CERIAS

The Center for Education and Research in Information Assurance and Security

PURDUE UNIVERSITY

IS THIS HARDCOPY AN ORIGINAL?

S. Palakodety, A. K. Mikkilineni, M. Atallah, E. J. Delp

PROBLEM

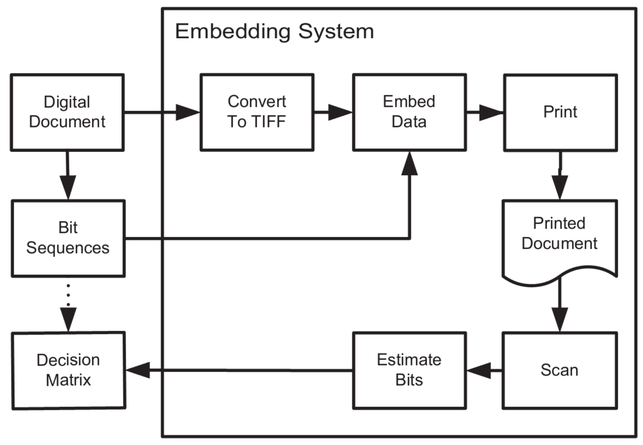
- Cheap high quality scanners and printers make counterfeiting relatively easy
- Malicious changes of important document content

GOALS

- Detect counterfeit documents reliably using commodity hardware
- Identify malicious changes in a document
- Make **no changes** to the logical document content

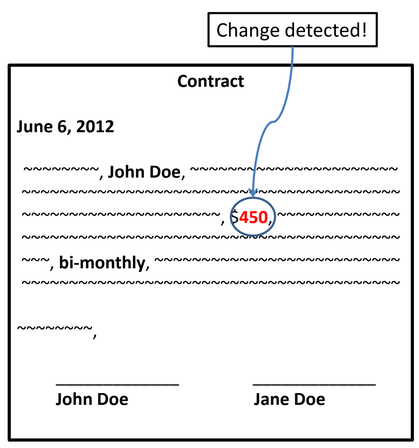
DETERMINING DOCUMENT AUTHENTICITY

- Use an existing high-capacity data hiding technique to embed bits
- Each character is embedded with a unique HMAC
- To test authenticity:
  - Recover HMAC from document
  - Compare recovered HMAC with the known HMAC for that document
  - Document is considered a counterfeit if the number of matching bits is less than an empirically derived threshold (*threshold test*)



DETECTING AND LOCATING MALICIOUS CHANGES

- Identify *n* important items such as names, dollar amounts, and dates in a contract
- Embed HMACs of important item(s) in *n* (or *log(n)*) regions of the document
- **Approach 1: Protecting *n* items with *n* checksums (Identify any number of changes)**
  - 1 HMAC per item embedded in document
  - To detect changes:
    - Compare recovered HMACs with recomputed HMACs of the *n* items
    - HMACs that fail a threshold test are considered suspect
- **Approach 2: Protecting *n* items with *log(n)+1* checksums (Identify at most 1 change)**
  - Based on combinatorial group testing
    - One checksum is global HMAC of all items
    - *log(n)* checksums are HMACs of distinct subsets of the *n* items
  - To detect changes:
    - If the recovered global HMAC fails a threshold test then at least 1 item has changed
    - Compare remaining *log(n)* recovered HMACs with recomputed HMACs
    - Use group testing with threshold test to determine which item has changed



EXPERIMENT + RESULTS

- Genuine documents showed *T=92.38%* correctly recovered bits with standard deviation *s=3.08*
- After one scan-print cycle only *49.04%* of bits are correctly recovered
- Detection threshold is set to *(T-2s)%*
- Both *log(n)* and *n* checksum approaches were able to detect and locate changes made to documents in all tested cases

Percentage of correctly recovered bits from first and second generation documents.

Doc ID	$T_{\hat{G}_1}$	$T_{\hat{G}_{2a}}$	$T_{\hat{G}_{2b}}$	#chars $\in \Omega$	#chars
Doc01	93.57	36.05	46.88	168	661
Doc02	91.19	37.95	48.20	267	978
Doc03	95.47	53.54	50.86	257	901
Doc04	93.45	53.43	49.06	383	1361
Doc05	94.05	36.90	50.79	254	920
Doc06	86.03	24.26	29.78	119	449
Doc07	90.05	35.75	48.92	101	421
Doc08	92.93	52.88	53.80	73	362
Doc09	88.29	45.24	57.14	237	907
Doc10	95.35	45.35	54.94	184	640

Portions of this work were supported by National Science Foundation Grants CNS-0915436, CNS-0913875, Science and Technology Center CCF-0939370; by an NPRP grant from the Qatar National Research Fund; by Grant FA9550-09-1-0223 from the Air Force Office of Scientific Research; by sponsors of the Center for Education and Research in Information Assurance and Security; and by a grant from the U.S. Army Research Office as a Multi-disciplinary University Research Initiative on Standoff Inverse Analysis and Manipulation of Electronic Systems under grant number W911NF-05-1-0337. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the sponsors.

CERIAS

Discovery Park e-Enterprise Center