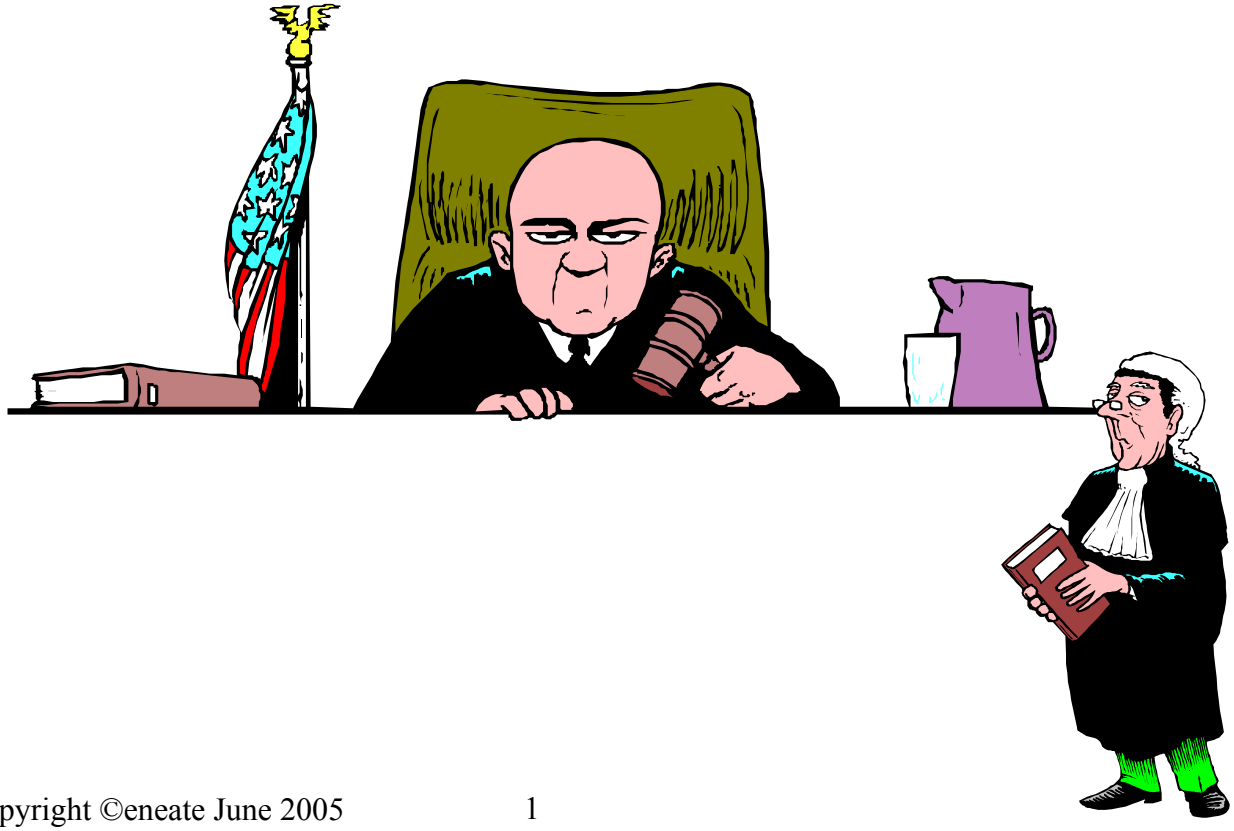
Digital Images as evidence in the judicial process



To enable us to use our digital images in court it is important that we have some means of being able to authenticate our images.
The DCS-3 was designed as a complete digital workstation, it was therefore an important design consideration that secure image integrity software was included which would demonstrate the credibility of the digitally photographed image. It was also important that the software was fast, efficient, simple to use, and most of all highly secure.
For additional information on the legal ramifications of digital imaging in law enforcement I suggest you look at the following documents :-

1. FBI definitions and guidelines for the use of imaging technologies in the criminal justice system.
2. Legal ramifications of Digital imaging in law enforcement.
3. Select committee appointed to consider Science and Technology. 3rd Feb 1998

Veridata

Veridata created by Signum Technologies provides a fast, simple and effective means of image authentication and file management. It will automatically perform the following tasks on all captured images

1. Perform a 'check-sum' method of image authentication which is saved with the image.
2. Record the operators name and personnel details with each image.
3. Record the date and time of image capture.
4. Give each captured image a sequential number which is stored with image details in a database.
5. Where available it records the serial number of the hard drive on which the image is captured.
6. It records the method of image capture (image authenticated at the point of capture or at a later date.)
6. Place the users images in their own folder (the system knows who they are from their own user name and password.

'One Touch'

All photographs are taken using the Veridata 'One Touch' facility. This involves the user pressing F12 on the keyboard or the Capture button in the DCS-3 Foster and freeman software. Veridata Idem is activated, and it calls up the DCS-3 camera capture software. Once the image has been captured Veridata will ask the user for a file name. Once this has been entered Veridata will authenticate the image and wave the unique code into the image data. The image is then saved into the users own (or a group) folder and a duplicate (without authentication) or working copy is saved into the users 'prints' folder. This image is opened in Image Pro Plus and converted into black and white, positive or negative as selected by the user.

Authentication

To authenticate the image Veridata exploits the fact that each pixel in a digital image is represented by a number that specifies it's colour (see information on bit depth in the digital imaging article.) The software breaks the picture into an unpredictable jigsaw of blocks , each of around 1000 pixels.
The value of all the pixels in the blocks are added together and the total is slightly altered, usually by plus or minus 1 (checksum value). This value is subsequently woven into the image data without visibly modifying the image or altering the image size.
All systems have their own unique alphanumeric key, this key selects sites in the file where the 'checksum' information will be hidden. The large number of ways in which this is possible provides yet another security feature. There are, for instance billions of ways of choosing 10 elements from 100, so the probability of correctly selecting the correct sets by chance is negligible.
To further ensure the security of the image the Veridata algorithm uses a level of security that far exceeds that offered by 128-RSA encryption, it is impractical to ' hack' images protected by Veridata without obvious detection. The Veridata algorithm uses 192-bit encryption.
The security of this form of image authentication has enabled the use (and acceptance) of digital fingerprint images in the UK courts.

The 'Digital negative'

The authenticated image is automatically stored in the photographers own negative folder on the computers hard drive. This image is never altered and is referred to as the 'Digital Negative'. It is automatically write protected, if anyone deliberately tampered with the image, the alterations would automatically be detected by the software. No image enhancement is ever applied to this original image. The image is always stored in a lossless format.

The working copy

The working copy is automatically generated at the point of image capture. It is a copy of the 'digital negative'. It can be altered in any way, we generally make the following statement :-

The goal of image enhancement is to improve the usefulness of a image for a given task, such as producing a more subjectively pleasing image for human viewing.

The images are not manipulated, they are enhanced. If too much enhancement is applied to the image it will eventually distort the image detail, but this is not a problem as we always have the original 'digital negative' to refer back to.

The Master Image

It is recommended that all images are copied to a non-rewritable medium as quickly as possible. This is to ensure that once the images and associated data have been copied to CD/DVD they cannot be overwritten or altered. It was also recommended in the June Home Office report that all WORM (write once read many) media is closed on the final session. This in effect, prevents any of the information about the images on the CD/DVD being changed including altering any directories. For technical information about cd's see the info on the Verbatim website select **downloads** followed by **understanding CDR/CDRW**. For further technical specification on the durability of archive CD see the info at Verbatim, under products CDR. For information on the DVD see the information on the Verbatim website.

The Database

The image is also linked into a database in the computer, this stores information relating to the image properties. In this database you will find:

- A complete sequential record of all the images captured through Veridata
- The users name
- Date and time of image capture
- Destination of the original image
- Serial number of the hard drive where the image was saved
- Method of capture - direct from the camera of hard disc transfer.
- Additional users personal details as determined by the organisation.

This database can only be accessed by the system administrator (another security feature). The database can be backed up and transferred to another computer . This enables you to restore the database, or transfer the database to another PC.
This is particularly useful if you need to demonstrate the integrity of an image in the court room on a laptop via a projector.

Verification (Detection of Alterations)

The detection process is the reverse of the creation of the 'digital negative'. It examines the data, selects the appropriate set of elements and locates the stored 'checksum' value. The value of the pixels are re-calculated and this number is compared against the recovered value. If the two are the same, the image is authentica-

tion, if they are different a message will appear stating that the image has changed. A new copy of the image will appear highlighting where the changes have occurred.

Home Office guidelines

One of the general recommendations from the UK Home Office relates to the simultaneous, or immediate creation of a working copy after the Master image has been defined.

Also all master images should be copied from the original storage medium in the original format onto a WORM (write once read many) medium, for example CDR DVDR. The disc must be closed preventing any additional material being added to the disc.

FBI Guidelines

The original image should be stored in an unaltered state. This includes maintaining original digital images in their native file formats.
Duplicates or copies should be used for working images.
Recommended media include CDR and DVDR.

Original images and images expected to undergo image analysis should not be subjected to lossy compression.

House of Lords Science and Technology recommendations for the use of Digital images 1998

The guidelines detailed below give us a good basis for how we should use and perceive digital technology within the judicial system. The full article cane be downloaded from http://www.parliament.the-stationery-office.co.uk.

This is taken from the summary and recommendations.

5. 1 We were pleased to find that digital images, which we initially thought might create difficulties for the court do not

5.2 But many people think there will be difficulty in obtaining legal acceptance of digital images. And many who understand there is no legal problem fail to appreciate fully the potential for tampering that the technology creates. The perceived difficulties mean that **opportunities are missed in a reluctance to use digital imaging technology** or to dispose of paper records, for example and the failure to understand fully the process means that too great a reliance can be placed on photographic or video evidence. The doubts and skepticism normally associated with unsubstantiated pieces of paper may be suspended when confronted with a very believable picture.

5.3 To counter the common misconception about the need for original documents, we recommend that the government encourage the appropriate legal bodies to draw greater attention to the change to digital document processing and to widen public awareness that the paper original are rarely necessary.

5.4 We do not support moves to establish specific requirements before digital images can be used as evidence and we recommend that evidence should not necessarily be inadmissible because it does not conform with some specific technological requirement.

5.5 But we are in favour of technical measures that assist with authentication of images and recommend that the government encourage the use of authentication techniques. Members of the legal profession should be made aware of the benefits of these techniques, their value in adding weight to evidence and the possible significance of their omission. Further we recommend that the government encourages the adoption of technological measures for the authentication of images as evidence by giving type approval to them. The Forensic Science Service should provide ongoing advice for manufacturers and users of imaging equipment on authentication technologies.

5.10 Overall we see a need for awareness by all those who are concerned with the potential difficulties with digital evidence. We recommend that the judicial studies board consider establishing a program of education on the implications of digital technologies for the judicial system.

Authentication Techniques

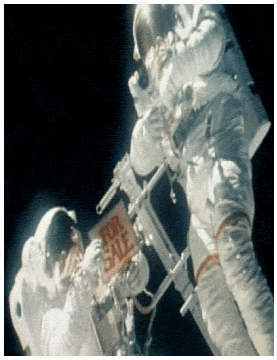
This relates to the use of a 'hash' function, where a numerical value is calculated and embedded into the metadata of the image file. A change in the pixel values causes the 'hash' function to change identifying if an image has been altered.

Watermarking

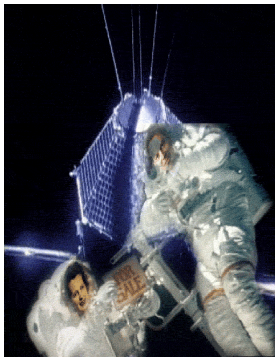
This technique describes visibly insignificant changes to pixel values. This changes if the pixel values are changed and the result is usually the deterioration of the image file through the visibility of a watermark. This type of authentication is not generally suitable for image within the judicial system.

DCS-3 Image Authentication

The DCS-3 was designed with full image authentication (not watermarking) software (Veridata) and it automatically creates a working copy of the original 'Master' image. A full audit trail records all operations on the system. All the original images are automatically saved using the lossless TIFF file format, they are all finally copied to archive compatible CDR or DVDR storage mediums for long term storage.



'Digital Negative'



Enhanced Image

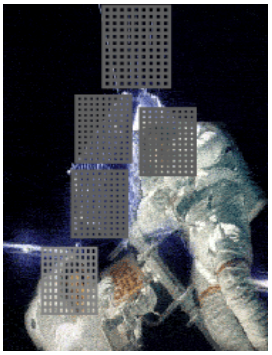


Image after Verification

The Fourier Transform and other Digital Enhancements in court

1972

The first known article published on FFT was by James Roberts in 1972 he removed the cloth weave background from a print, but the enhanced print was ruled as inadmissible in court.

1983

Housewife is found dead in a Los Angeles Suburb. A fingerprint was recovered but the surface texture from the box where the mark was found prevented any identification being made.

A Fingerprint Expert was sent to Canada to Infrascan a Canadian Electronics company. The mark was digitally enhanced and identified as that of the husband.

The case proceeded through the courts system but came to an abrupt halt when the husband committed suicide before the preliminary hearing.

1991

Finally in 1991 a ruling was made, which was to change the face of digital imaging for law enforcement world-wide.

1st Degree Murder

In March 1990, an unknown assailant sexually molested and fatally stabbed a young woman. The evidence recovered from the crime scene gave few leads, the only exhibit which gave any hope to the investigators was a pillowcase found adjacent to the victims body. It showed several blood stains, one of which showed very faint fingerprint detail.

The investigator took the pillowcase to the departments forensic unit for bloodstain pattern analysis. This resulted in the discovery of two things, firstly that the stains were consistent with transfer from a knife blade (no knife was found at the scene), secondly that the fingerprint presented enough ridge detail for a more extensive examination.

The fingerprint was subsequently treated with DFO whereupon it became more visible, however the fabric weave still prevented identification. Sometime later the fingerprint was subjected to a digital enhancement facility which resulted in an identifiable print being produced. The print was identified as that of the suspect, the DNA evidence also produced a match with the suspects code (the DNA placed the subject as only 1 in 30 million people with this DNA).

During the resultant court proceedings (Commonwealth of Virginia v. Knight, CR--90--1353--02--F)the defence attorneys launched an attack on what they believed to be the most potentially vulnerable piece of evidence, the scientific acceptance of fingerprint image processing. Due to the dispute by qualified professionals concerning the technique, it was decided to hold a Frye hearing (the test for the admissibility of a scientific process within the American courts (Frye v. United States, 293F.1013,1014(D.C.Cir. 1923)). It was held in Henrico County Virgina, and to counter to allegations a a full complement of image enhancement equipment was used by an analyst to take the court step by step through the fourier process. An expert in the field of Image processing also offered supporting testimony to the court. The court finally ruled that *"the process did not alter the characteristic arrangement of the fingerprint impression; it only made it more visible"*. The evidence had passed the test, resulting in the first documented case where image enhancement technology withstood the challenges of a Frye hearing. Click here for further information

On June 18th 1991 the court sentenced the accused to four life sentences for murder and related offences.

1991 Canada

The accused is charged with one count of robbery of Amarjit Gill on May 28 1999 at the city of Vancouver, contrary to s.344 of the criminal code of Canada, R.S.C. 1985, c.-46.

The case involved the digitisation and enhancement of video footage of the offence which would aid in the identification of the offender. The following was put to the court by the defence:

Mr McMurray submitted that the constables evidence was not admissible because it does not fall within the parameters of admissibility discussed by the supreme court of Canada in R. V. Nokolovski, (1996), 111 C.C.C. (3d) 403 (S.C.C.). There the facts were similar to those in the case at Bar, including the fact that the eye witness clerk in Nokolovski could not identify the robber from the photograph line up. Counsel submitted

that the case stands for the proposition that a trial judge can only compare the original video tape to the accused and then make his determination on whether or not he is satisfied beyond a reasonable doubt that the person on the video is the accused. At pg 416, Mr Justice Cory, speaking for the majority, pointed out that the video tape in that case had not been altered or changed, and that it depicted the scene of the crime, and therefore was admissible and relevant evidence.

Conclusion of Honourable Mr Justice Hood

In my opinion the digitisation, blowing up, and lightening of the images on the video tape does no more than enhance or clarify the images. They are not changed. The digitised images are the same images seen in the video tape. One only need compare the faces to see that the image have not been changed in the manner contemplated by Nokolovski. Digitisation is clearly a useful tool to assist the court in viewing and comparing the video tape images. Accordingly I find that Constable Frederick's video slides and other work product are admissible into evidence.

I find the accused guilty as charged

California v Phillip Lee Jackson

Mr Jackson was charged with two murders and one attempted murder. The San Diego Police Department obtained fingerprints from two of the crime scenes and enhanced them using traditional methods. The prints were those of the defendant.

However fingerprints from the third scene presented a problem, the fingerprints were difficult to focus on as the ridges were seen as 'tonal reversal'. Digital enhancement techniques were used to improve the fingerprints and it was found that they matched the prints from the other two scenes.

The evidence was disputed and the defence requested a Kelly-Frye hearing to determine the admissibility of the digitally enhanced fingerprint evidence.

However the court ruled that this was unnecessary stating that digital processing is a readily accepted practice in forensics and that new information was not added to the image.

1995

In 1995 on May the 14th Dawn Fehring a 27 year old student was dead on the floor of her Kirkland apartment. She was discovered nude near the foot of her bed with her top bed sheet and t-shirt wrapped around her head and neck. Blood stains were found on the carpet near her body and bloody hand prints were visible on the fitted bed sheet covering the mattress. An autopsy revealed that Fehring died from asphyxiation sometime the previous Friday evening and that the source of the blood was two tears in her hymen.

The suspect was an Eric Hayden a fellow occupant of her apartment building who claimed he had been drinking with friends the night before and could not remember where he had been.

The bed sheet was submitted to Holshue, a King county latent print examiner. He stained the sheet with Amido black. The Amido black process stains the proteins present in blood and other body fluid's to produce a dark blue/back product.

The result of this examination was taken to Erik Berg an expert in enhanced digital imaging at the Tacoma Police Department. He used the fourier technique to remove the interfering cloth weave resulting in the development of both finger and palm impressions. Holshue examined the enhanced fingerprints and found 12 points of comparison on one of the fingers and more than forty on one of the palm prints .

Consequently on June 5th 1995 the state charged Hayden with one count of felony murder in the first degree in violation of RCW 9A.32.030(1)(c) . Hayden was duly convicted of the offence.

Appeal

Filed 17th February 1998

Title of case: State of Washington, Respondent

v

Eric H Hayden, Appellant

Kennedy, AJC __ Eric H Hayden appeals against his conviction of felony murder in the first degree, contending that the trial court erred in admitting enhanced fingerprint evidence after conducting a Frye hearing and by ordering him to obtain a mental health evaluation and undergo treatment as a condition of his confinement and placement.2 finding no error, we affirm facts

Final Ruling

It is clear even to the untrained eye that the fabric contains a hand print and that nothing appears in the digitally enhanced photograph that was not present in the fabric. Rather the image of the hand print is merely enhanced by removing background detail unrelated to the points of identification by which the hand print was identified as Haydens……

Accordingly we reject Haydens contention that the court erred by admitting the challenged evidence and affirm his conviction judgement and sentence.

Australia

In Perth Australia a case was heard where a photograph of fingerprint was enhanced using V++ software by Imaging Expert Bruce Comber. He removed a portion of the centre spike in the diffraction pattern to "flatten" the dark and light extremes in the image, thereby allowing more contrast to be applied. There was low-contrast detail in the image but it wasn't discernible without the extra contrast.
In Court Bruce Comber gave a brief overview (in layman's terms) of the digital process in his evidence. The defence did not query the process or digital aspect in any way. He had the process reviewed by an imaging representative from a local university before offering the evidence. This review was not mentioned in court the evidence was not challenged.

South Africa

The South African Police in Pretoria are also successfully utilising this digital technology to photograph their fingerprint impressions.

United Kingdom

I started using digital enhancement techniques in 1995 after a case where the only available evidence had been a fingerprint impression on a five pound bank note.
The fingerprint was located directly on top of a series of regular lines. The Fingerprint Expert came to see me to say

"If I could remove the background pattern, the fingerprint could be proved as belonging to the offender"

However at that time I did not have access to a digital imaging system and the lines could not be removed with conventional photography. As a result the fingerprint was listed as having insufficient detail for a comparison.

Since 1995 I have processed thousands of fingerprint and footwear images with 'digital technology'. On many occasions the use of Image enhancement Tools in the DCS-3 has resulted in the identification and subsequent conviction of offenders. One such case was documented in Readers Digest October 2004:

Senior police Officers in Wiltshire were alarmed. Reports of a sharp rise in crack cocaine and heroin use led them to suspect that drugs gangs from Birmingham had infiltrated the quiet county. Undercover work by detectives posing as drugs users on the streets of Swindon led to a raid with a stash of £20,000.00 in cash was found - but the fingerprints on the money were unclear against the background. It was impossible to match them to suspects.
Enter Esther Neate the Wiltshire Forces Senior Fingerprint Development Officer. Neate took digital photos of the notes and using a computer program filtered out the background to reveal clear prints that helped jail Mosorof ali, Iqbal Ahmed and delroy McIntosh for a total of 15 years.

Today with the introduction of Digital technology previously unidentifiable fingerprint impressions can be successfully enhanced resulting in improved rates of crime detection.