EyeDecrypt — Private Interactions in Plain Sight

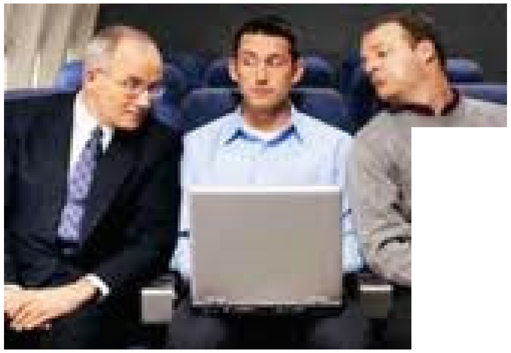
Andrea Forte , **Juan Garay** , **Trevor Jim** and **Yevgeniy Vahlis**

AT&T Security Research Center

at&t

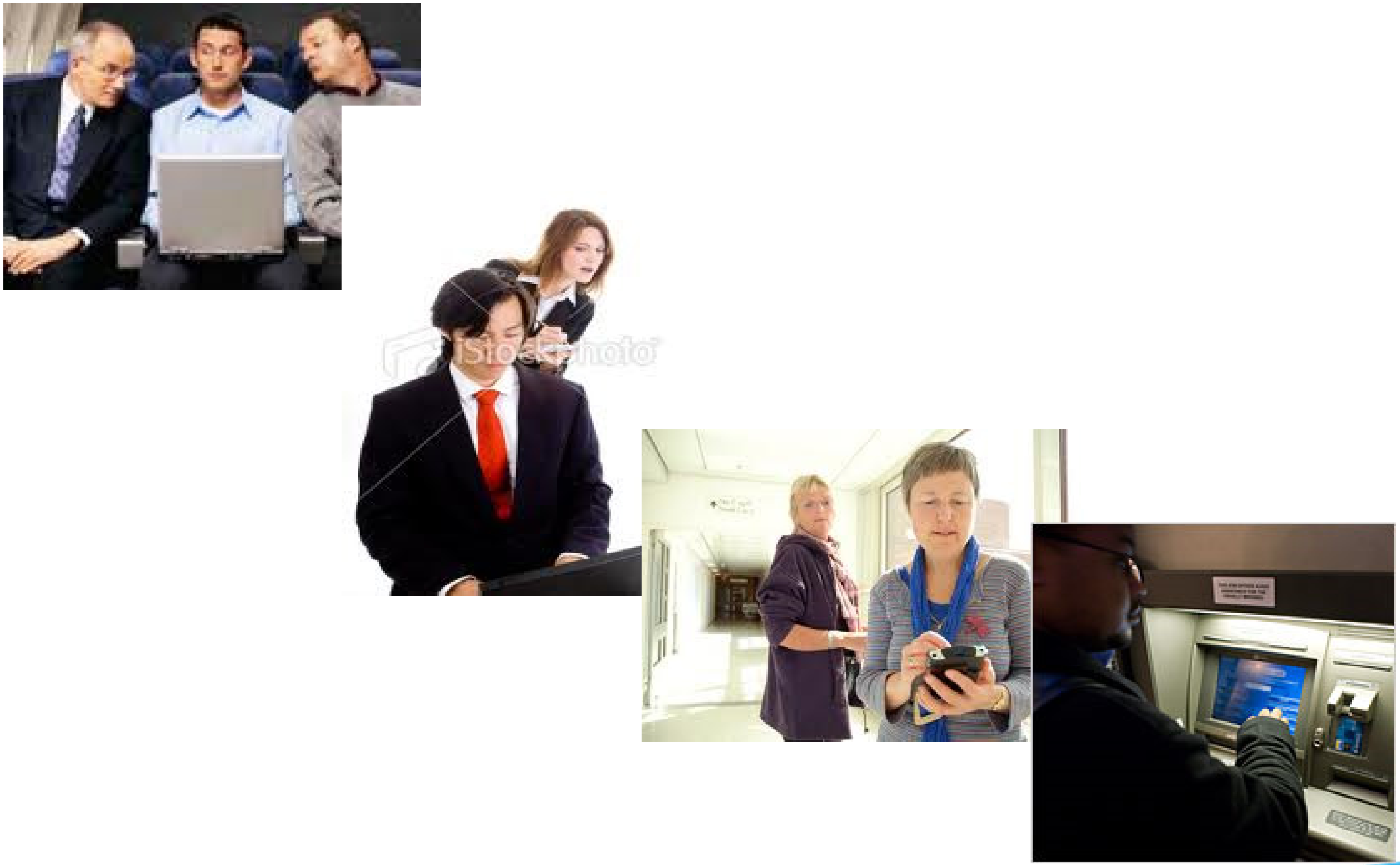
“Shoulder Surfing”

“Shoulder Surfing”



“Shoulder Surfing”

“Shoulder Surfing”



This Work: *EyeDecrypt*

- Content protection in new setting: *public-view* rendering device

This Work: *EyeDecrypt*

- Content protection in new setting: *public-view* rendering device
- Content can be stored/offline or dynamically captured (streaming)

This Work: *EyeDecrypt*

- Content protection in new setting: *public-view* rendering device
- Content can be stored/offline or dynamically captured (streaming)
- Two "modes" of operation:
  - Non-interactive (e.g., printed material, screen viewing)
  - Interactive (e.g., display + keyboard, gesticulation)

This Work: *EyeDecrypt*

- Content protection in new setting: *public-view* rendering device
- Content can be stored/offline or dynamically captured (streaming)
- Two “modes” of operation:
  - Non-interactive (e.g., printed material, screen viewing)
  - Interactive (e.g., display + keyboard, gesticulation)
- Three main components:
  - *EyeDecrypt* security definition
  - *Visualizable* encryption scheme
  - Visual encoding technique(s)

This Work: *EyeDecrypt*

- Content protection in new setting: *public-view* rendering device
- Content can be stored/offline or dynamically captured (streaming)
- Two “modes” of operation:
  - Non-interactive (e.g., printed material, screen viewing)
  - Interactive (e.g., display + keyboard, gesticulation)
- Three main components:
  - *EyeDecrypt* security definition
  - *Visualizable* encryption scheme
  - Visual encoding technique(s)

“For your eyes only!”

Model: Parties

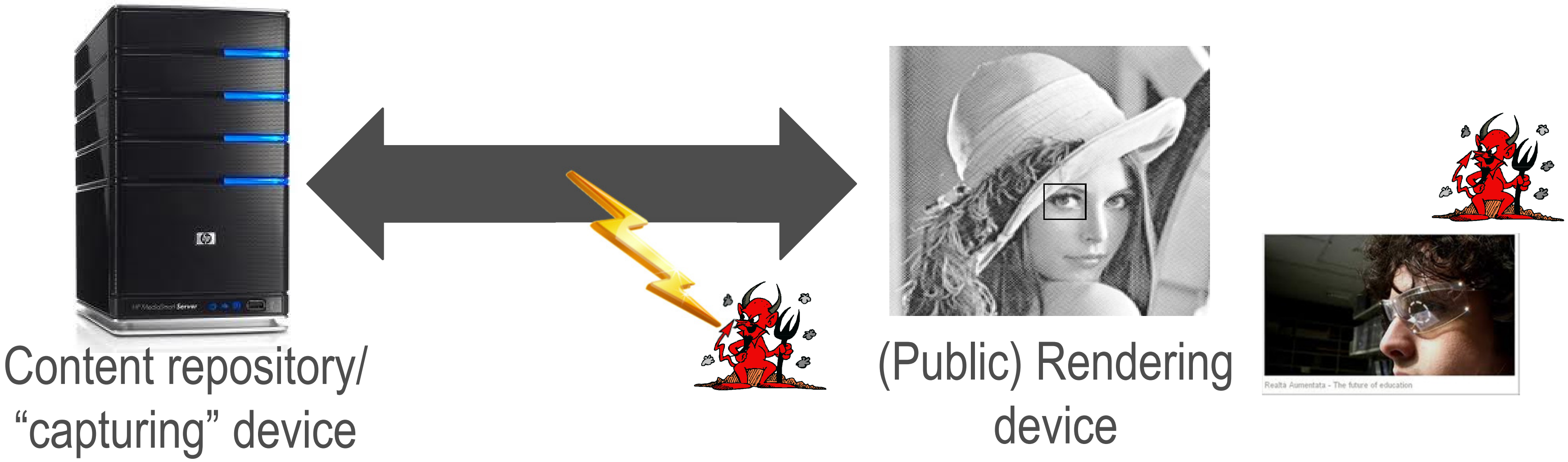
Server

Adv

Realta Aumentata - The future of education

User
(Viewing device)

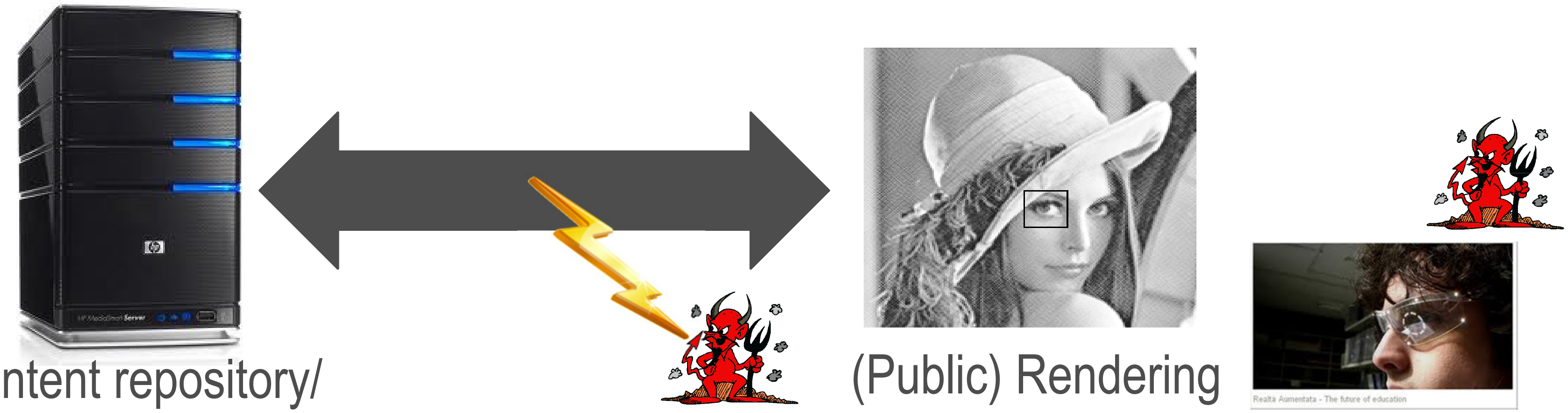
Model: Parties (cont’d)



Content repository/ “capturing” device

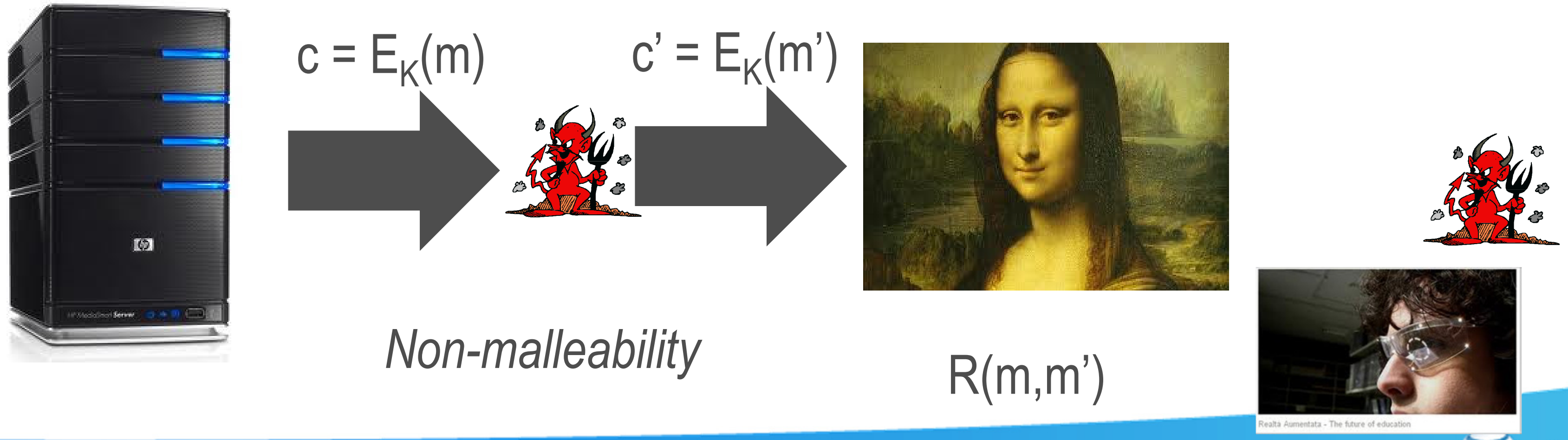
(Public) Rendering device

Model: Parties (cont’d)



Content repository/ “capturing” device

(Public) Rendering device



$c = E_K(m)$

$c' = E_K(m')$

Non-malleability

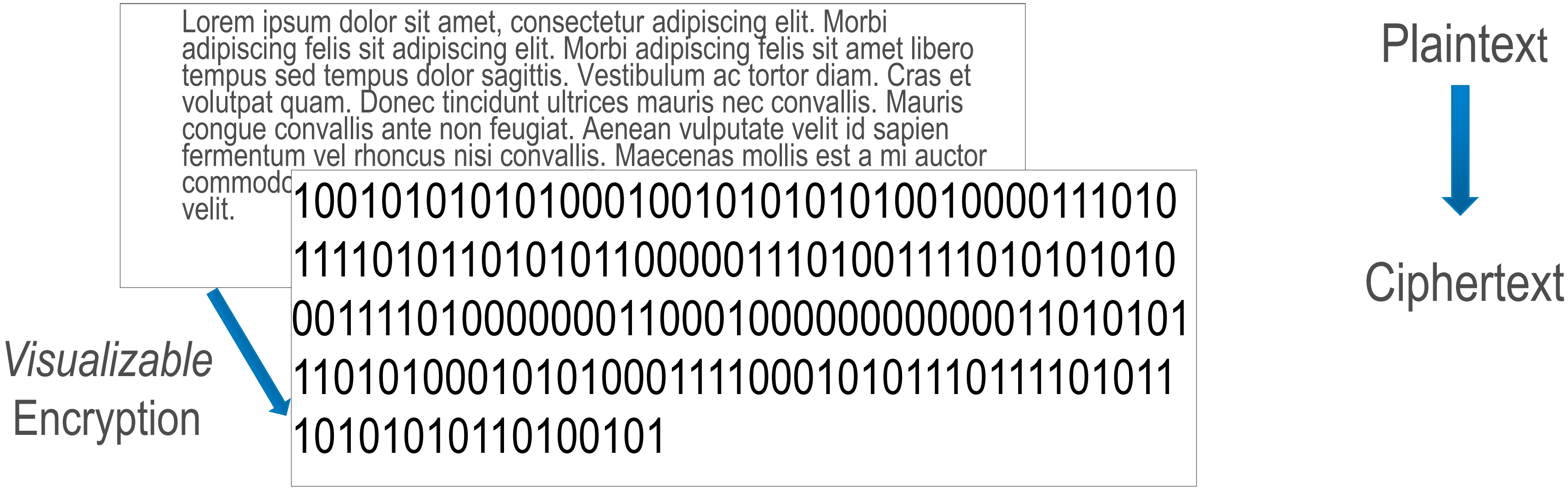
$R(m,m')$

EyeDecrypt in a Nutshell

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Morbi adipiscing felis sit adipiscing elit. Morbi adipiscing felis sit amet libero tempus sed tempus dolor sagittis. Vestibulum ac tortor diam. Cras et volutpat quam. Donec tincidunt ultrices mauris nec convallis. Mauris congue convallis ante non feugiat. Aenean vulputate velit id sapien fermentum vel rhoncus nisi convallis. Maecenas mollis est a mi auctor commodo. Vivamus sollicitudin eleifend. tincidunt. Phasellus vel varius velit.

Plaintext

EyeDecrypt in a Nutshell



Lorem ipsum dolor sit amet, consectetur adipiscing elit. Morbi adipiscing felis sit adipiscing elit. Morbi adipiscing felis sit amet libero tempus sed tempus dolor sagittis. Vestibulum ac tortor diam. Cras et volutpat quam. Donec tincidunt ultrices mauris nec convallis. Mauris congue convallis ante non feugiat. Aenean vulputate velit id sapien fermentum vel rhoncus nisi convallis. Maecenas mollis est a mi auctor commodo velit.

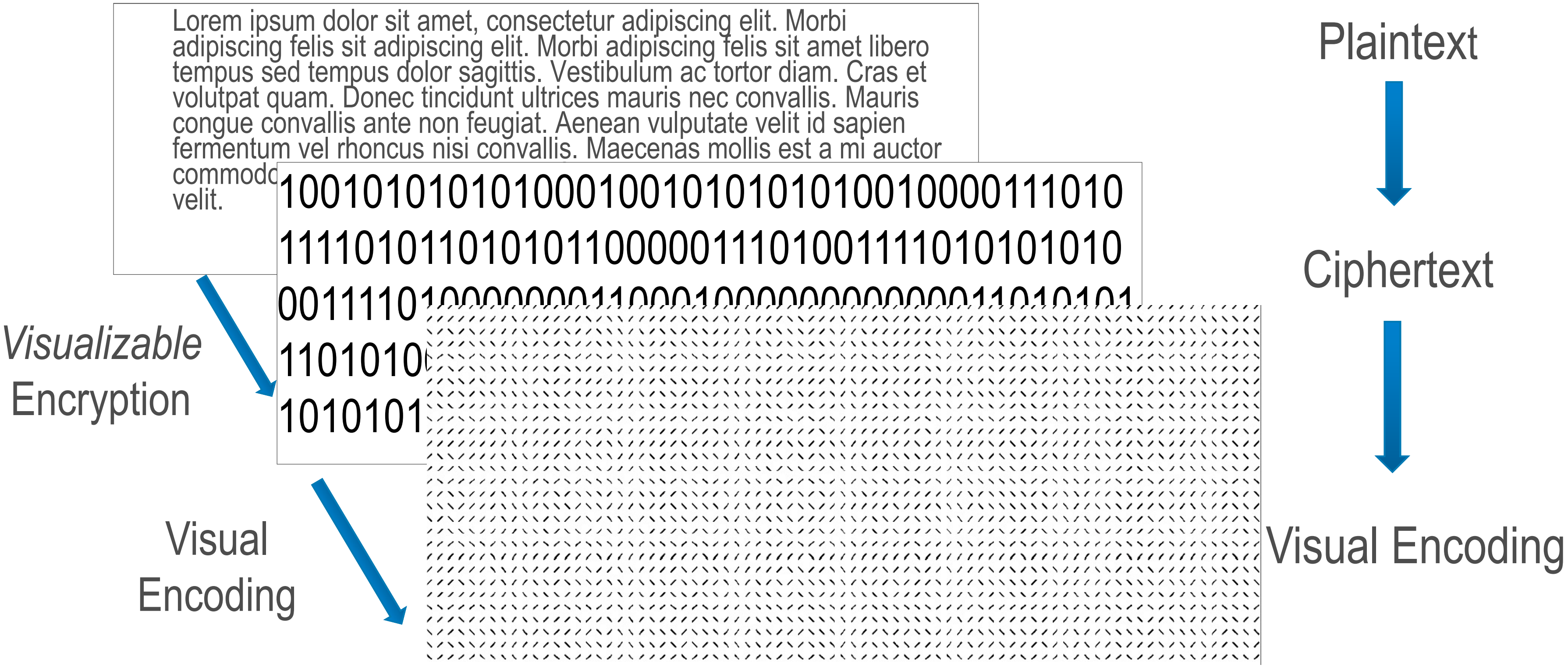
1001010101010001001010101010010000111010
11110101101010110000011101001111010101010
0011110100000000110001000000000000011010101
11010100010101000111100010101110111101011
10101010110100101

Visualizable
Encryption

Plaintext

Ciphertext

EyeDecrypt in a Nutshell



Lorem ipsum dolor sit amet, consectetur adipiscing elit. Morbi adipiscing felis sit adipiscing elit. Morbi adipiscing felis sit amet libero tempus sed tempus dolor sagittis. Vestibulum ac tortor diam. Cras et volutpat quam. Donec tincidunt ultrices mauris nec convallis. Mauris congue convallis ante non feugiat. Aenean vulputate velit id sapien fermentum vel rhoncus nisi convallis. Maecenas mollis est a mi auctor commodc velit.

```
1001010101010001001010101010010000111010
11110101101010110000011101001111010101010
0011110100000000110001000000000000011010101
1101010
1010101
```

Visualizable Encryption

Visual Encoding

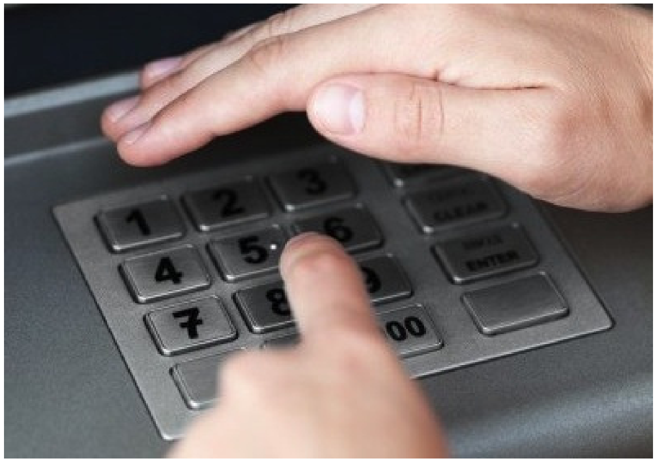
Plaintext

Ciphertext

Visual Encoding

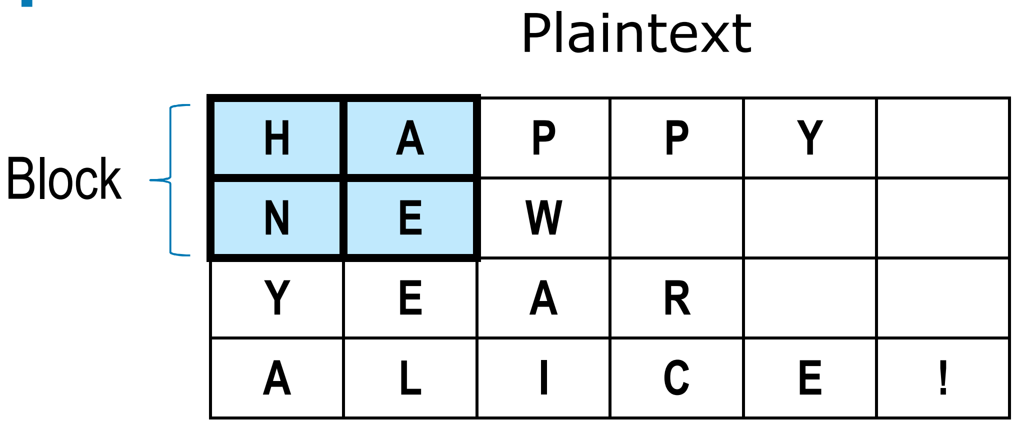
Defining *EyeDecrypt*'s Security

- **Important:** Encryption ***does not*** (on its own) make new application secure — solve shoulder surfing in our case
- Attacker can still see the buttons that the user presses, gestures, eye movement,…
- Security is defined with respect to a function *Leak* that determines, at each step, the information learned by Adv



A Visualizable Encryption Scheme

- Plaintext space is a matrix of text (for example)



Plaintext

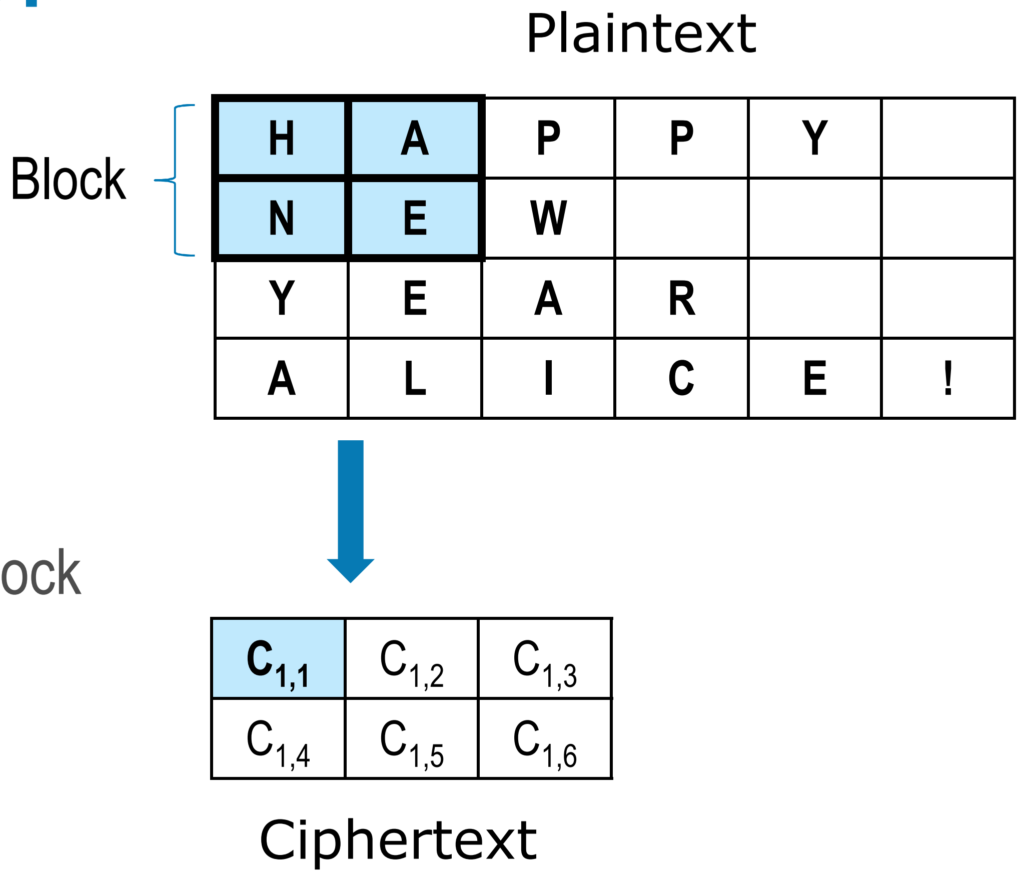
Block

H	A	P	P	Y	
N	E	W			
Y	E	A	R		
A	L	I	C	E	!

A Visualizable Encryption Scheme

- Plaintext space is a matrix of text (for example)

- Encryption is performed per block



Plaintext

Block

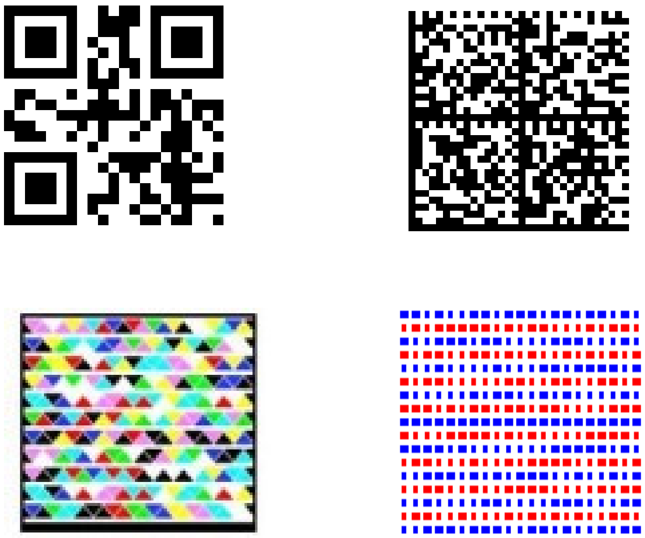
H	**A**	**P**	**P**	**Y**	
N	**E**	**W**			
Y	**E**	**A**	**R**		
A	**L**	**I**	**C**	**E**	**!**

$\mathbf{C_{1,1}}$	$C_{1,2}$	$C_{1,3}$
$C_{1,4}$	$C_{1,5}$	$C_{1,6}$

Ciphertext

Visual Encoding

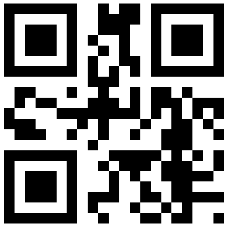
- Many existing visual encoding solutions: QR codes, Data Matrix, HCCB,…
- Most require capturing the entire encoding

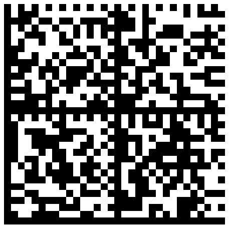


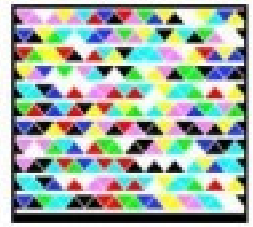
Visual Encoding

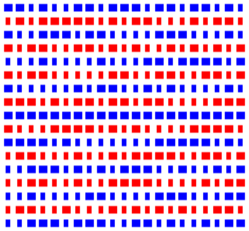
- Many existing visual encoding solutions: QR codes, Data Matrix, HCCB,…
- Most require capturing the entire encoding
- We require:
  - *Locality* – cropped encoding decodes to sub-matrix of input
  - *Relative positioning* – adjacent input sub-matrixes are adjacent in encoded image

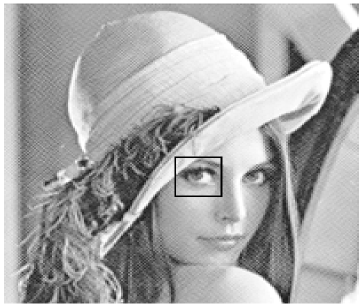
→ ***Dataglyphs***

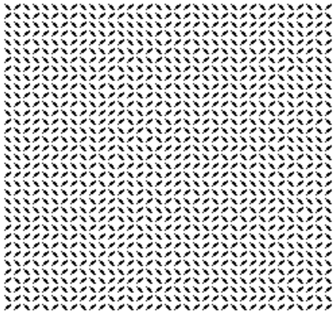








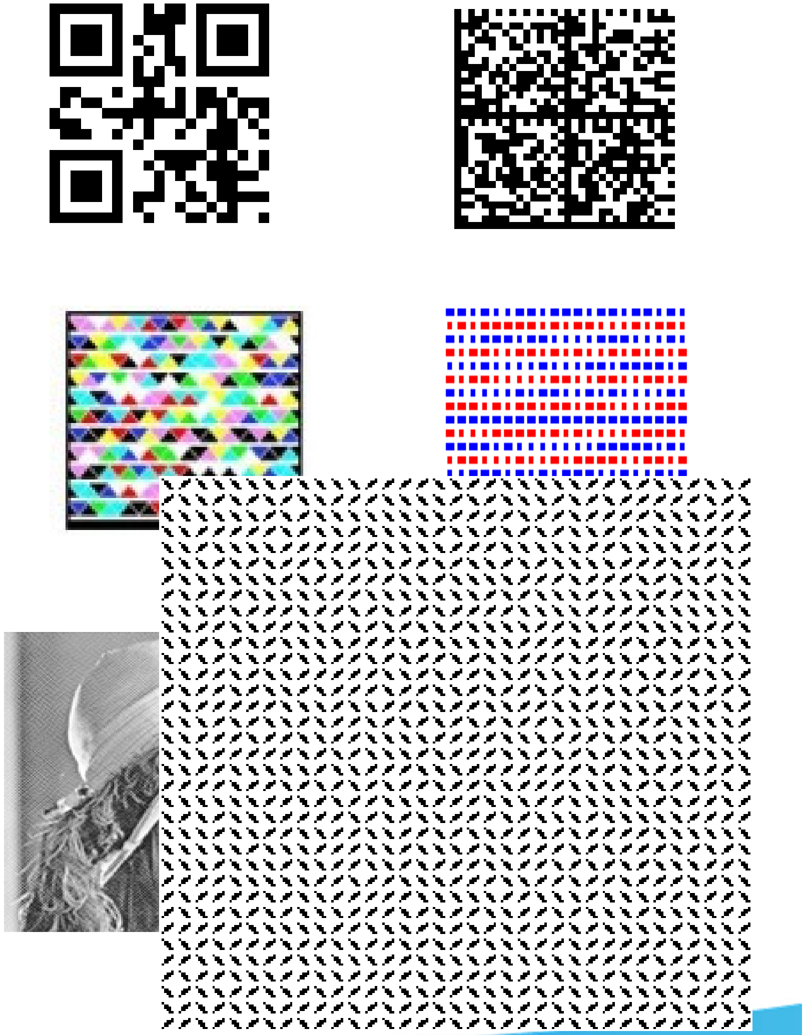




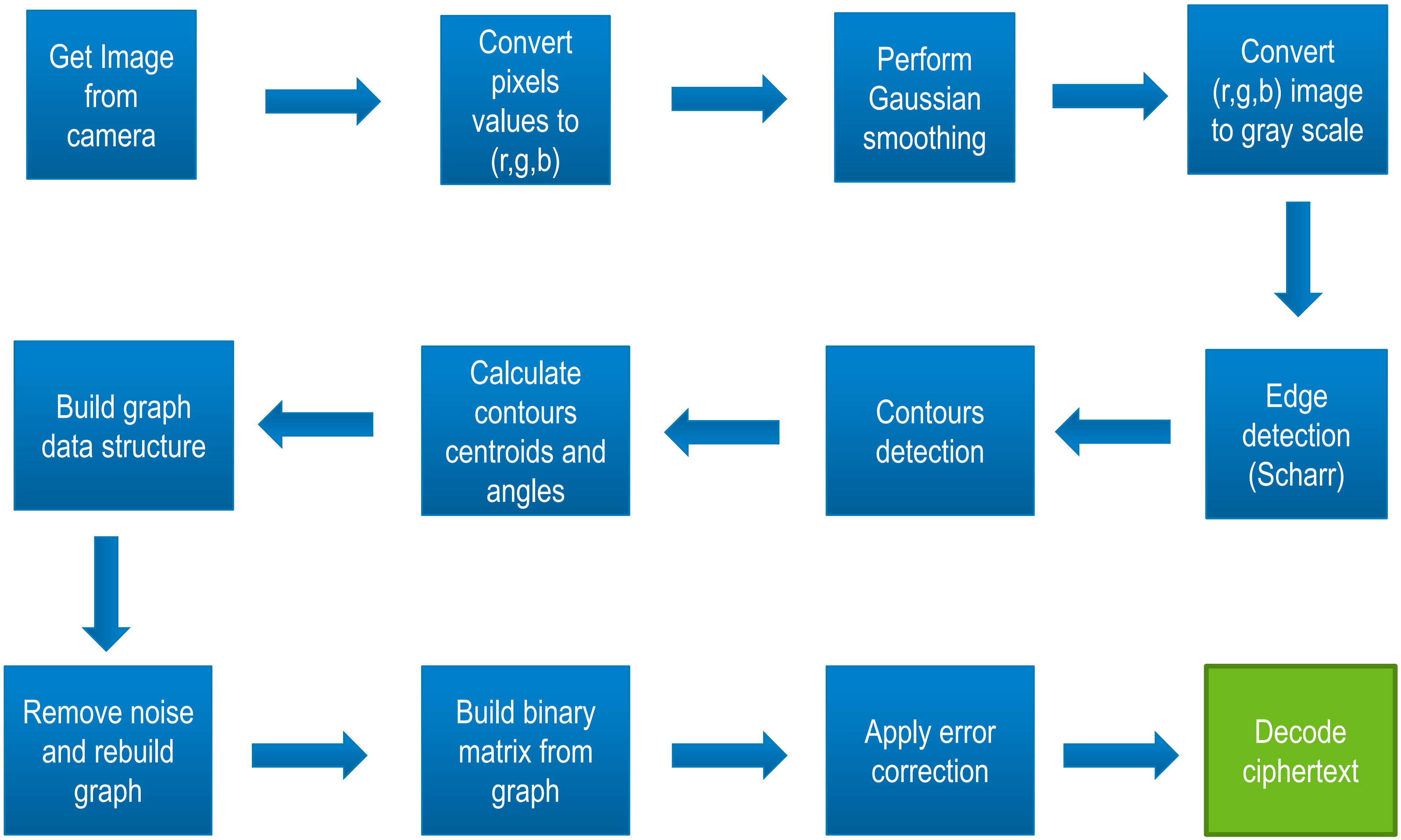
Visual Encoding

- Many existing visual encoding solutions: QR codes, Data Matrix, HCCB,…
- Most require capturing the entire encoding
- We require:
  - *Locality* – cropped encoding decodes to sub-matrix of input
  - *Relative positioning* – adjacent input sub-matrixes are adjacent in encoded image

→ ***Dataglyphs***



Visual Decoding Steps



Get Image from camera

Convert pixels values to (r,g,b)

Perform Gaussian smoothing

Convert (r,g,b) image to gray scale

Edge detection (Scharr)

Contours detection

Calculate contours centroids and angles

Build graph data structure

Remove noise and rebuild graph

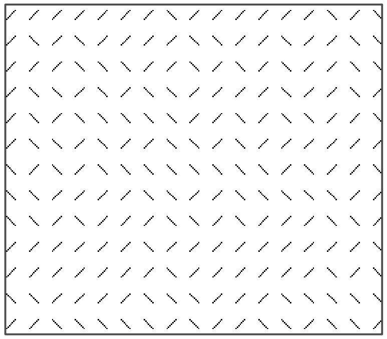
Build binary matrix from graph

Apply error correction

Decode ciphertext

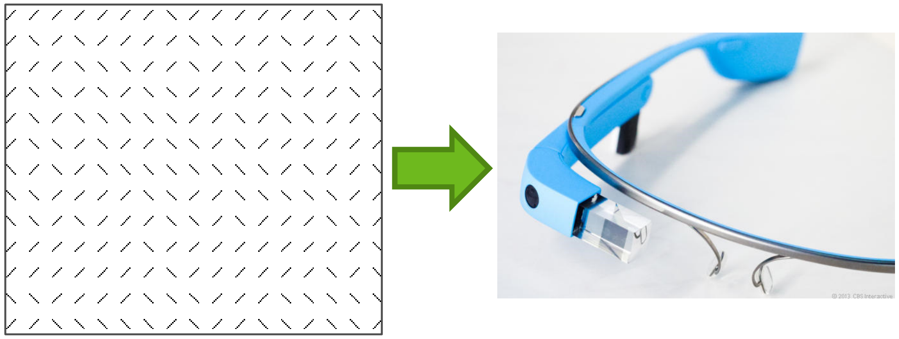
Instantiating EyeDecrypt: Secure PIN Entry

- Aka: Randomized keypad



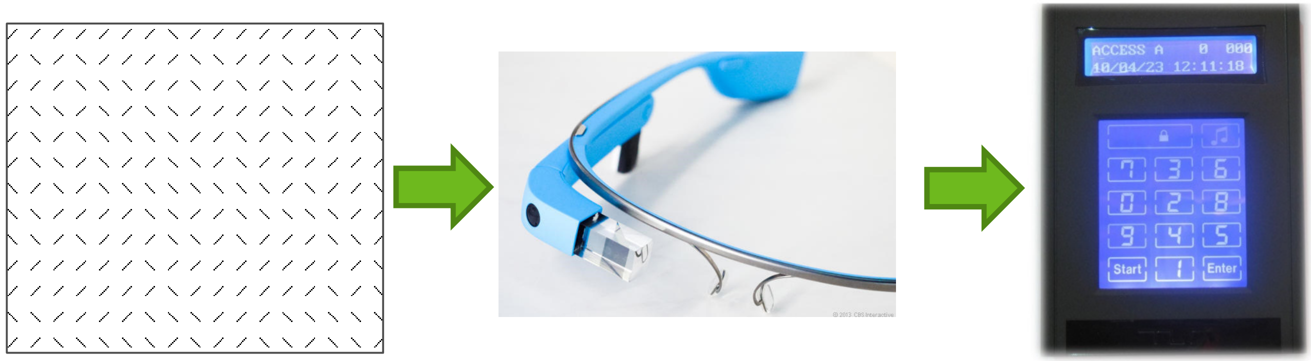
Instantiating EyeDecrypt: Secure PIN Entry

- Aka: Randomized keypad



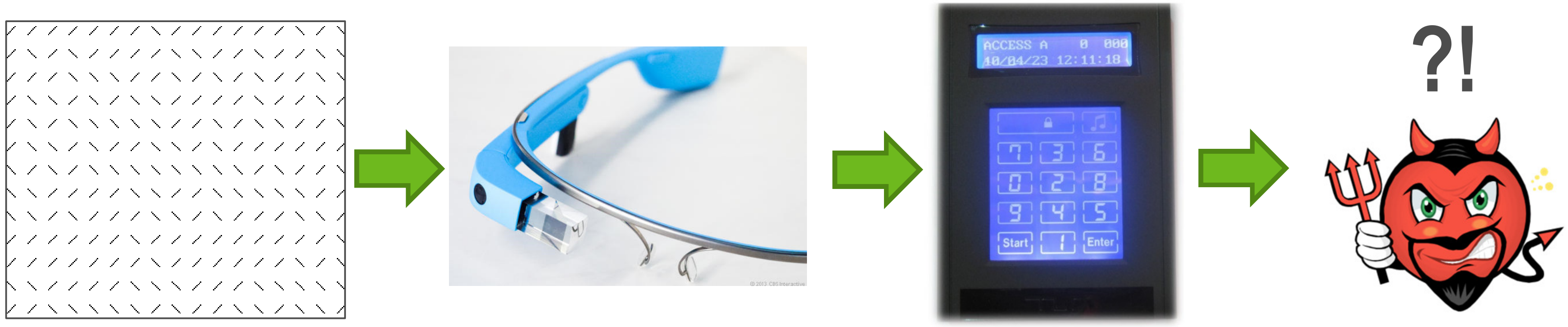
Instantiating EyeDecrypt: Secure PIN Entry

- Aka: Randomized keypad

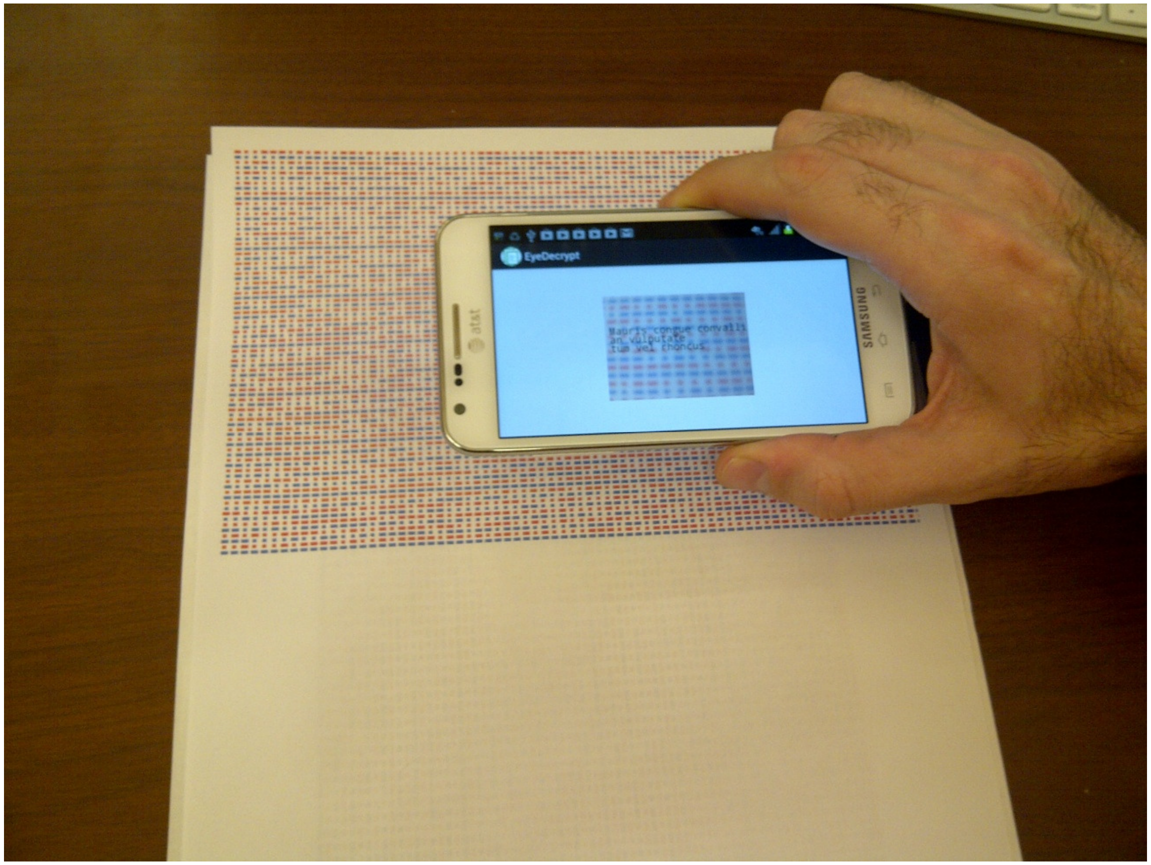


Instantiating EyeDecrypt: Secure PIN Entry

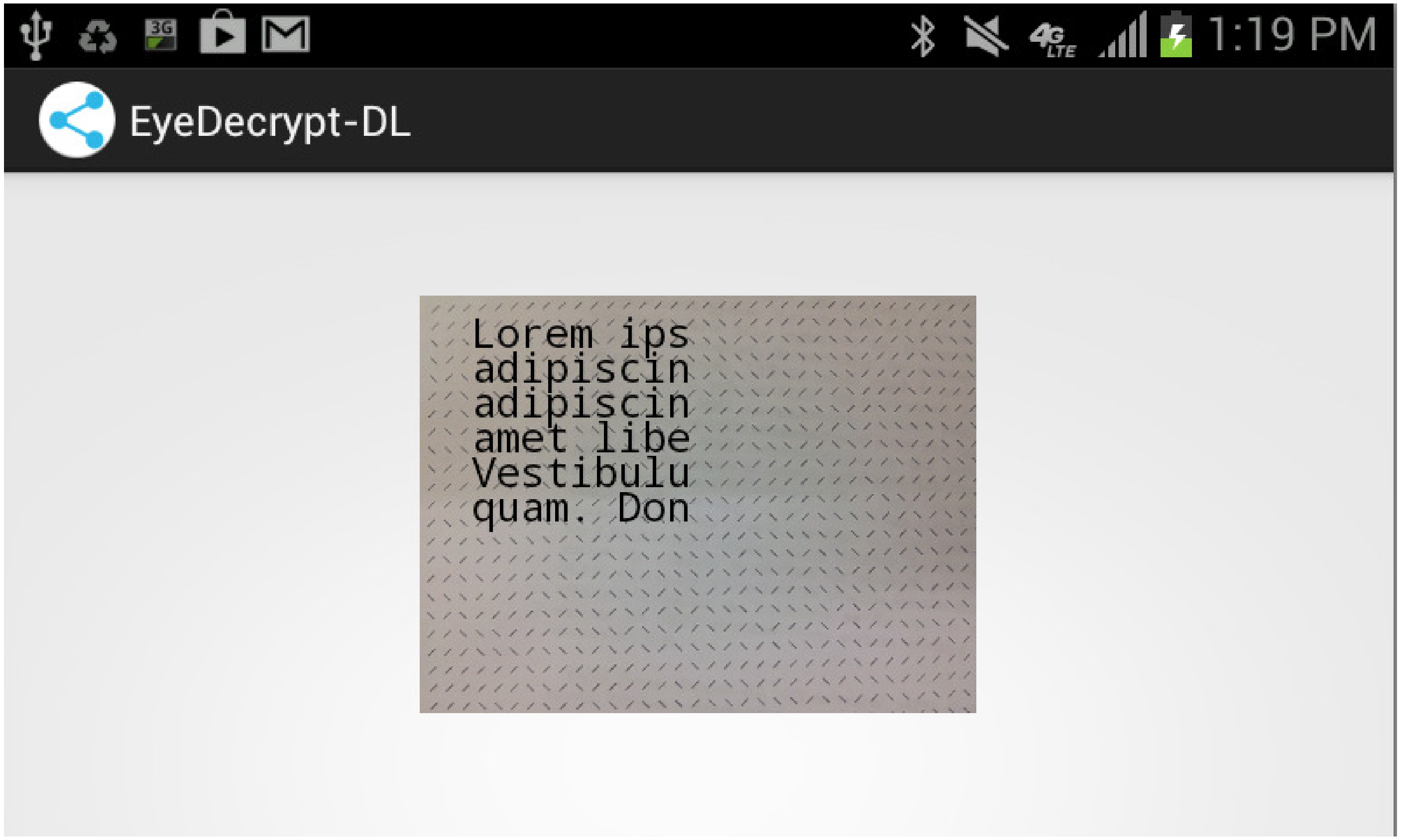
- Aka: Randomized keypad



Implementation



Implementation (cont'd)



```
Lorem ips
adipiscin
adipiscin
amet libe
Vestibulu
quam. Don
```

Thanks!