Overview of Recent Content Authentication Research at MSR Crypto, Redmond

M. Kivanc Mihcak
Microsoft Research, Cryptography and Anti-Piracy Group
Redmond, WA, 98052, USA

kivancm@microsoft.com

OUTLINE

- Tamper-resistant biometric IDs: Using encrypted face and iris information to prevent forged identities
- Counterfeit resistant optical fibers: Using randomly-scattered optical fibers to detect forged products
- Image watermarking against content forgery: Using fragile and robust invisible watermarks to yield tamper-evident and traceability information

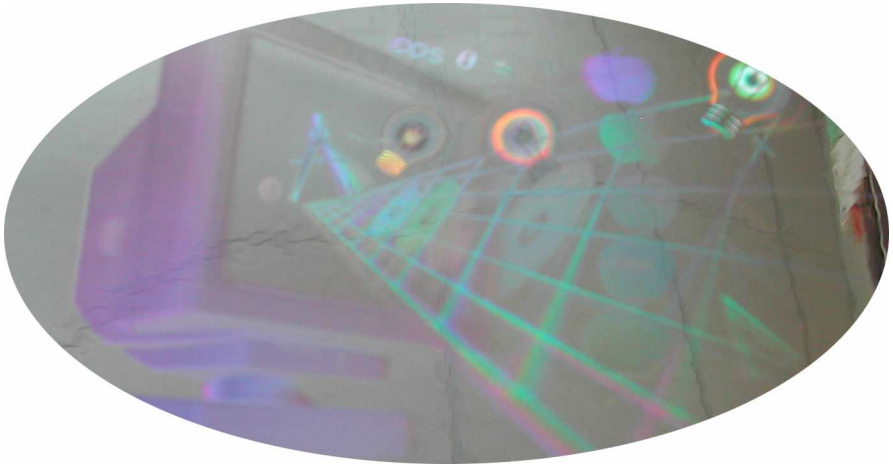
Part I: Tamper-Resistant Biometric IDs

Main Contact: **Darko Kirovski**
E-mail: ***darkok@microsoft.com***

What is a Photo ID?

ID# : 0123
Name: trausti
Eyes: blue

Photo +Text + Counterfeit deterrence = Photo ID



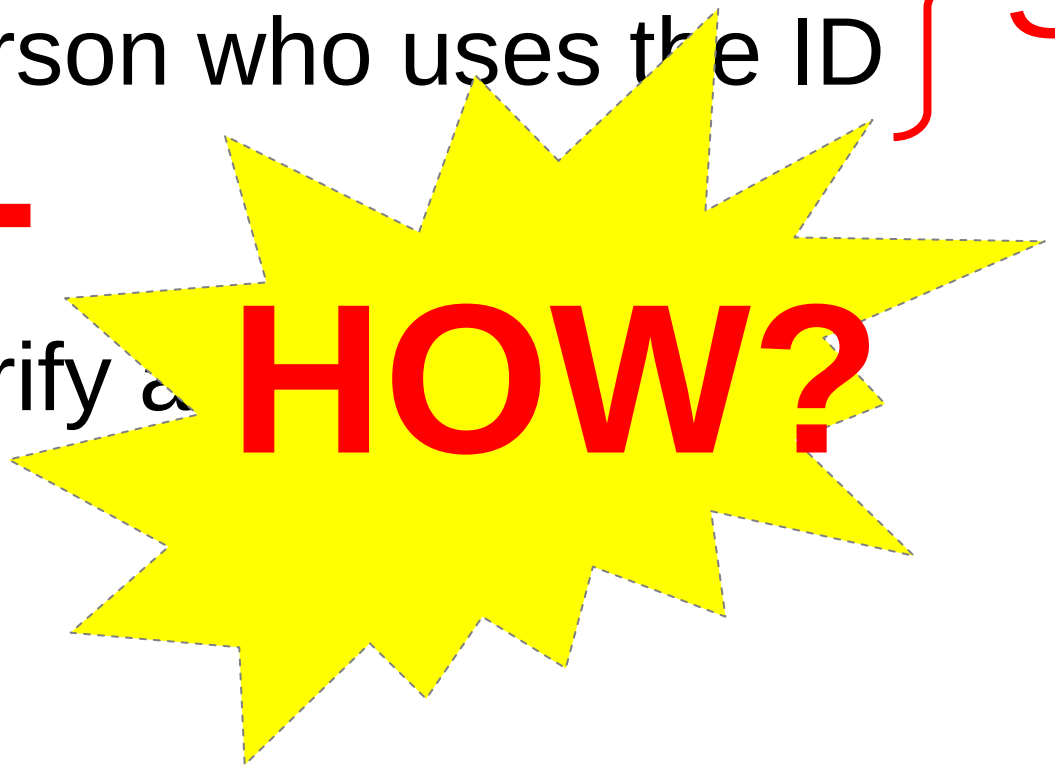
How to Verify Photo IDs?

- Person on Photo ID
- Person who uses the ID

} SAME

+

- Verify a



SECURITY

LICENSES TO KILL

For terrorists, getting fake ID is simple and cheap

ON THE LOOSE: *Suspected terrorist El Shukrijumah has several passports*

On Mar. 20, the FBI put out an all-points bulletin for Adnan G. El Shukrijumah. A suspected al Qaeda terrorist last seen near Miami, he allegedly speaks English, pilots planes, and "poses a serious threat to U.S. citizens," according to the FBI. But despite a worldwide dragnet and near-blanket distribution of his photo by the U.S. news media, authorities have been unable to track down the alleged Saudi national—who, officials say, evades capture using several fraudulent passports, six known aliases, and a forged green card.

The case highlights one of the biggest holes in the war against terrorism: the easy availability of fake ID. After September 11—and the discovery that 18 of the 19 terrorists had used fraudulent IDs to complete their

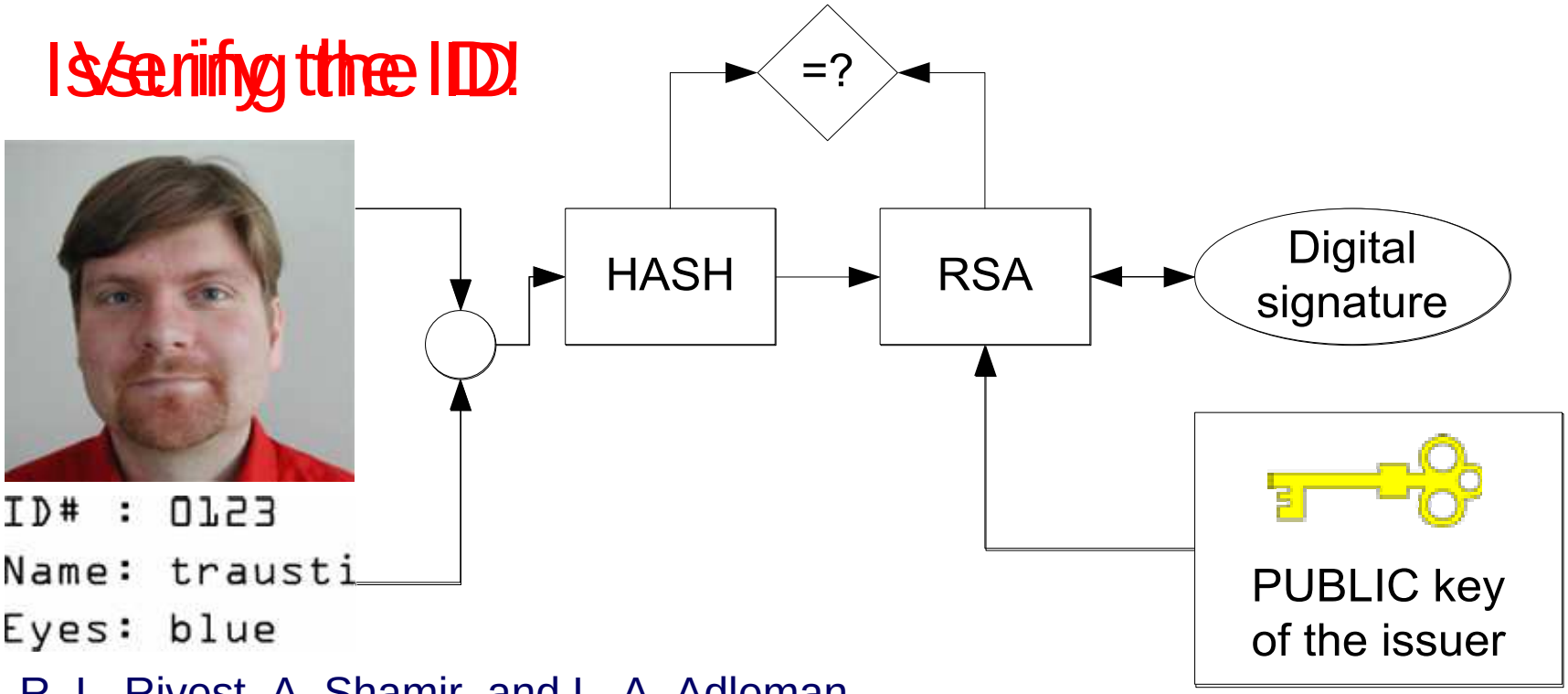
nuclear facilities have stepped up ID checks, while the Homeland Security Dept. now requires some visas to include fingerprints and photos.

But nobody believes these steps have come anywhere close to solving the problem. According to immigration experts and forensic document specialists, the U.S. fake-ID trade is at least a $1 billion annual business that produces as many as 10 million bogus passports, Social Security cards, birth certificates, and driver's licenses each year. Using $500 laser printers and Adobe PhotoShop software, counterfeiters keep cranking out credible paperwork for a pittance. "It's frightening that people are turning themselves into de facto U.S. citizens," says Marti Dinerstein, president of Immigration Matters, a New York-based reform group, who has studied the fake-document industry.

Based on information that has emerged from the recent crackdown, *BusinessWeek* has pieced together a comprehensive view of how the counterfeit underground works. For most illegal immigrants, the first stop on the path to a new identity is usually a document mill. These businesses are located everywhere—boarded-up laundromats in Atlanta, storage warehouses in Los Angeles, strip malls in Tulsa. Typically, they are run by the dominant local ethnic group—Hispanics in Florida and Los Angeles, Chinese in San Francisco, Middle Easterners in Detroit. Security is tight: Customers contact the mills through unlisted phone or beeper numbers passed out by insiders.

The document factories used to be

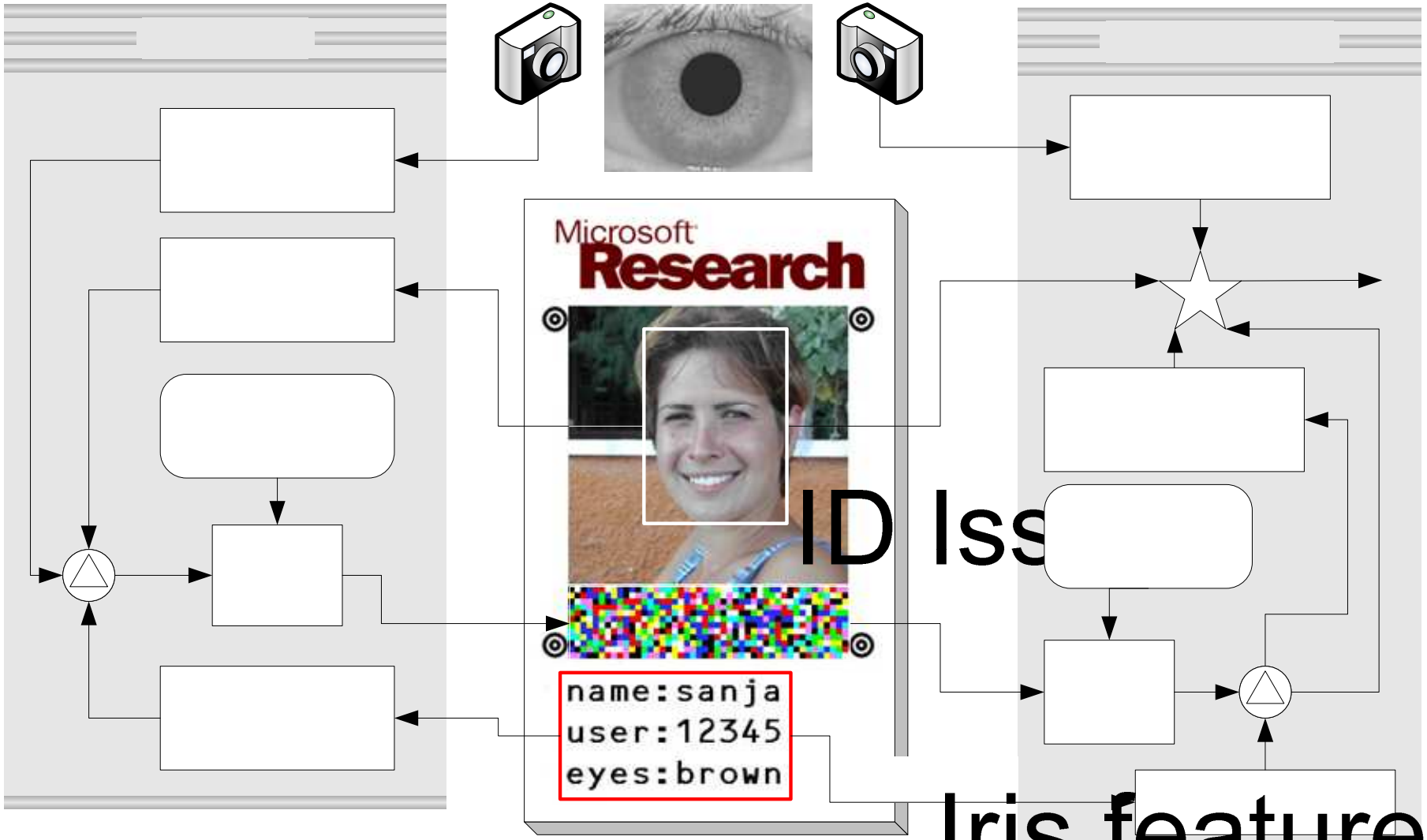
Recipe from the Crypto Community



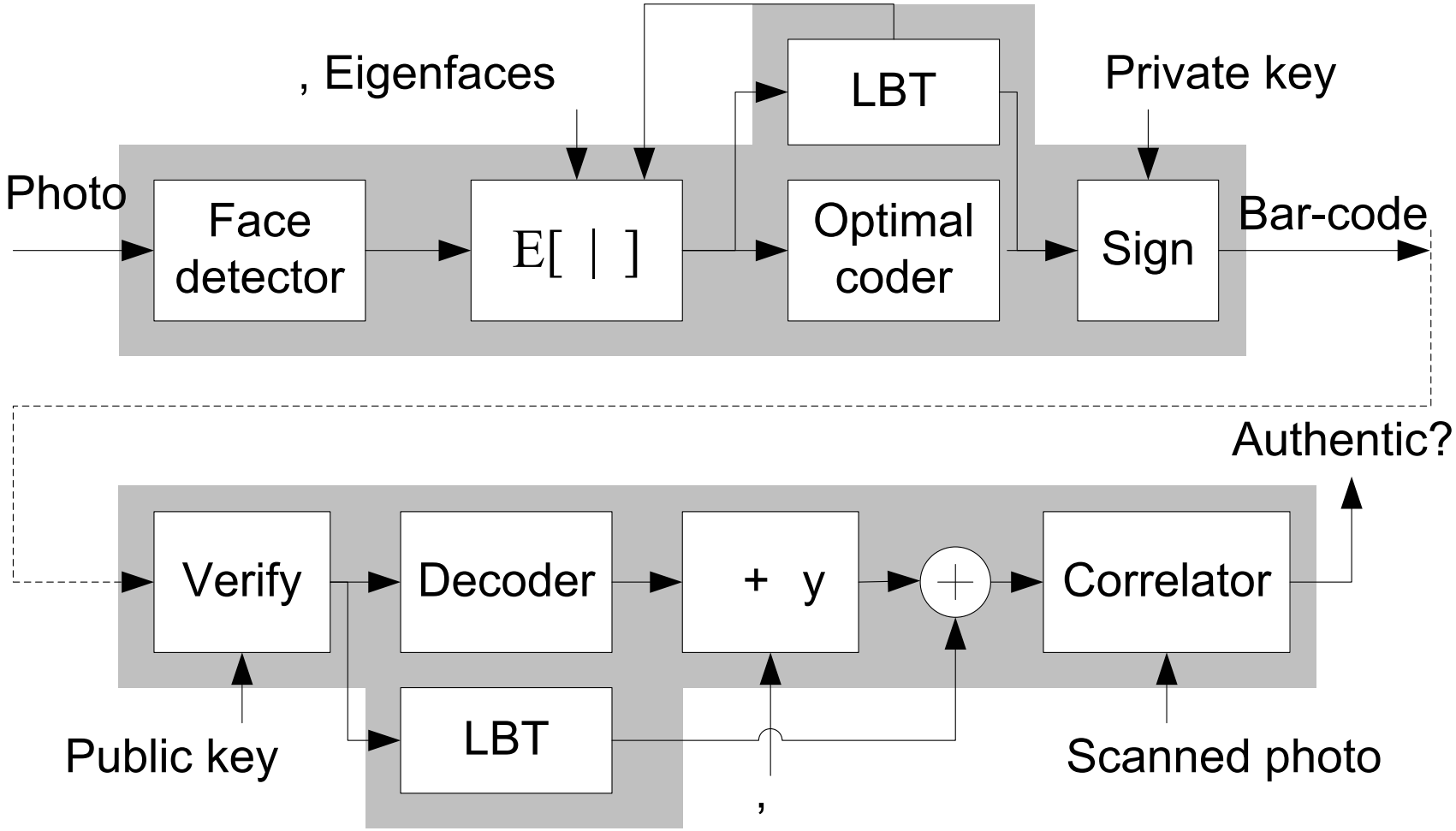
R. L. Rivest, A. Shamir, and L. A. Adleman.
A method for obtaining digital signatures and public-key cryptosystems.
Communications of the ACM, vol.21, no.2, pp.120--126, 1978.

Problem!

- DESIGNED FOR DIGITAL DOMAIN
  - Photo, text, and signature are all reconstructed exactly
  - COST = $15+ [SMART CARD]
- PAPER DOMAIN
  - COST = CENTS
  - NOISY MEDIUM

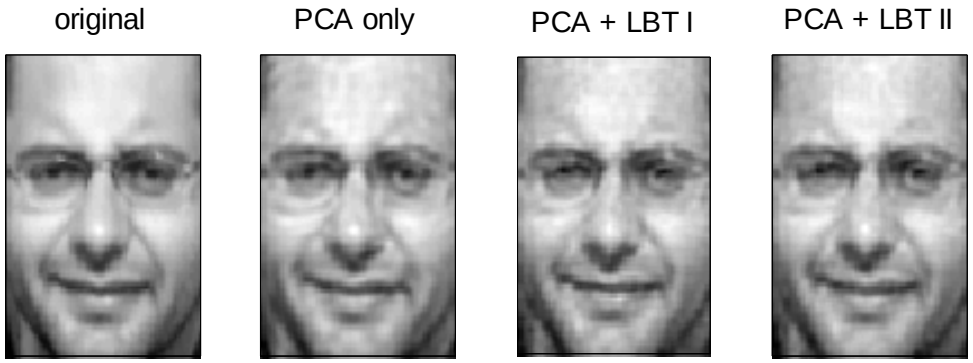

Microsoft
Research
name:sanja
user:12345
eyes:brown
ID Iss
Iris feature
compression

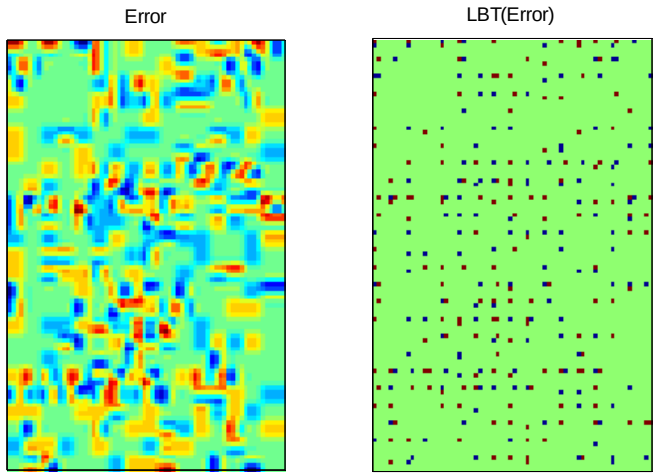
Face Compression



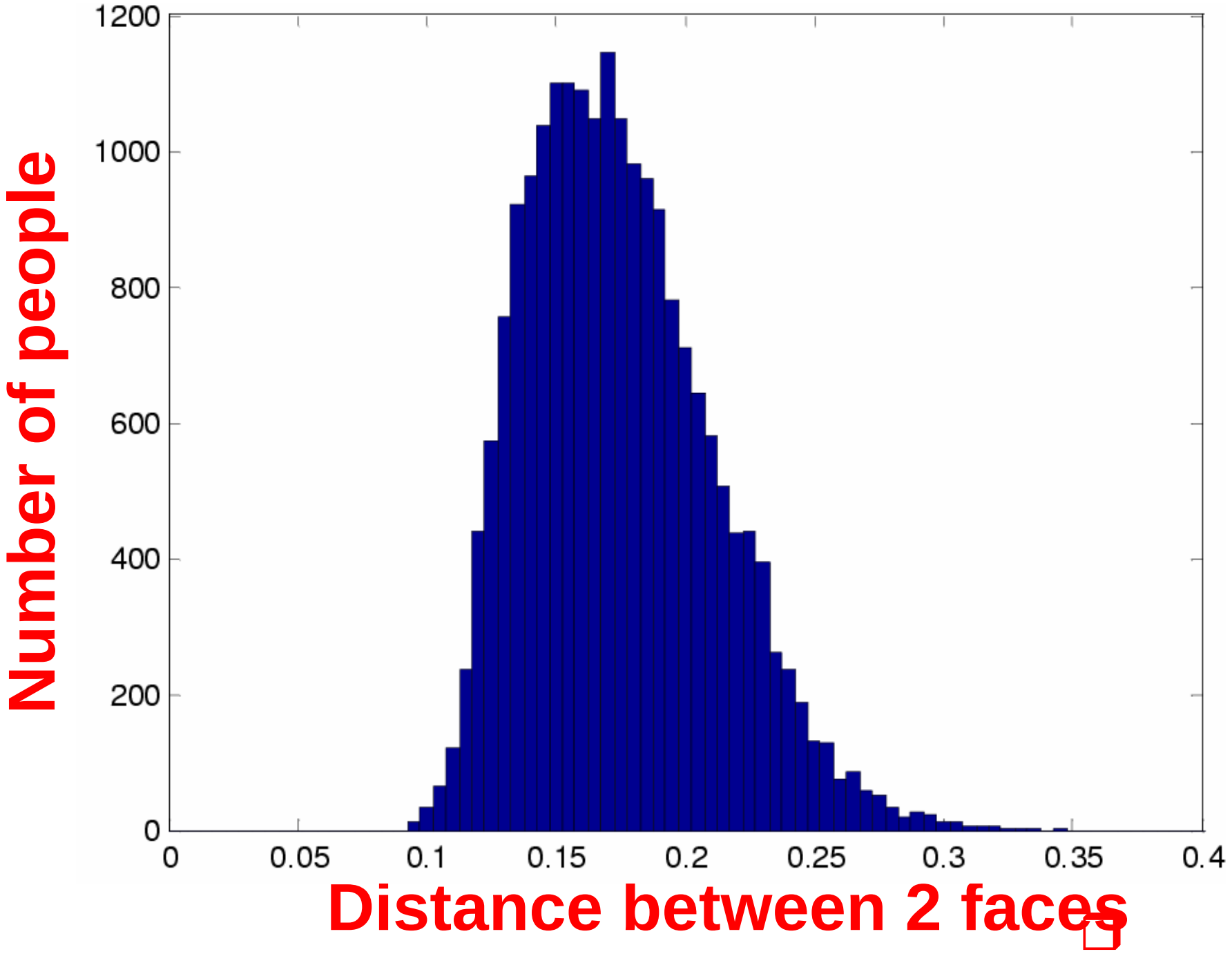
Face = Linear combination of Eigenfaces

Error encoded using a lapped biorthogonal transform





Euclidean distance = 0.011

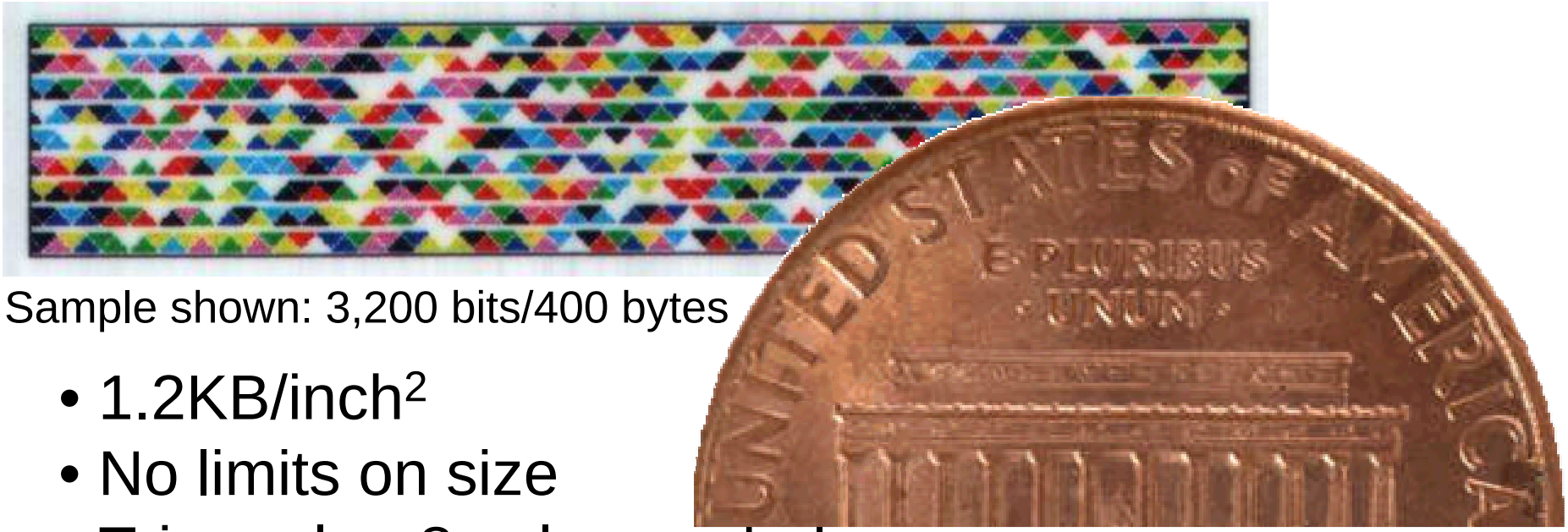

Number of people
1200
1000
800
600
400
200
0
0
0.05
0.1
0.15
0.2
0.25
0.3
0.35
0.4
Distance between 2 faces

Pros & Cons

- PROS:
  - Paper
  - Inexpensive verification device
  - Off-line verification
  - Cryptographically secure
  - Print, scan anywhere
- CONS:
  - Look-a-likes

Embed biometric info in barcode

Two Dimensional Barcode Design



Sample shown: 3,200 bits/400 bytes

- 1.2KB/inch^2
- No limits on size
- Triangular, 8 color symbology
- Built-in Reed-Solomon error correction
- Printed using ordinary color printer
- Uses computer vision techniques for decoding
- Scanned using 300dpi technology
  - – off-shelf business card readers, CCD matrices


ID# : 0123
Eyes: blue

Summary

- Face + iris + fingerprint = biometric ID
  - Microsoft barcode, OCR
- Passports, national IDs, driver's licenses
- As reliable as biometrics, as secure as cryptographic standards
- Inexpensive verification and ID creation
- Technology available for licensing

Part II: Counterfeit Resistant Optical Fibers

Main Contact: **Yuqun Chen**
E-mail: ***yuqunc@microsoft.com***

Motivation

- Billions of dollars are lost to counterfeiting each year
  - Microsoft's own estimate is $2 billion
  - Big problem in the drug industry
    - Safety issue
- Goal: Develop anti-counterfeiting labels that are
  - Very cheap to produce
  - Very difficult to counterfeit *en masse*
  - Superior to existing techniques (e.g., holograms)

Background: Certificate of Authenticity - COA

- Donald Bauder, Gustavus Simmons @ Sandia Labs
  - Count # of missiles during Cold War - 70s
  - Spray-paint epoxy on a nuclear warhead
  - Shed light from a certain angle
  - Take a picture of the reflection
- Paper-bill counterfeit deterrence
  - Again Bauder in the 80s

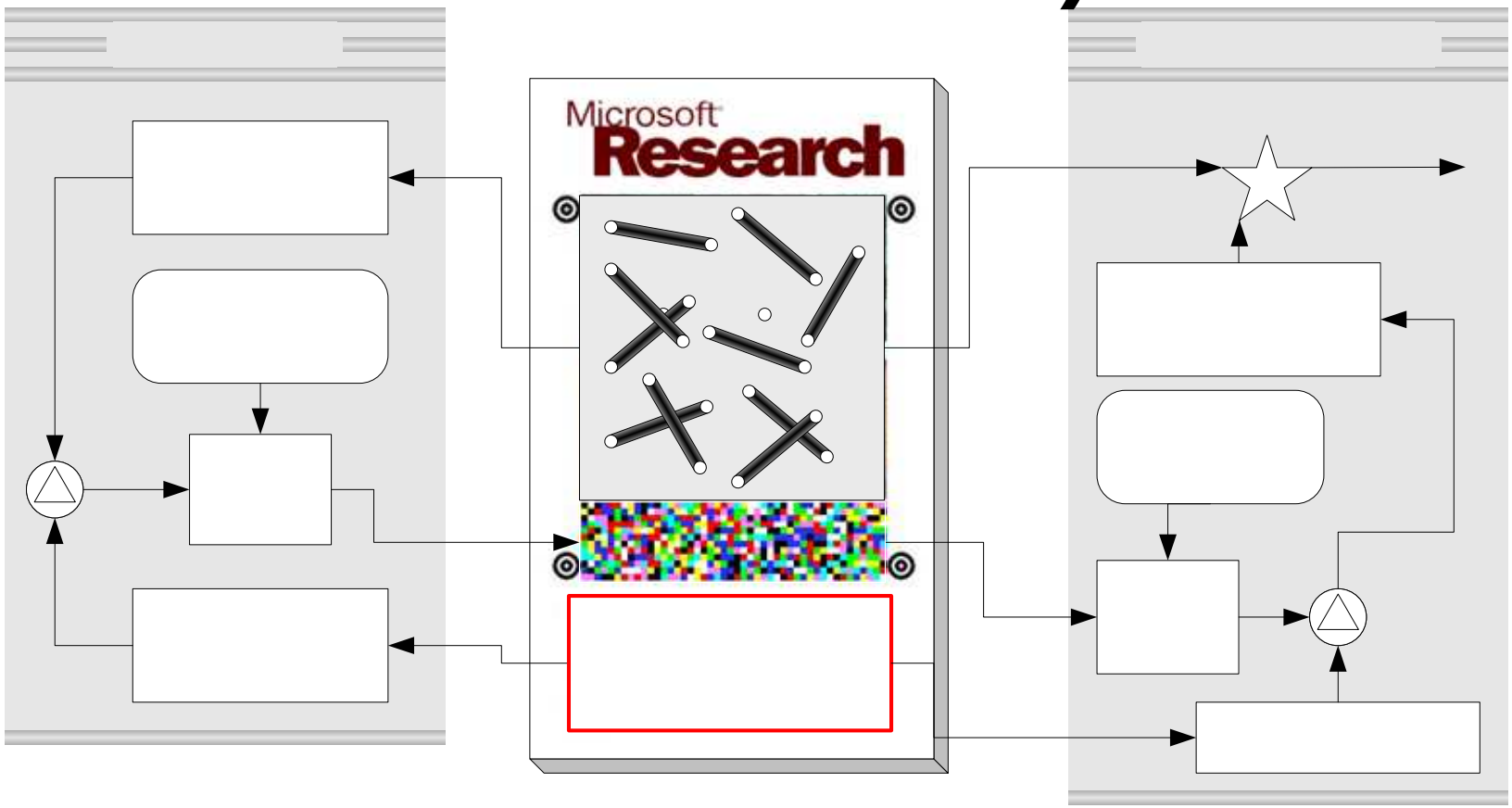
Requirements

- Physical object
  - Unique randomness
  - Expensive to create a near-exact replica
  - Inexpensive to manufacture
  - Inexpensive to scan the random structure
    - Inexpensive signing and verification
    - Sub-cents to single digit dollars per COA
  - Robust to wear and tear

Basic Idea

- Spread random optical fibers in a label
  - Initial concept proposed by Sandia in 70's
  - The substrate can be paper, plastic, or metal
  - Highly unforgeable
  - The pattern is unique to each label
- *Measure* the random fiber pattern
  - The unique pattern serves as a fingerprint
- Digitally sign the pattern thus obtained and print the signature on the label

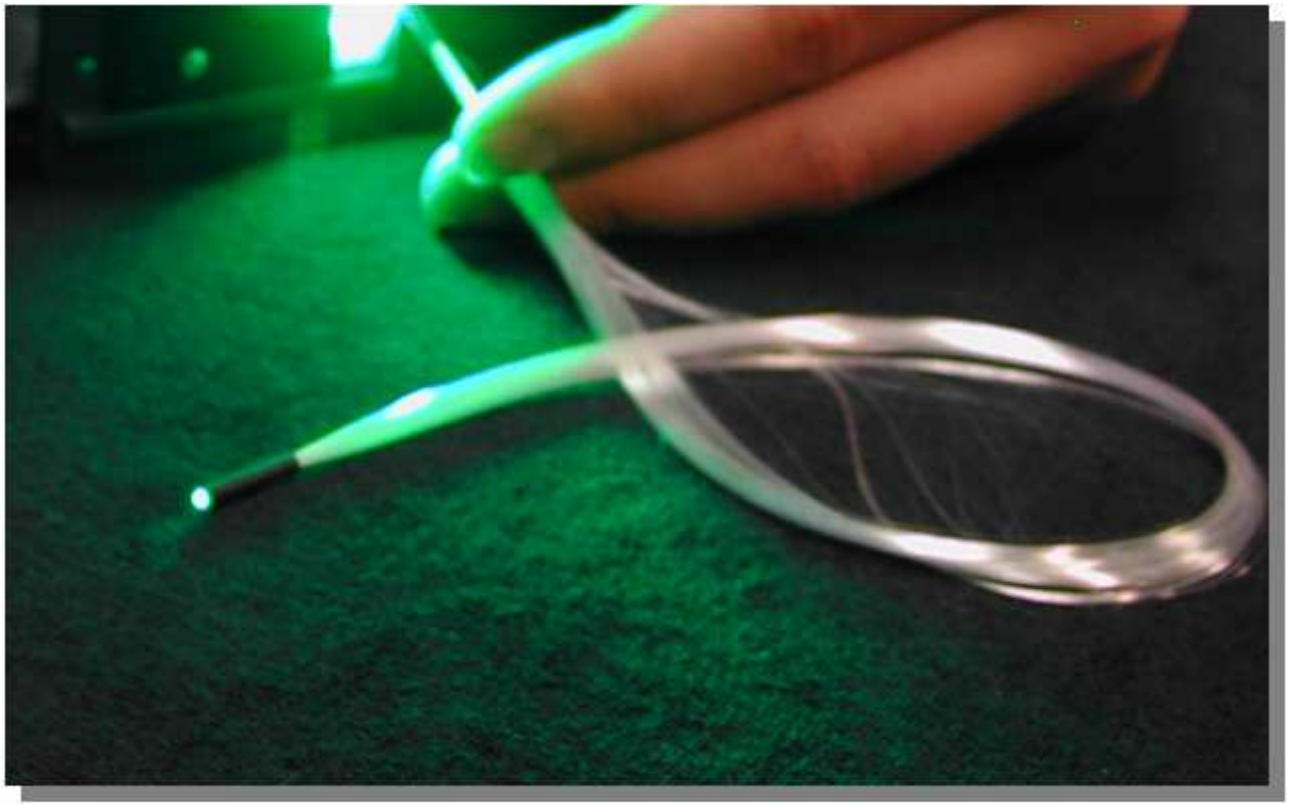
Issuing and Verifying COAs (Analogous to Tamper-Resistant Biometric IDs)



COA issuing

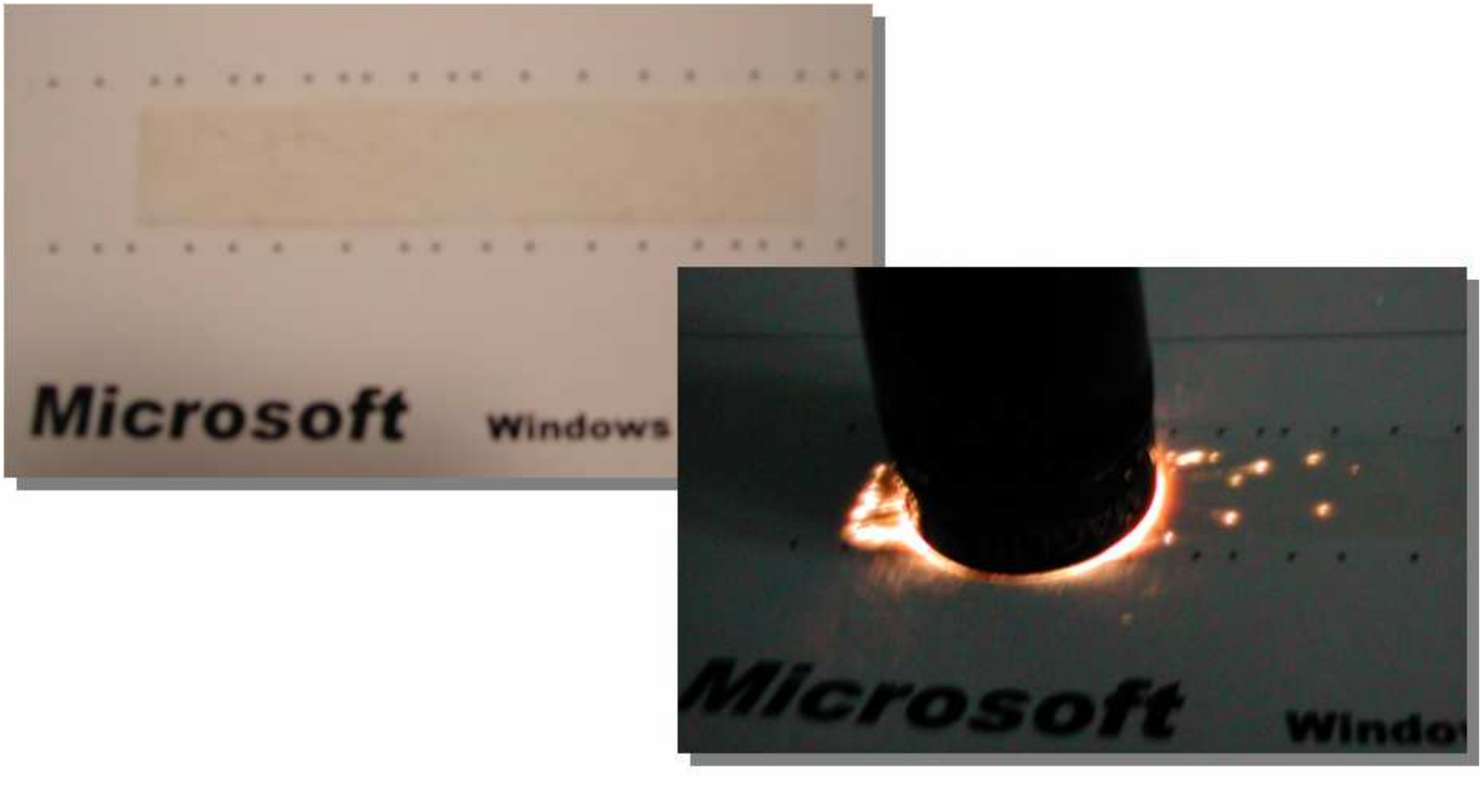
Optical Fibers

Can be extremely thin (a couple of microns)



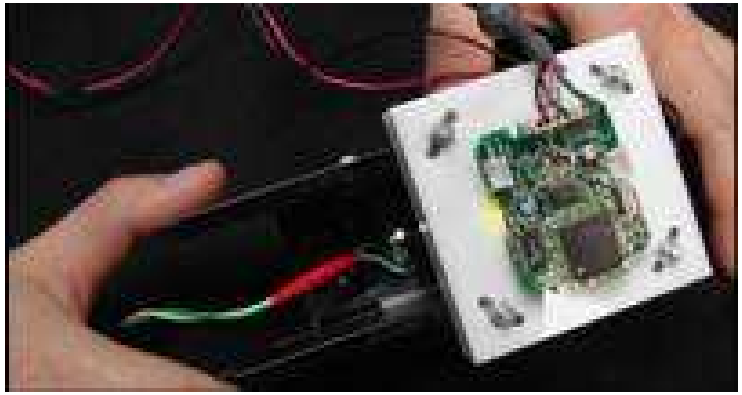
Embedding Fibers Within Labels

Presence of black dots essential for synchronization



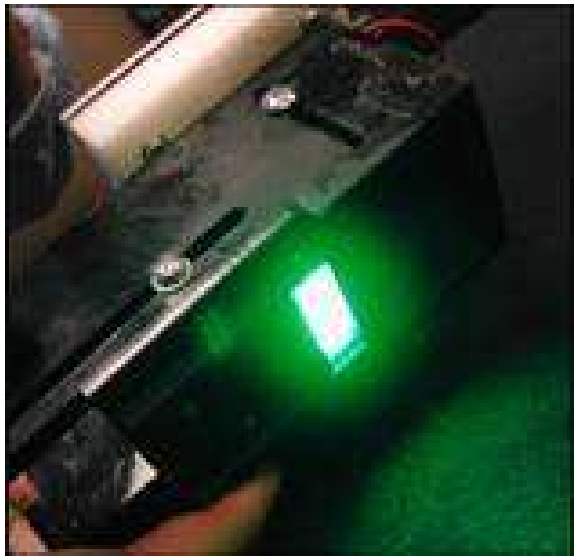
Scanner Specifications

Top view of scanner

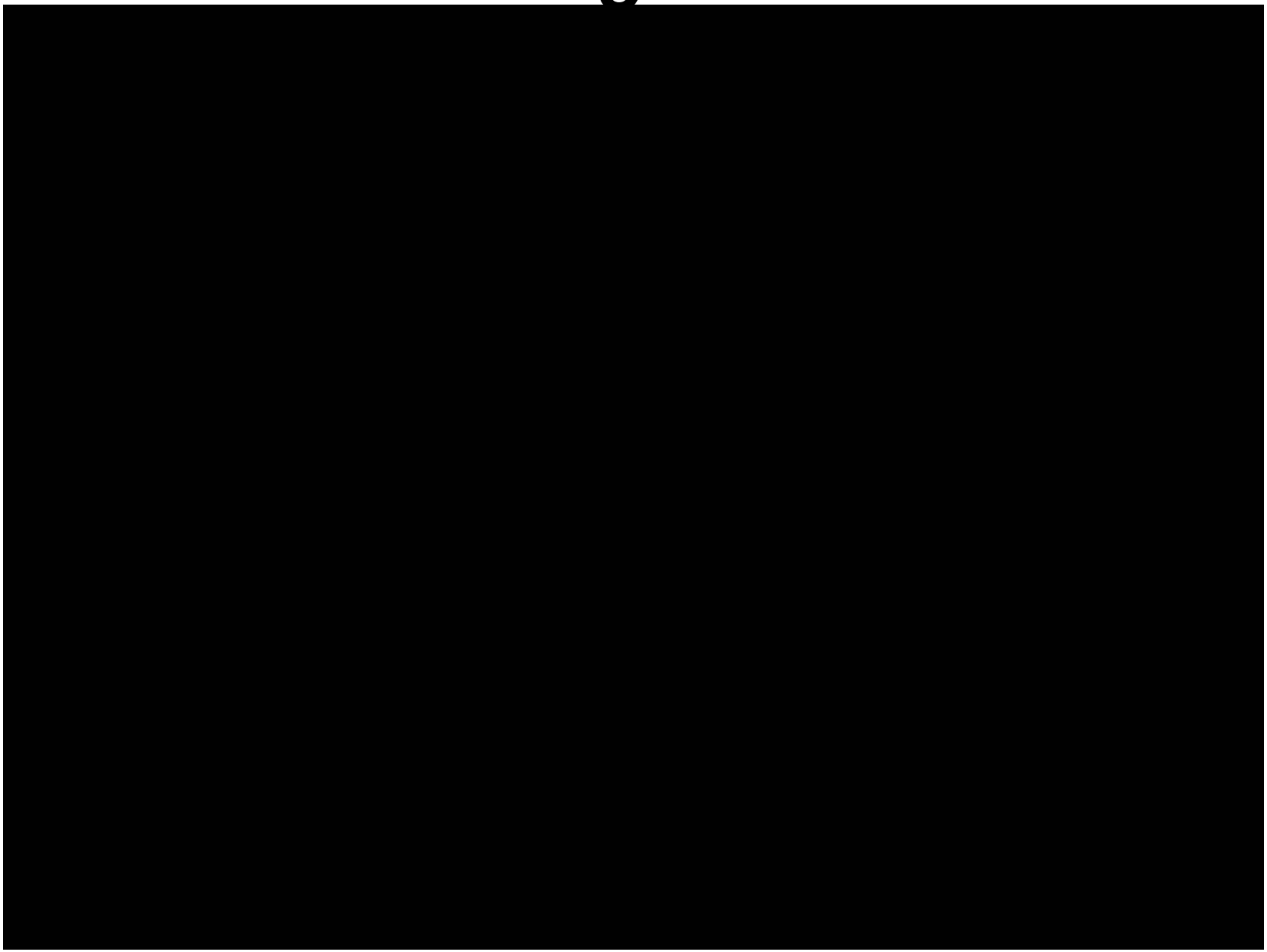


Imaging Chamber

Fiber Illumination Strip



Scanning A Label



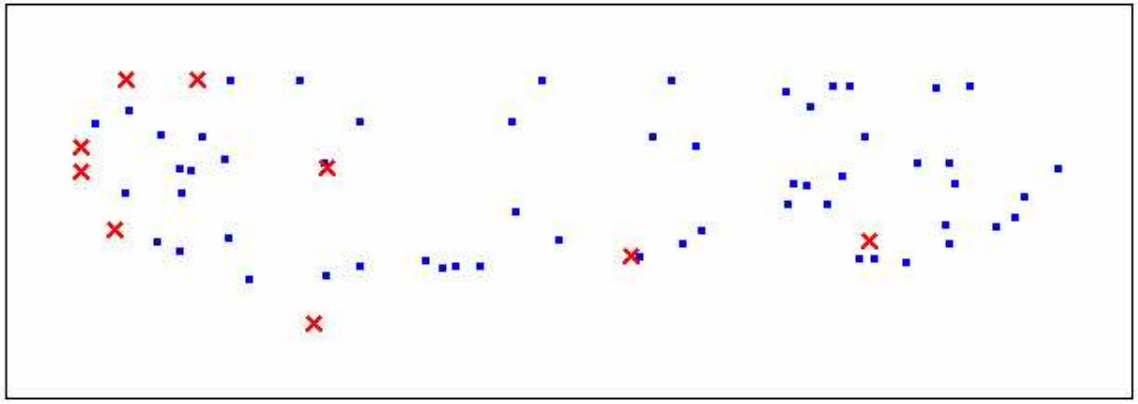
Processing After Image Capture

1. The captured image is analyzed; location of each fiber endpoint is identified
2. Captured image is *compressed* (lossless at a specified resolution)
3. Compression output is combined with contextual information (e.g., product ID codes)
4. The total data is *signed* with the private key of the issuer
5. Information is translated into a barcode or other machine readable format (e.g., RFID, magnetic strips)
6. Final output is sent to printer

Receiver Operation

Verification By Receiver

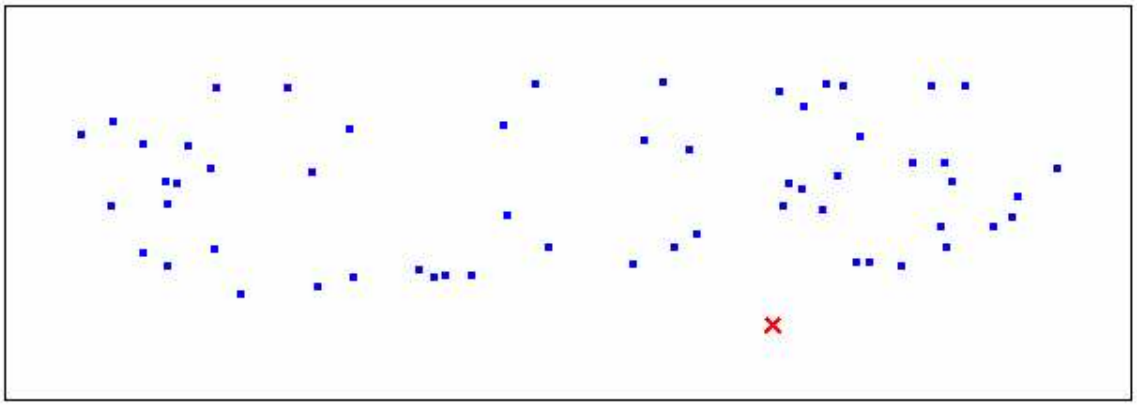
Scanned barcode



Fiber pattern stored in the barcode

Barcode Text : Windows XP, UK. C11-00036

Field Scan Match = 91.9%. ProductID is Valid. Label is Genuine !!



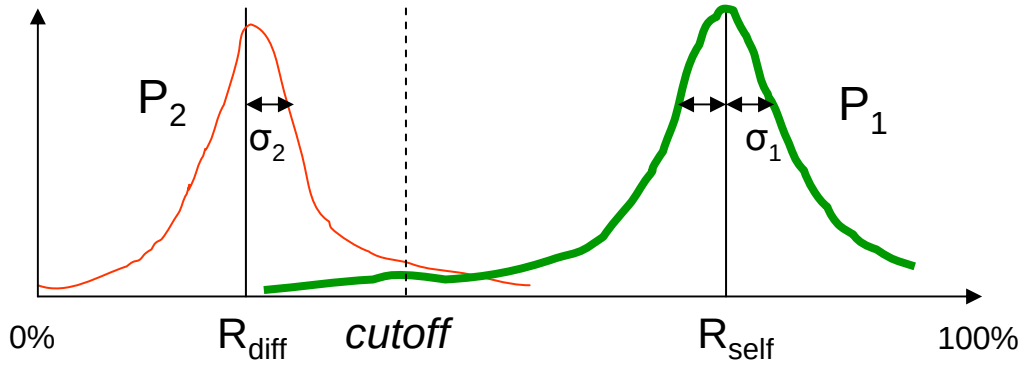
Fiber pattern scanned from the label

Attacks

- Exactly reproduce the fiber pattern
  - Physically hard
  - May be able to produce a mold to stamp thousands
  - But the each genuine label should have unique pattern
- Crack the secret key used to sign the pattern
  - Computationally infeasible given current technology

Error-rate Analysis

- Current results indicate a fairly wide separation between self correlation and cross correlation



P(false positive) = $P_2(x > \text{cutoff})$, P(false negative) = $P_1(x < \text{cutoff})$

Plug in some numbers based on our experiments

R_{diff}=12%, R_{self}=89%, $\sigma_1 = \sigma_2$ =5%, cutoff = 50%

Assuming normal distribution

false positive	≈	$1.5 * 10^{-14}$
false negative	≈	$5.6 * 10^{-23}$

Advantages

- Each label is unique due to random embedding
- Labels are relatively inexpensive to produce
- Re-producing the labels exactly is costly
  - Must place the ends of each fiber to exact locations
- Scanning & Printing fiber pattern is easy
  - Can tolerate fiber damage, wear and tear, etc.
- System cost is low
  - Estimated cost per scanner is $50 - $250

Some Issues

- A new manufacturing stage in producing the labels
  - Need to add a special scanner/printer (one-time investment)
  - It's probably easier to modify the plastic label machine to embed the fibers
- The bad guys may build special-purpose counterfeit machines
  - Carefully arrange the fibers to duplicate the pattern
  - Use special process to "print" fibers, for example, deposit two layers to plastic materials with different refractive indices
  - Costly but not impossible

Summary

- Exciting research challenges
  - Investigation of different materials and physical domains
  - Analysis of adversarial efforts
- Compression is crucial for cost-efficiency
- Label manufacturing is important from an industrial point of view
- Technology available for licensing

Part III: Joint Fragile and Robust Image Watermarking Against Content Forgery

Main Contact: **M. Kivanc Mihcak**
E-mail: ***kivancm@microsoft.com***

Problem

- Counterfeiting of physical contents (e.g., Microsoft products, currency, Yeni Raki)
- Current technique: Mostly relies on expertise of field investigators, assisted by conventional methods (e.g., holograms)
- Goal: A more reliable technique, that yields
  1. Information on content authenticity
  2. *Information on content origins for forensics analysis*

Proposed Approach

- Include a pictorial "*invisibly watermarked*" logo on physical products (paper, boxes, CD's, etc.)
- Embed identification data of the product ID (e.g., shipment information, customer ID), to be decoded reliably under printing & scanning *(robust image watermarking)*
- Tamper detection & attack classification if the examined item is forgery *(fragile image watermarking)*

Overview

- Resulting benefits
  - Quicker field tests on suspected products in warehouses
  - Determine if the product is forgery
  - Trace the origins
  - A tool for possible evidence in court
- Novelty in approach: Visual decoding possible
  - Human eye is a better decoder than most automated schemes
  - Allows field agents to develop their own forensics

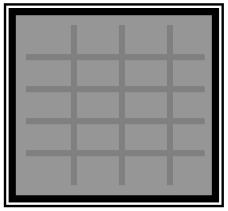
Problem Constraints

- Drastically different from conventional image watermarking (WM) scenario
- Small area logo (dime size, ~1/2 inch, ~40x40 image), large target bit rate for a small image (~40 bits)
- Only 32 gray levels allowed (limitations of CD printing)
- Would like to achieve “fragile” watermarking (FWM) and “robust” watermarking (RWM) at the same time
- FWM : Tamper detection & attack classification
- RWM : Embed ~40 bits, robust to printing & scanning, rotation, translation

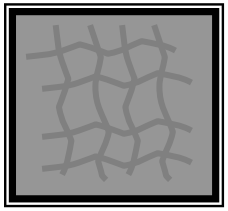
Fragile Watermarking

- FWM (Fragile Watermark)
  - Purpose: Reveal counterfeit attack, tamper evident
  - Collapse/deteriorate when copied or scanned
  - Collapse not visible to the human eye – watermark decoder analysis required to validate FWM presence
- Detection results
  - FWM in-tact = Genuine
  - FWM collapsed = Counterfeit

Genuine FWM



Counterfeit FWM



Robust Watermarking

- RWM (Robust Watermark)
  - Purpose: Carrier of the history of the examined item (version, sales office, shipment date, etc) – compressed ID embedded
  - Will **NOT** collapse/deteriorate when copied or scanned, under rotation, translation
  - **MAY** distinguish between counterfeit and genuine product
- Detection results
  - RWM will display ID on genuine
  - RWM will display ID on copied or scanned counterfeit product (traceability)
  - RWM will not display ID on artist rework by hand (tamper evident, but not traceable)

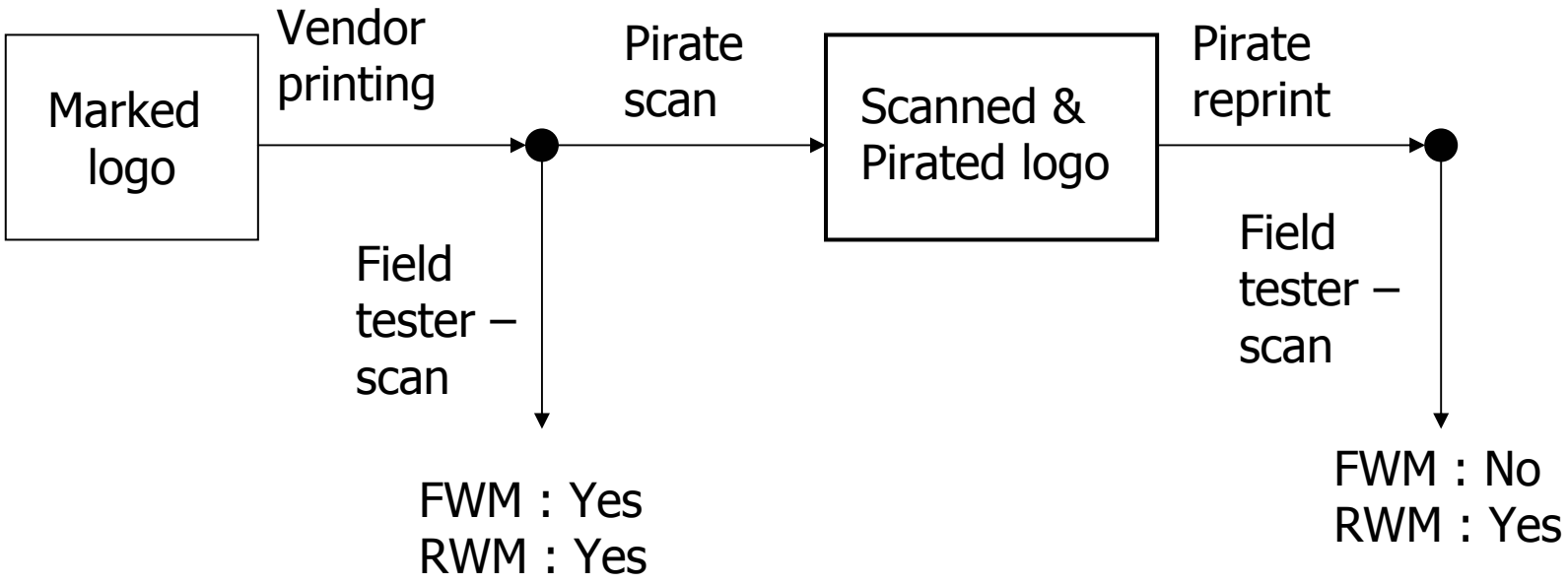
Genuine RWM

Counterfeit RWM

Counterfeit Attack Scenarios

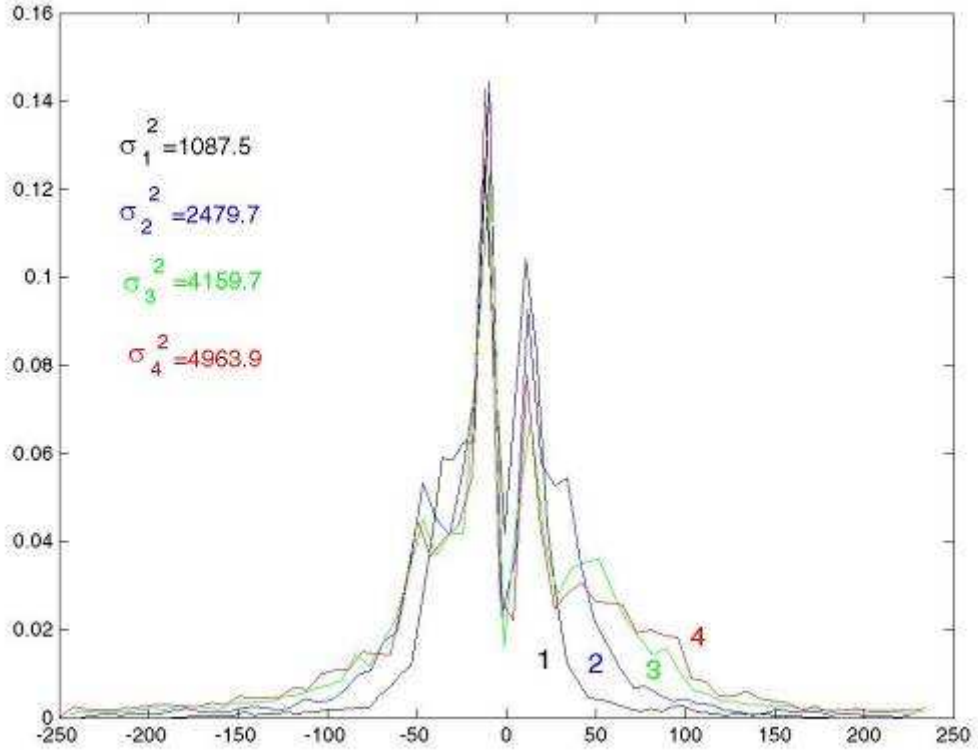
- **Scanning and reprinting**
  - Purchase genuine product
  - Scan artwork
  - Reprint artwork
  - Counterfeit visually identical to genuine
  - FWM gone, RWM remains
- **Artist rework**
  - Recreate artwork by hand
  - Touch up scanned copy to emulate original version
  - FWM gone, RWM also gone if recreated by hand
- **Greedy vendor :** Production more than allowed.
  - FWM is still there, but RWM yields info on origins of overproduced product (permitted max # for production)

Scan & Reprint Attack



Scanning & Reprinting Experiments

Histogram of difference between original and scanned



Scan & reprint once

Scan & reprint twice

Scan & reprint 3 times

Scan & reprint 4 times

Overview of Watermarking Approach

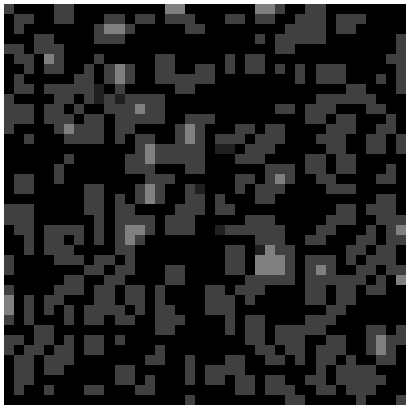
- Watermark w is pseudo-randomly generated, such that it is smooth and orthogonal to unmarked input s. Marked data x is sum of w and s.
- Perform ***visual*** decoding at the receiver: Linear mapping to a high dimensional space and use human eye to perform decoding.

Embedding Method

Original unmarked logo s

+

Watermark w



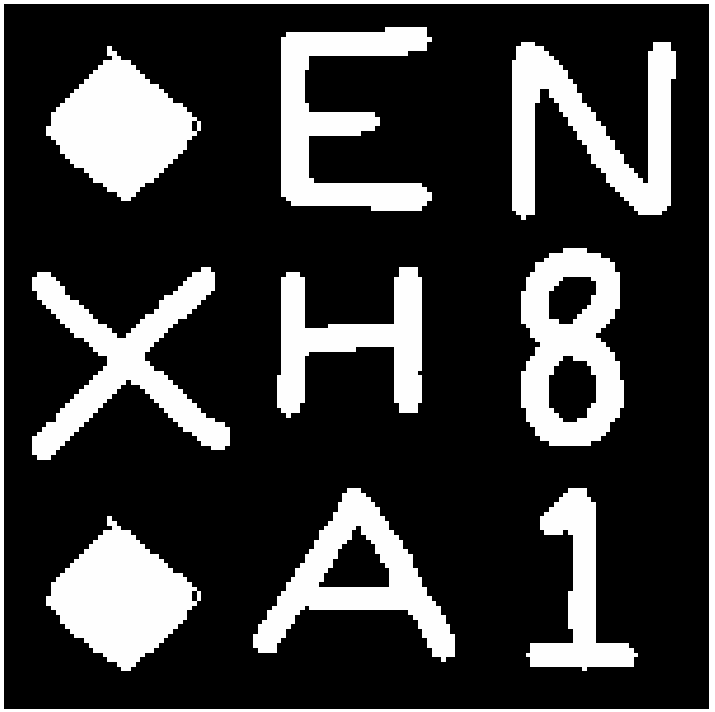
=

Marked logo x

- w pseudo-randomly generated
- $< s , w >=0$
- w smooth (projected to low frequency domain)

Decoding Method

Transform matrix T · Marked logo $\mathcal{X}$ = Visual decoder output Δ

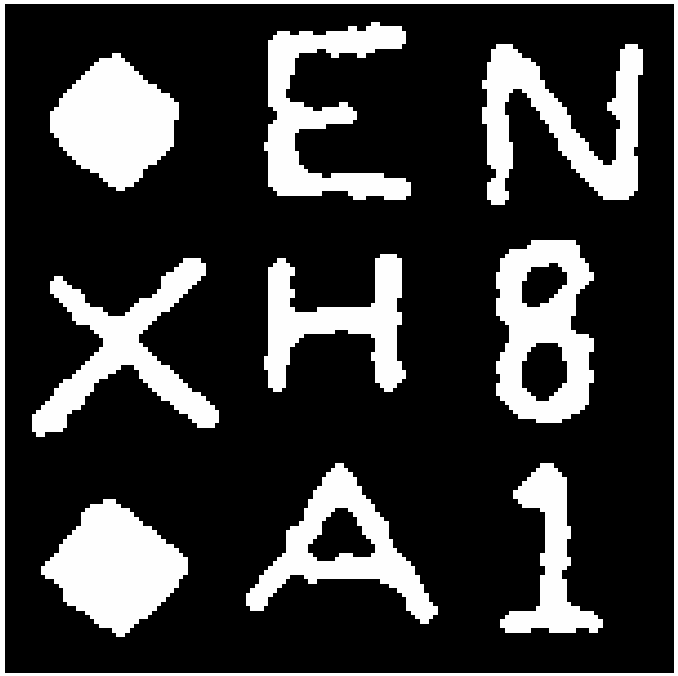


- T pseudo-randomly generated
- t^i : row i of T, Δ_i: i-th element of Δ
- $< t_i , s > = 0, < t_i , w > = \Delta_i$

Print-Scan Simulations

Initial decoder output

Decoder output after post-processing

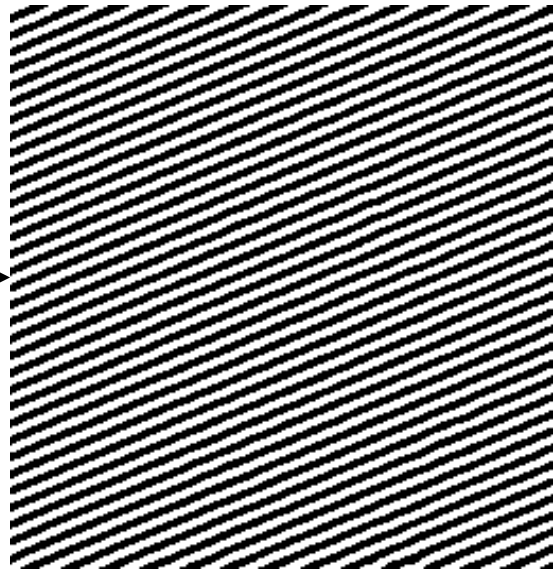


Solved Practical Problems – Undoing Rotation

Printed & scanned input

Carefully-chosen LSI filter applied

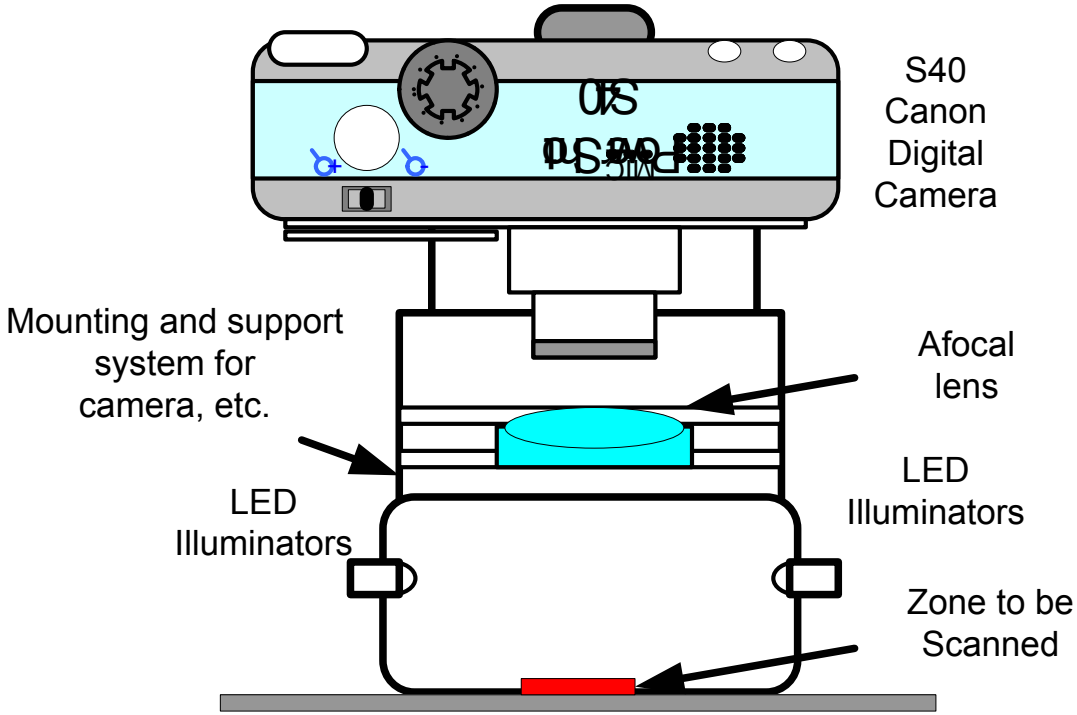
Filtered version



- Rotation angle can be accurately estimated using the filtered version and printer properties (e.g., printing angle)
- Original logo is not necessary for re-synchronization

PTI Detection Device

- Digital camera to scan and transfer data to decoder
- Mounting support system
  - Afocal lens to enable close-up focus
  - LED illuminators
- $600-800



Summary

- A new technique for authentication of physical products
- Joint fragile and robust watermarking for tamper evidence and traceability
- Main assumption: Pirates should not be able to produce a copy which is close to original
- Pro: Does not require fundamental changes in production chain
- Con: Weaker than counterfeit-resistant optical fibers for tamper evidence; may be defeated if pirates use a large number of logos