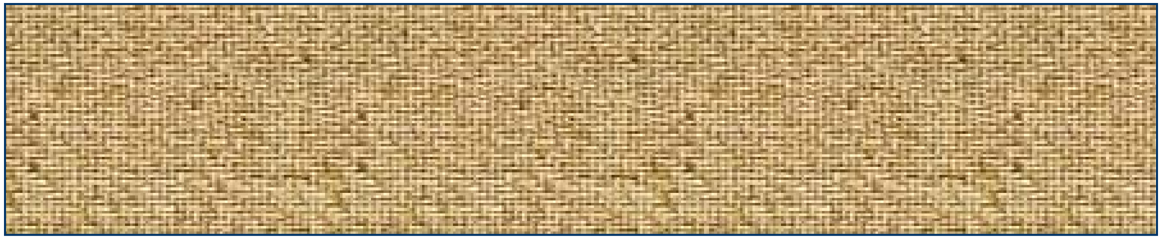
Anti-Counterfeit Labeling Method

Çetin Kaya Koç &
James Van Vechten

General Method

A label consists of two distinct parts:

- Unique Random Image: M
- Unique Product Signature: S



M

10101011101011001010110001001100111101010

S

About Unique Random Image

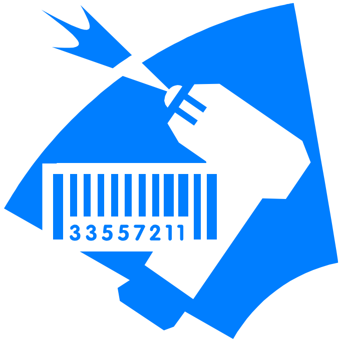
- Created using a controlled or random process
- Should be impossible to re-create the same image by scanning or copying
- Example 1: The way the silk threads are randomly distributed in US paper money creates a unique, unintentional, and irreproducible image
- Example 2: Dispersion of colored sand in plastic will also create an irreproducible image

About Unique Random Image

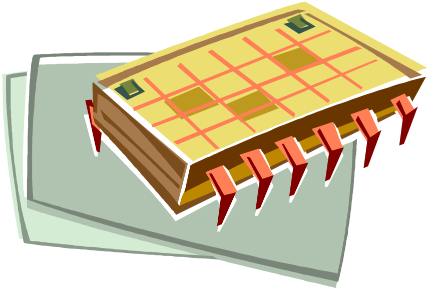
- After the image created on the label, it is scanned and encoded
- Encoding produces a number M which represents the image
- Size of the image does not need to be larger than a square centimeter; size of the number M is 20-100 bytes
- There are very efficient codes for robustly encoding such images (chain codes)
- Error-correcting codes can be used to add more resiliency

About Unique Label Signature

- A number S which is placed on the label or product
  - Barcode
  - Magnetic number
  - Printed number
  - Placed inside an RFID chip



0101101001 78593783937



Relationship of M and S

- M is the binary number representing the unique random image
- S is obtained from M using cryptographic techniques

S = SignatureFunction(M,privatekey)

Digital Signature Function

- SignatureFunction is a mathematical function taking M and another number, privatekey
- privatekey is known only to the owner, and is kept secure
- Only the owner can produce S given M since only the owner knows privatekey

Verification Process

- To verify, S is an authentic (true) signature of M, we need another function

  VerificationFunction(M,S,publickey)

- VerificationFunction is a mathematical function which takes 3 parameters
- M, S, and publickey are numbers
- The result is either YES or NO

Verification Process

VerificationFunction(M,S,publickey)

- YES means, M and S are authentic, S is produced by privatekey
- privatekey and publickey are mathematically related: privatekey produces S for M, and publickey verifies that S is authentic
- publickey is given to anyone who wishes to participate

Label Factory

- Makes the label
- Creates the Unique Random Image
- Encodes the image to obtain M
- Communicates M to Producer
- Receives S from the Producer
- Prints S on the label or on the product

Producer

- Makes the product
- Receives M from Label Factory
- Executes the SignatureFunction using the secret entity privatekey and M
- Obtains S
- Communicates S to Label Factory

Any Third Party

- Previously establishes the relationship with the Producer and obtains publickey
- Scans the Unique Random Image and obtains the encoding M
- Scans the Unique Product Signature and obtains S
- Executes VerificationFunction with M, S, and publickey: Result is YES or NO

Equipment Needs – Label Factory

- Manufacturing equipment to create the unique random images
- Optical scanner with encoding software to obtain M
- Internet connection to send M and receive S from Producer
- A 56kbit Internet connection can send and receive 28 signatures per second
- Printing or other methods place S on the label or on the product
- The cost of optical scanner with encoding software is about $100

Equipment Needs – Producer

- Internet connection to receive M and send S to Label Factory
- An ordinary PC with cryptographic software to execute SignatureFunction to obtain S
- The cost of such equipment and software is about $2000.

Equipment Needs – Third Party

- An optical scanner to obtain M and S from the product and label
- Cryptographic software inside the scanner to execute VerificationFunction with parameters M, S, and publickey
- Same scanner can hold thousands of different publickey values belonging to different vendors
- The total cost per scanner is probably around $200