Digital Detective

Investigating lookup tables

Lesson

Forensic science uses the principles of scientific investigation to gather and interpret evidence for civil or criminal law cases. Forensic evidence includes photographs, documents, DNA, weapons, and fingerprints as well as trace evidence such as hair, footprints, and fibers. Image processing has had a major impact on the field of forensic science. It has enabled investigators to examine evidence with an additional set of eyes—the "eyes" of the computer and other digital devices. In this lesson, you will examine several lines of forensic evidence. As a digital detective, you will use image processing techniques to help you solve crimes. You may be asked to testify in court, so you will need to document your methods carefully.

Forensic Science—the science of interpreting or establishing the facts in civil or criminal law cases.

Part 1: *Photographic evidence*

In the course of solving crimes, detectives sometimes gather photographs and other images. Photo radar and surveillance cameras are two common sources of photographic evidence. Details in these images are not always perfectly clear. With image processing you can expose hidden features and compare details of crime scene images.

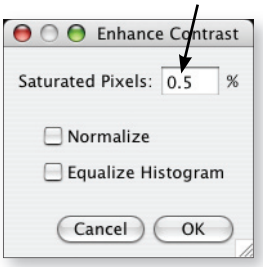
- As you look at each piece of photographic evidence, experiment with the following techniques for bringing out hidden details. Try to obtain the sharpest and most detailed image possible.

Image enhancement techniques

To use this technique…	do this
Change the brightness and contrast of the image.	Choose Image > Adjust > Brightness/Contrast, and adjust the **Minimum**, **Maximum**, **Brightness**, and **Contrast** sliders, or choose Process > Enhance Contrast. (See tip at right.)
Highlight a range of pixel values	Choose Image > Adjust > Threshold, and adjust the upper and lower threshold limits.
Change the image's lookup table	Choose Image > Lookup Tables, and select one of the available lookup tables.
Magnify the image	Click on the image, or drag to define the area you want to magnify using the tool.
Invert the image	Choose Edit > Invert.
Sharpen the image	Choose Process > Sharpen or Process > Filters > Unsharp Mask. (Other filters under the Process menu may be useful too.)

Process > Enhance Contrast *tip*

For best results, experiment with different percentages of Saturated Pixels.



Open **01 ATM Receipt.tif**.

File > Open…

A faint receipt from an ATM (Automatic Teller Machine) was found at the home of a suspected burglar. Unable to read the account number or the amount of the deposit, you scanned the receipt to convert it into a digital image. Use the techniques described earlier to reveal this information.

1. What is the account number? How much was deposited?
2. Describe the steps you used to reveal the information.

Close **01 ATM Receipt.tif**.

Open **02 Surveillance Camera.tif**.

You've asked the bank for photos of anyone using the account number above. They were able to provide one picture, but the quality is poor.

Enhance the image to bring out the details.

3. Describe the suspect and how you were able to see him or her.

Close **02 Surveillance Camera.tif**.

Open **03 License Plate.tif**.

The license plate of this car was caught on camera as the suspect was fleeing from a burglary. You believe your burglar has struck again.

Enhance this image to reveal the license plate number of the car.

4. What is the license plate number?
5. Describe the method you used to reveal the plate number.

Close **03 License Plate.tif**.

Part 2: *Examining documents*

Documents are another major focus of forensic science. Examiners determine the authenticity of written materials and look for signs of alteration or forgery. They determine the age of documents, examine the printing or writing, and even analyze the paper and ink itself. They work with typewritten, photocopied, and handwritten materials ranging from personal correspondence to legal documents. Validating signatures is an important part of document examination.

Open **04 Dated Will.tif**.

At first, this will appears to be genuine and unaltered. However, you believe it is actually an older will, and that someone changed the date to make it seem to be the most recent version.

6. Can you show that the date has been changed? Describe your technique.

Close **04 Dated Will.tif**.

A woman named Susan Jones has just been arrested for suspected fraud. She is accused of forging checks using several aliases, one of which is Sarah Black. As the document examiner in charge of the case, you have asked Susan to submit a handwriting sample to you. Even though no one signs his or her name exactly the same way each time, there will be many similarities between signatures from the same person.

Open **05 Sample Signatures.tif** and **06 Questioned Signature.tif**.

- Arrange the images so you can see both of them at the same time.

The questioned signature has faded from exposure to the sun.

- Activate each image, and enhance it to make the writing as dark and clear as possible. If you enhance the image contrast using Image / Adjust / Brightness/Contrast, be sure to click the **Apply** button in the **B&C** window before continuing.

Image > Adjust > Brightness/Contrast

Now compare the questioned signature to the sample signature using the following overlay technique. Watch for similarities in the strokes of letters.

Making transparent overlays

- Activate the **06 Questioned Signature.tif** image, click , and select a rectangle around the signature.
- Copy the selection, activate **05 Sample Signatures.tif**, then paste the selection on top to create a "floating" copy of the questioned signature.

Edit > Copy
Edit > Paste

- Open the **Paste Control,** and try out different transfer modes to find one that makes the pasted signature transparent while allowing you to see the sample signatures beneath it.

Edit > Paste Control...

7. Which transfer modes make the pasted signature transparent?

- Drag the questioned signature over the sample signatures, and look for similarities between letters.

8. What letter or letters share a similar shape and style between the two signatures?

- Choose Edit > Undo to remove the pasted signature.

Paste Control tip

Do not click on the image outside the area you pasted or it will become a permanent part of the image, and you will not be able to reposition it. If this happens, immediately choose Edit > Undo and repeat the select, copy, paste process.

You will be presenting your evidence to a jury, so you need to gather additional data for comparing the signatures. Document examiners often characterize signatures by measuring the angle of slant and calculating the ratio of uppercase to lowercase letter sizes. For the best results, average the data from at least four of the sample signatures.

Calculating the average slant angle

Before you can measure the slant angle of the letters in the signature, you need to be sure the baseline—the imaginary line that touches the bottoms of the letters—is horizontal. The questioned signature is tilted slightly.

- Activate the **06 Questioned Signature.tif** image.
- Click , then drag a straight line from left to right that touches the bottoms of most of the letters. As you move the line, its angle is displayed in the status bar of the ImageJ window. You can adjust the line after you select it by dragging the small handles at the ends or in the middle.

Read angle of line here

9. What is the angle of the baseline you selected?

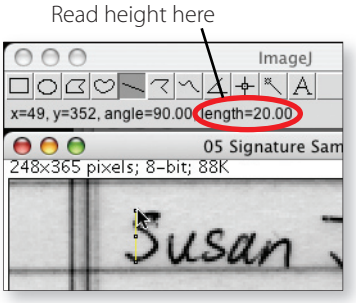
- Choose Edit > Selection > Select All to select the entire image.
- Choose Image > Rotate > Arbitrarily, and enter the angle of the baseline you recorded. Check the **Interpolate** option, and click **OK**. The signature should now be horizontal. (If not, press the R key to revert to the original image and repeat the measurement and rotation process.)

- Use again to measure the slant of several letters in both the sample signatures and the questioned signature. To measure consistently, drag each line selection from the baseline up.

10. Record your angle measurements on your **Data Sheet**. When you have finished the angle measurements for each signature, calculate and record the average angle for each signature in the table.
11. How does the average slant of the letters in the questioned signature compare to the average slant in the sample signatures?

Calculating the uppercase-to-lowercase letter height ratio

To calculate a ratio of uppercase to lowercase letter sizes, you will measure the heights of the first two letters of the first and last names. Divide the average uppercase height by the average lowercase height to obtain the ratio. Use this technique for both the sample signatures and the questioned signature. (Note: With the questioned signature you will only have two uppercase and two lowercase measurements.)



- Click , then click on the images to magnify both to 200% or larger to make the letters easier to measure.
- Click , and hold down the **Shift** key to make a straight vertical selection from the top to the bottom of each letter. The length of the line is displayed in the status bar of the ImageJ window as you drag the line selection. Record the height of each letter on your **Data Sheet**.

12. Record the heights of the uppercase letters of the sample signatures and the questioned signature on your **Data Sheet**.
13. Calculate the average uppercase heights for the sample signatures and the questioned signature, and record them on your **Data Sheet**.
    - Repeat the procedure to measure and record the heights of the lowercase letters on your **Data Sheet**.
14. Record the heights of the lowercase letters of the sample signatures and the questioned signature on your **Data Sheet**.
15. Calculate the average lowercase heights, and record them on your **Data Sheet**.
16. Divide the average uppercase height by the average lowercase height for the sample signatures and the questioned signature, and record them on your **Data Sheet**. This is the letter height ratio.
17. How does the ratio calculated for the questioned signature compare to that for the sample signatures?

- Close all images when finished.

You solve it!

- Open any of the cases in the **07 More Signatures** folder, and use the identification techniques of this lesson to solve the crime.

Part 3: *Latent prints (fingerprints)*

Latent fingerprints are one of the most common forms of forensic evidence collected at crime scenes. Since every fingerprint is unique, a suspect's fingerprint found at the scene of a crime is an undeniable way to prove the person was there at some time.

- Open **08 Fingerprints.tif**.

The set of fingerprints you are looking at was photographed, cut out, pasted onto a card, and then scanned into the computer. The crime scene fingerprint comes from a glass display case at a jewelry store that was burglarized. You also have fingerprints of several suspects.

18. Whose fingerprint do you think the crime scene print most closely resembles?

It is difficult to see details in these fingerprints, so you will use larger versions that have been scanned at higher resolution.

- Close **08 Fingerprints.tif**.
- Open all the images in the **09 Large Fingerprints** folder. (Click **Window > Tile** to spread them out.)
- Enhance each fingerprint to obtain the sharpest, most detailed image possible.

One way to begin eliminating suspects is to classify each fingerprint by type. You may want to move the windows around to place fingerprints side by side for comparison.

- Open **10 Fingerprint Types.tif**.

Fingerprints are classified into three main types: arches, loops, and whorls.

- Classify each suspect fingerprint by type. Click A to label each suspect image with its fingerprint type. Remember to click on the image using the text tool, type the name, then press **Ctrl-D (Opt-D** on Mac) to print the name on the image. (Double-click to open the **Color Picker** and change the color of the text.)

19. Which suspects can you eliminate based on the fingerprint type?

- Close the fingerprint images of the suspects you have eliminated.

At this point, you may think you know who committed the burglary. To help you make a positive identification, you need to gather more data from the fingerprints. You will mark and label key features and calculate ridge counts.

- Open **11 Fingerprint Info.tif**. Use the **<** and **>** keys or the slider control to move through the slices of the stack as instructed.

When evidence is presented to a jury, labeled diagrams of fingerprints are used. The key features of a fingerprint that used to characterize it include the core, the delta, the ridge count, and several points of comparison.

- Move to the second slice of the stack.

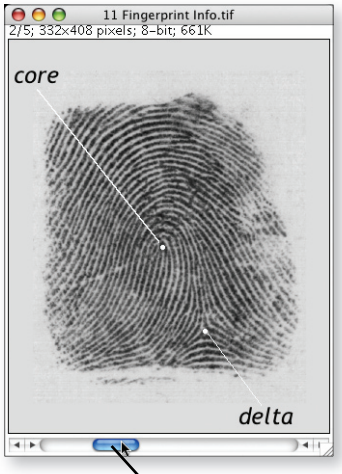
The *core* is the central point in the fingerprint pattern, and the lines are known as *ridges*. The *delta* is the point closest to the core where the ridges diverge or pull apart. Cores and deltas are unique features of loop- and whorl-type fingerprints, but arches lack them.

Latent?

The word "latent" means present but not evident. A latent fingerprint is a fingerprint that is not apparent to the eye, but can be made visible by dusting or some other method to make it identifiable.

Ten types of fingerprints?

The 10 in the file name means it is the tenth image you open, not that there are ten types of fingerprint patterns! There are only three main types of fingerprint patterns.



Slider control—drag to move through stack

- Move to the third slice of the stack.

The number of ridges crossed by a line drawn between the core and the delta is called the *ridge count*.

- Move to the fourth slice of the stack.

In a fingerprint, points where ridge lines split are known as *bifurcations*. Any of these can be marked, as they are unique to the fingerprint. Typically, 5–10 points of comparison are selected for each fingerprint. The legal number of points required to confirm a match vary from state to state.

- Label each fingerprint in the manner shown on the fifth slice of the stack. To make the dots, click to use the Point Selection tool, and then click on the image. Click to draw the lines and to insert text labels. Remember to press **Ctrl-D** (**Opt-D** for Macs) to "lock" the point or lines on the image!

20. Based on your analysis, which suspect was definitely at the scene of the crime?

- Close all the fingerprint images.

Part 4: *Trace evidence*

Trace evidence includes many kinds of material left at crime scenes, including footprints, tire tracks, hair, blood, bullet markings, clothing, and bodily fluids.

Hair and fibers

- Open all the images in the **12 Hair** folder. (Choose Window > Tile to spread the images out.)

These hair samples were gathered from friends and associates of a murder victim. Each sample is magnified about 400 times actual size.

- Choose Window > Hair Structure.tif to activate the hair structure image and familiarize yourself with the terminology and criteria for categorizing and comparing hair specimens.

The central core of a hair, the *medulla*, is made of large cells that are often separated by air spaces. When viewed under a microscope, the medulla is often clearly visible. You will use the features of the medulla to help you describe each hair and try to find a match to the crime scene hair.

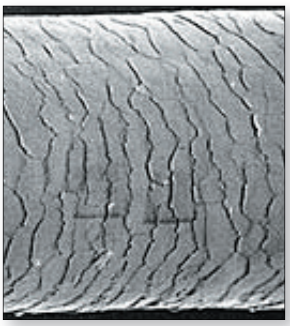
- Enhance each image to show the most detail.
- Label each hair with its medulla classification: none, fragmentary, discontinuous, or continuous.
- Compare the suspects' hair to the hair from the crime scene. Close the hair images from the suspects you eliminate.
- When you have narrowed down the list of suspects to a few, measure the diameters of the remaining hairs and the diameters of their medullas.
- Calculate ratios by dividing the diameter of each hair by the diameter of its medulla.

21. Who was at the murder scene, and what evidence do you have to support your claim?

Hair structure

Each strand of hair contains three distinct layers. From the outermost layer inward:

- The **cuticle** is a single layer of scales that interlock with the cells of the hair's inner root sheath to firmly anchor the hair in the follicle.
- The **cortex** is composed of keratinized cells that are tightly bound around each other. These bands provide the hair with strength.
- The **medulla** consists of large, loosely connected cells with air spaces between them. By reflecting light, these air spaces help to determine the sheen and color tones of the hair.



Cuticle of a normal hair shaft.

- Close all the hair images when you are finished.

Tire tracks

- Open all the images in the **13 Tire Tracks** folder.

Automobile tires also have characteristic patterns that help to determine whether or not a particular vehicle was at the crime scene. The three **Tire Tread** images show the tire tread patterns from the cars of three suspects, and the **Crime Scene Track** image is a photograph taken of a track left on a driveway at the crime scene. The lighting was poor when the picture was taken, so the track pattern is nearly impossible to see.

- Process the **Crime Scene Track** image to obtain the clearest possible view of the tread pattern, and compare it to the tire patterns from the three suspects' vehicles.

22. Based on your examination of the evidence, which suspect's vehicle was at the scene of the crime?

- Close all the tire track images when you are finished.

On your own

Create your own "forensic evidence" for an imaginary crime. Write a short story describing the crime, the suspects, and any available clues. Challenge others to use image processing techniques to help solve the crime.

Name(s) _____ Class _____ Date _____

Data Sheet

Digital Detective

1. What is the account number? How much was deposited?

2. Describe the steps you used to reveal the information.

3. Describe the suspect and how you were able to see him or her.

4. What is the license plate number?

5. Describe the method you used to reveal the plate number.

6. Can you show that the date has been changed? Describe your technique.

7. Which transfer modes make the pasted signature transparent?

8. What letter or letters share a similar shape and style between the two signatures?

9. What is the angle of the baseline you selected?

10. Record your angle measurements in the table below. When you have finished the angle measurements for each signature, calculate and record the average angle for each signature in Table 1.

Table 1

Letter Number	Letter Angle	
	Sample Signatures	Questioned Signature
1		
2		
3		
4		
5		
6		
7		
Average angle		

11. How does the average slant of the letters in the questioned signature compare to the average slant in the sample signatures?

12. Record the heights of the uppercase letters of the sample signatures and the questioned signature in Table 2.

Table 2

Sample letters for measurement		Letter height (pixels)	
		Sample signatures	Questioned signature
Uppercase	Letter 1		
	Letter 2		
	Letter 3		
	Letter 4		
	Average		
Lowercase	Letter 1		
	Letter 2		
	Letter 3		
	Letter 4		
	Average		
Ratio (Upper/Lower)			

13. Calculate the average uppercase heights for the sample signatures and the questioned signature, and record them in Table 2. (Divide average uppercase height by average lowercase height.)
14. Record the heights of the lowercase letters of the sample signatures and the questioned signature in Table 2.
15. Calculate the average lowercase heights, and record them in Table 2.
16. Divide the average uppercase height by the average lowercase height for the sample signatures and the questioned signature, and record them in Table 2. This is the letter height ratio.
17. How does the ratio calculated for the questioned signature compare to that for the sample signatures?

18. Whose fingerprint do you think the crime scene print most closely resembles?

19. Which suspects can you eliminate based on the fingerprint type?

20. Based on your analysis, which suspect was definitely at the scene of the crime?

21. Who was at the murder scene, and what evidence do you have to support your claim?

22. Based on your examination of the evidence, which suspect's vehicle was at the scene of the crime?