Magnetic Forensics
David Pappas
National Institute of Standards & Technology
325 Broadway, Boulder CO 80305
Phone: +1-303-497-3374, FAX - +1-303-497-4311
e-mail: pappas@boulder.nist.gov

Presented at the THIC Meeting at the National Center for Atmospheric Research, 1850 Table Mesa Drive, Boulder CO 80305-5602
July 18-19, 2006
Magnetic Forensics
The Lost 18 ½ minutes of the Nixon Presidency
=> a magnetic microscopy study

David P. Pappas
Fabio da Silva
Sean Halloran
NIST, Boulder, CO

Ken Marr, James Ryan
FBI Academy, Quantico, VA
FBI - magnetic tape media forensic audio examinations

Cassette & digital audio tapes (DAT), 911 tape (DDS), VHS

Cases: Homicide, armed robbery, fraud, corruption, money laundering, drugs…

- Very labor intensive
- High profile cases
- Need to testify in court

674 cases

Ferrofluidic imaging
Other Magnetic Imaging Techniques

- Magnetic force microscopy (MFM)
  - High resolution, polarity sensitive
  - Cost, mechanical range ~ 0.1 mm, slow
- Scanning SQUID microscopy
  - Polarity sensitive, long range
  - Cryogenics, low resolution, cost
- Magneto-optically active garnet crystals
  - High resolution, polarity sensitive
  - Applied field necessary, complicated optical setup
- Magneto-resistive elements
  - High resolution, contrast, polarity, fast, long scans, inexpensive, scalable
  - Thermal asperities and drift
Outline

• Development of magnetic sensors
  – Hard disk drives
• Cassette & DAT Tape
  • How data is stored on tapes
• Analysis of magnetic tapes
  – Authenticity
  – Data recovery
• Studies of magnetic tapes
  – NARA test tapes for Nixon 18 ½ minute gap
• Development of high resolution real-time imaging system
• Outlook for data-recovery using high resolution imaging
Intense development of magnetic sensors has enabled high density hard disk drive (HDD) storage.

Thomas N. Theis and Paul M. Horn, Phys. Today, July 2003
Improvements in areal density

- **Write heads**: Smaller, stronger
- **Magneto-Resistive Read Elements**: Small, sensitive
- **Mechanical actuators, interface**
- **Error code correction**
- **Heads**
- **Media**
  - High stability
  - Small bits

Commercial technology at ~ 100 Gbit/in², demos ~ 300
- Currently limited by field strengths of write heads
- Enabled by the existence of magneto-resistive read elements
What is a Magneto-Resistor?

- Thin film resistor made with magnetic material (NiFe, Co)

1890 - AMR – “Anisotropic”: single layer film, 2% change
1985 - GMR – “Giant”: tri-layer film, Cu spacer, 50% change
1995 - TMR – “Tunneling”: tri-layer, thin oxide spacer, 400% change
Compare inductive head reader to MR

- Inductive & MR essentially the same signal
- MR signal is velocity independent
  - Move tape or disk very slowly
- Scalable down to very small dimensions
- Easily fabricated & integrated onto read head
- Can be very small – makes a good scanned probe

\[ V_{IH} \propto \frac{\Delta B_x}{\Delta t} \]

\[ V_{MR} \propto B_z \]
NIST – Built MR imaging system
HDD head as a scanned probe magnetic microscope

- Scan MR head in direct contact
- Use both the read & write elements

Applications – head, media diagnostics
- Calibrate R/W fields/currents
- Thermal decay of data
- Frequency response of heads
- Spatial transfer function
Low level digital hdd data imaged & written

- Need cutting edge heads, media
- Industry moves very fast – hard to get samples
- Data recovery –
  - Need high resolution head than disk written with
  - No standard data format

100 \mu m
Platter from 1 GB hdd
circa 1996
Other magnetic media

- Video tape
  - Helical scan
  - sample 1 µm
  - could be recovered
- Digital Audio tape
  - sample 0.1 µm
  - track pitch 13.6 µm
NTSB - Digital waveform recovery

- Airline flight data recorder – need to evaluate small scraps of tape
- 8 track
- 0.48 in blocks
- Harvard Bi-phase coding
- Sample every $1\,\mu m$
- Decoded data blocks of data

=> Solution looking for a problem
Audible tape authenticity evaluation

Work-horse analysis technique for forensics investigators
ferrofluid + microscope + dexterity + patience

$\Rightarrow$ Authenticity analysis - erasure, alteration, duplication

$\Rightarrow$ Need to screen entire roles of tape

$\Rightarrow$ Need to identify signatures of evidence tampering – head edge marks
Scanned MR image

- Detects zero frequency signals
- Higher contrast (45 – 50 dB)
- Field direction (polarity)
- High resolution
- Time consuming ~ 10 - 30 min
High resolution computer rendering

- Write head stop event
- Audio test tones
Analog waveform recovery

• Test sample with a recording of “F B I” in analog audio

~½ second of data (2.5 cm)

- 2 µm wide sample
- Sample every 6 µm (8 kHz)
- 4 kHz bandwidth
- Voice can be identified

Journal of Electron Imaging, 2005
“The Feasibility of Recovering Erased Material from the 18.5 Minute Gap in the Nixon Tapes”

National Archives and Records Administration
October, 2001
Nixon White House Tapes

• 3700 hours of recordings between Nixon, staff, visitors

• Systems installed by Secret Service in February, 1971

• As many as nine Sony machines
  – Sound activated microphones in various locations
  – Thin tape, running very slow
  – Original recordings were very low quality

• Existence made public during Senate testimony in 1973
  – Recording stopped soon afterward
  – Equipment removed in 1974

http://nixon.archives.gov/index.php
The infamous 18 ½ minute gap

- June 20, 1972 (3 days after breakin)
- Nixon & H.R. Haldeman
- Erased gap with 60 Hz buzz

- Panel of experts prepared report to Judge Sirica
  - Tapes were imaged using ferro-fluid technique
  - Head events in erased areas match Uher dictation machine used by secretary
  - Rose Mary Woods testified that she may have accidentally erased some of the tape
  - Evidence of at least 5, perhaps nine, separate and contiguous segments

AP wire story 1/24/2005
Ferrofluid image of last erase mark from Watergate tape 18 ½ minute gap (Fig. 17, event F)

Courtesy of D. Lacey, B. Koenig
NARA test protocol

- Simulate events using similar machines
- Proof of concept
  - Record test tapes
    - Intermittent audio data on vintage Sony deck
    - Erase entire tape with vintage Uher
  - Distribute to participants (gov’t and industry)
- Litmus test – recover intelligible audio data
NIST/FBI scanned MR results from NARA test tape

Did find anomalous signals on edge where there was erased audio

No recoverable audio there or anywhere else on the test tape

Next step for the FBI: real time tape imaging for authenticity analysis
255 element read heads fabricated at NIST

- 13 mm² footprint
  - Both 4 mm wide and 13 mm wide arrays
- 16 x 18 LGA on 26 mil pitch
Sensor configuration

- Wheatstone bridge configuration – signal adds on all 4 legs
- Temperature compensation between top & bottom
- ½ step from V+ to V- to next V- to V+
Calibration of 255 element die

Calibration of 256 Channel Die

Histogram of slopes
Include 255 element imager in tape path

- 256 channels

Differential 16 x 16 MUX + Preamps

16 simultaneous A/D @ 250 kHz

- 265 channels @ 10 kHz while tape moving
- Image Cassette, DAT VHS tapes in real time, while listening
Image erase head events in real time

Erased data

Image

Linescan

Record head stop event

Head start
Real time audio capture from single track

- 10 seconds of audio
- Can see signature of head stop event as it is played
VHS tape images

- Can observe tracks and alignment marks
- Currently studying for evidence of start/stop events
Summary

- Magneto-resistive microscopy is useful for forensic analysis of audio tape evidence
  - Stop/start events on cassette tapes
  - Can recover data from specific areas of the tapes that may not be accessible to standard read heads
  - These techniques may be useful for reading the data from very old tapes that cannot be played at full speed
- The data on the 18 ½ minute gap in Watergate tapes is probably not recoverable.
- Currently studying erase/stop events on VHS, DAT, DDS tape to fingerprint them.
- Finding other uses for imaging heads
  - NDE of IC’s, mechanical integrity, Biomagnetics