printers did in fact produce yellow dots on all color pages that we printed. We contacted the EFF regarding these omissions.

3.1.2 Analysis

The four printers that were tested all displayed the yellow dots. Images of these results appear in the Appendix.

We used cover slips gridded with 0.5mm squares in a 20x20 pattern (Figure 5) as overlays on the printed samples to quantify the size and spacing of the dot patterns. The microscope, set to 60x magnification, was used to capture images of the samples. The resulting images were then imported into AutoCAD. The cover slip grid was used as a reference distance of 0.5mm to determine all other observed distances (see the Appendix for images).

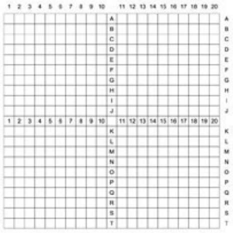

Figure 5. 0.5mm Gridded Cover Slip

3.1.2.1 Grid Spacing

The HP LaserJet Pro Color printers all used 0.8 mm Grid-Spacing. The Konica-Minolta printer used 0.5 mm Grid-Spacing.

This implies that there will be no way to make a universal steganographic template that will work for all printers. A separate template must be created for each specific grid spacing layout.

3.1.2.2 Dot Size

Three of the printers (Konica-Minolta C452, HP M451nw, and HP M251nw) all appear to use dots approximately 0.19mm in diameter.

The HP 451dn uses dashes (0.06mm x 0.14mm) rather than dots.

This implies that for best results the least observable steganographic dot should be customized for each printer according to the dot size it is embedding on the document.

3.1.2.3 Yellow Field Treatment

All of the tested printers were found to have a method for dealing with printing a yellow field (Yellow Block obfuscation).

The Konica-Minolta C452 leaves white/negative space where the Yellow Dot would be expected to appear.

The HP printers all printed the Yellow Dot (or dash) where it would be expected to appear in the yellow field, but created negative space above and below the dot.

3.1.2.4 Steganographic Template Results

There is a small offset to the tracking dots that varies by printer. The obfuscation grid layer, not individual dots, must be moved to compensate for this offset for each individual printer. Once this offset has been made, the obfuscation grid overlays the pattern of the tracking dots and renders them useless.

4. CONCLUSIONS

There are multiple discussions about the yellow dots and their potential impact on privacy (see references), including requests to at least one manufacturer [4] and a Freedom of Information Act request to the US Secret Service. [5]

None of these discussions about the yellow dots has explored what can be done about them. The only “solution” has been to discourage the purchase of printers that appear on the “known to produce dots” list maintained by the EFF.

To the best of our knowledge, the steganographic obfuscation technique developed by our team is the first time anyone has taken direct action to render the printer firmware generated yellow dots useless.

As a proof of concept, we have succeeded in showing that the dots can be effectively and unobtrusively obfuscated by filling the page with a grid pattern of yellow dots that are slightly larger than those generated by the printer.

We encourage the development of printer model-specific templates to obfuscate Yellow Dots.

Further development of this project could incorporate Root Level Bypass as described in Section 2.2.1.

User Manuals and the Yellow Dot Template that was created by our team can be found online in our Google Drive. [6] The Images generated using the QX7 microscope can be found in a separate folder. [7]

5. ACKNOWLEDGMENTS

Steganographix would like to thank Professor William Lidinsky, his Teaching Assistant Ben Khodja, and the staff and faculty at Illinois Institute of Technology Rice Campus for their contributions of testing materials, equipment, time, and guidance.

We would also like to thank Samuel (Stephen) Martin, a member of the initial team (TH2). Mr. Martin came up with the concept of obfuscation that Steganographix is utilizing in our research. Due to scheduling conflicts, Mr. Martin was unable to continue participating, however we would like it to be noted that he will always be considered a member of our team.

6. REFERENCES

[1] Schoen, S. October 16, 2005. Secret code in color printers lets government track you. Electronic Frontier Foundation. Retrieved November 3, 2013 from https://www.eff.org/press/archives/2005/10/16

[2] EFF. List of printers which do or do not display tracking dots. Electronic Frontier Foundation. Retrieved September 22, 2013 from https://www.eff.org/pages/list-printers-which-do-or-do-not-display-tracking-dots

[3] EFF. DocuColor Tracking Dot Decoding Guide. Electronic Frontier Foundation. Retrieved September 22, 2013 from https://w2.eff.org/Privacy/printers/docucolor/

[4] Neufeld, B. 2008 – 2012. FOIA request nets list of manufacturers. Brahm’s Yellow Dots. Retrieved September 22, 2013 from http://brahmsyellowdots.blogspot.com/

[5] Prewitt, K. 2012. Freedom of information act appeal – file no. 20100517. U.S. Department of Homeland Security United States Secret Service. Retrieved September 22, 2013 from http://www.scribd.com/doc/94599181/FOIA-release-names-spy-printers

[6] Steganographix, 2013-2014. Steganographix Documentation Retrieved May 20, 2014 from https://drive.google.com/folderview?id=0B9ZrovajUPg2NFEtNXZKUi02Tjg&usp=sharing

[7] Steganographix, 2013-2014. Steganographix Images Retrieved May 20, 2014 from https://drive.google.com/folderview?id=0B9ZrovajUPg2U3Z2Ul9WSXI0b1U&usp=sharing

[8] Wikipedia. The Free Encyclopedia. Retrieved September 22, 2013 from http://en.wikipedia.org/wiki/Obfuscation

7. APPENDICES [*]

7.1 Images produced from documents printed from HP Color Laser Jet Pro printers

7.1.1 HP LaserJet Pro Color M251nw

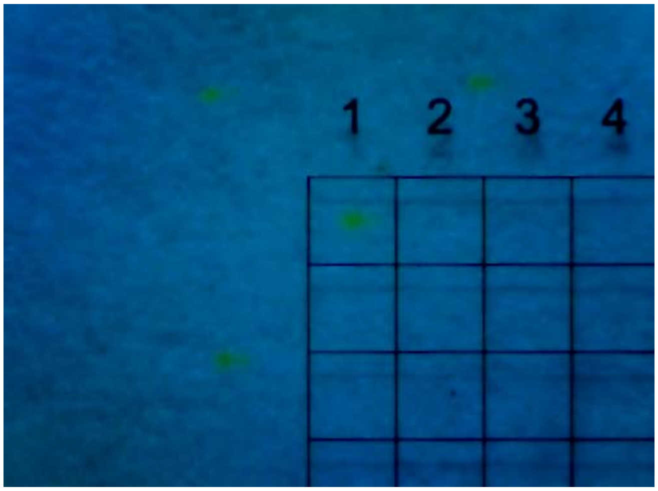

Image 1 (Blue lit, 60x mag.)
Original - No Modification

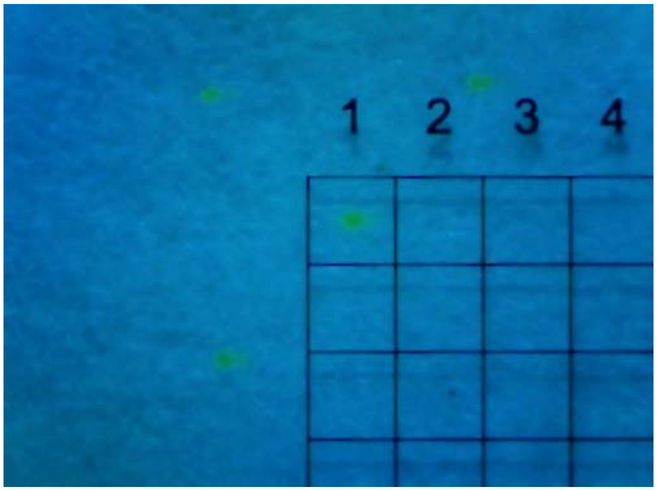

Image 2
Enhanced to showcase yellow dots

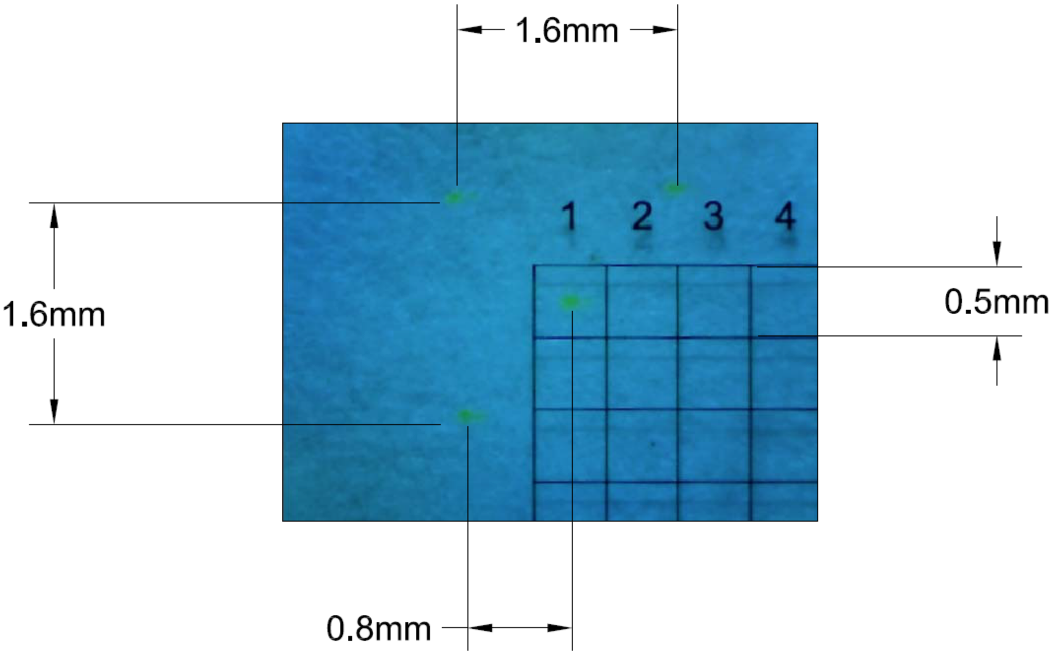

Image 3
Image 2 yellow dot spacing measured with .5mm cover slip

7.1.2 HP LaserJet Pro Color M451dn

[*] The full collection of images obtained by our team can be found at:
https://drive.google.com/folderview?id=0B9ZrovajUPg2U3Z2Ul9WSXI0b1U&usp=sharing
The images are contained in folders labeled by date.

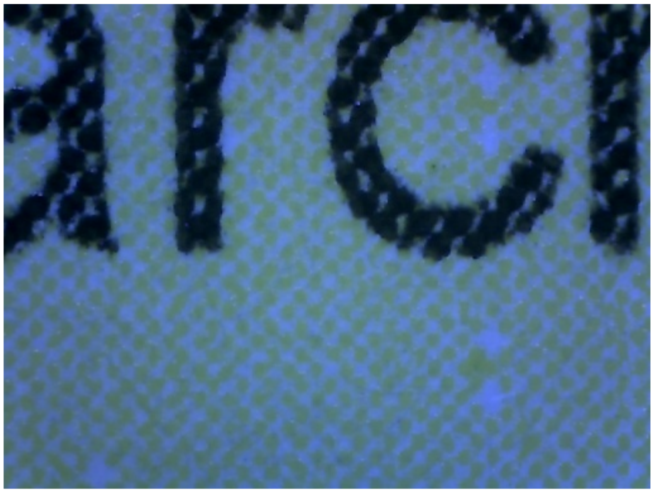

Image 4 (Blue lit, 60x mag.)
Original - No Modification

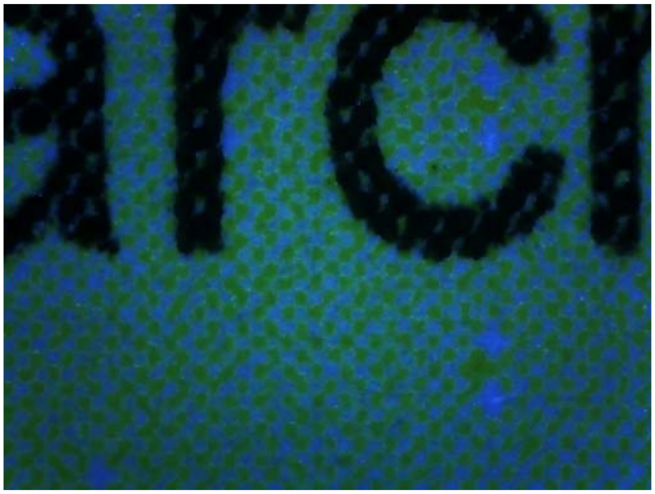

Image 5
Enhanced to showcase yellow dots

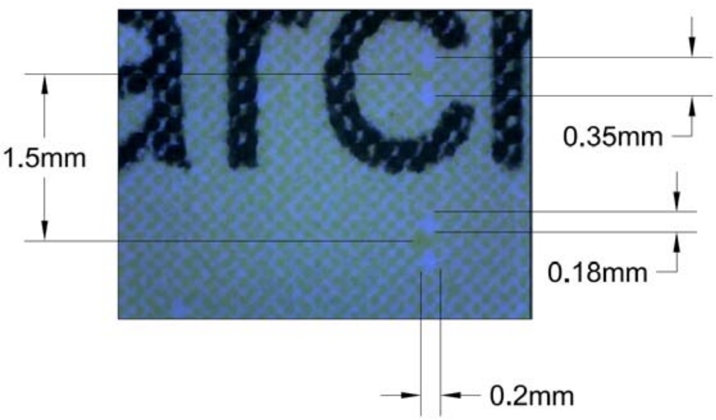

Image 6
Image 4 measured with .5mm cover slip

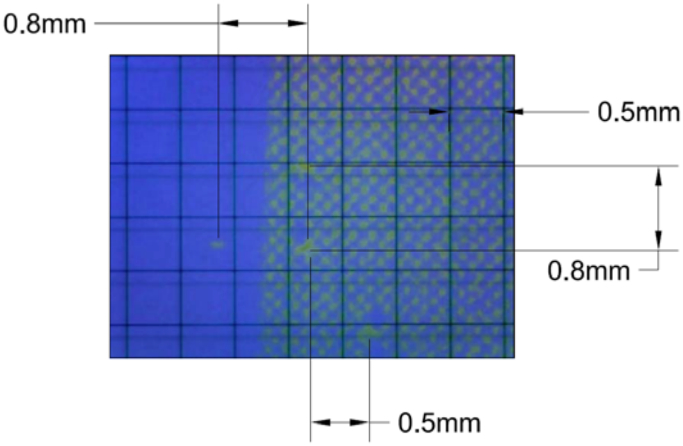

Image 7
Image 5 measured with .5mm cover slip