Cover Synthesis Steganography with Cellular Automatons

Neil Babson

The Plan

The encrypted message is used as a rule to generate a cellular automaton.

A four state neighborhood seven cellular automaton has a rule of length 4^7.

Each element of the rule is a two bit value from 0 to 3.

Therefore 2^{14} / 4 = 4 K bytes of information can be stored in an image.

The first eight spaces of the rule are reserved as a header to record the message length.

Eight state CAs could be used that store a byte per rule element.

enc - encrypt a plain text message (from HW 1)

embed - embed a message in a CA rule -

draw - draw a CA from a ca.txt file and save to ppm 3 file

makeCA - create a CA from a rule and call **draw**

extractRule - extract a CA rule from a ppm 3 file

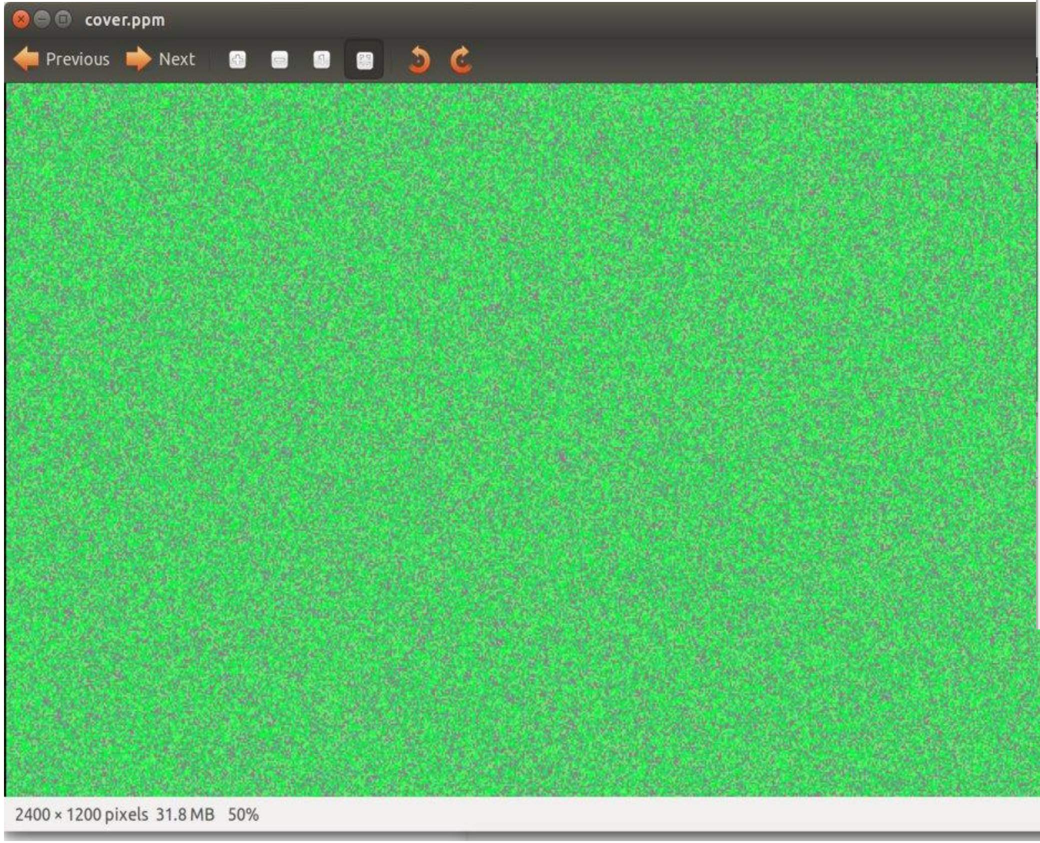
extract - extract a message from a CA rule

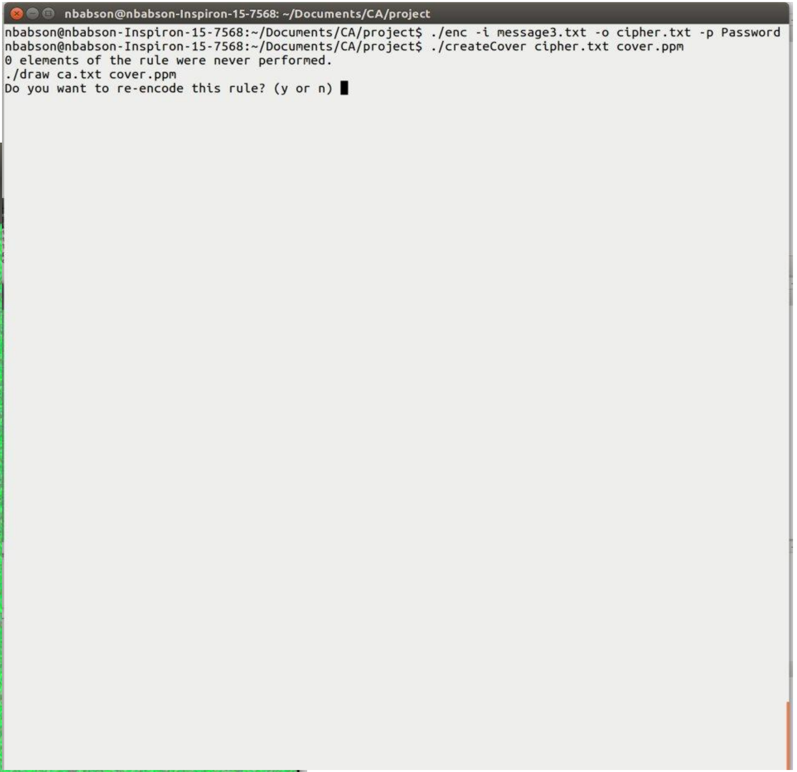
dec - decrypt cipher text message (from HW 1)

createCover - call **embed** and **makeCA** to synthesize new image

recoverMessage - call **extractRule** and **extract** to get message from an image

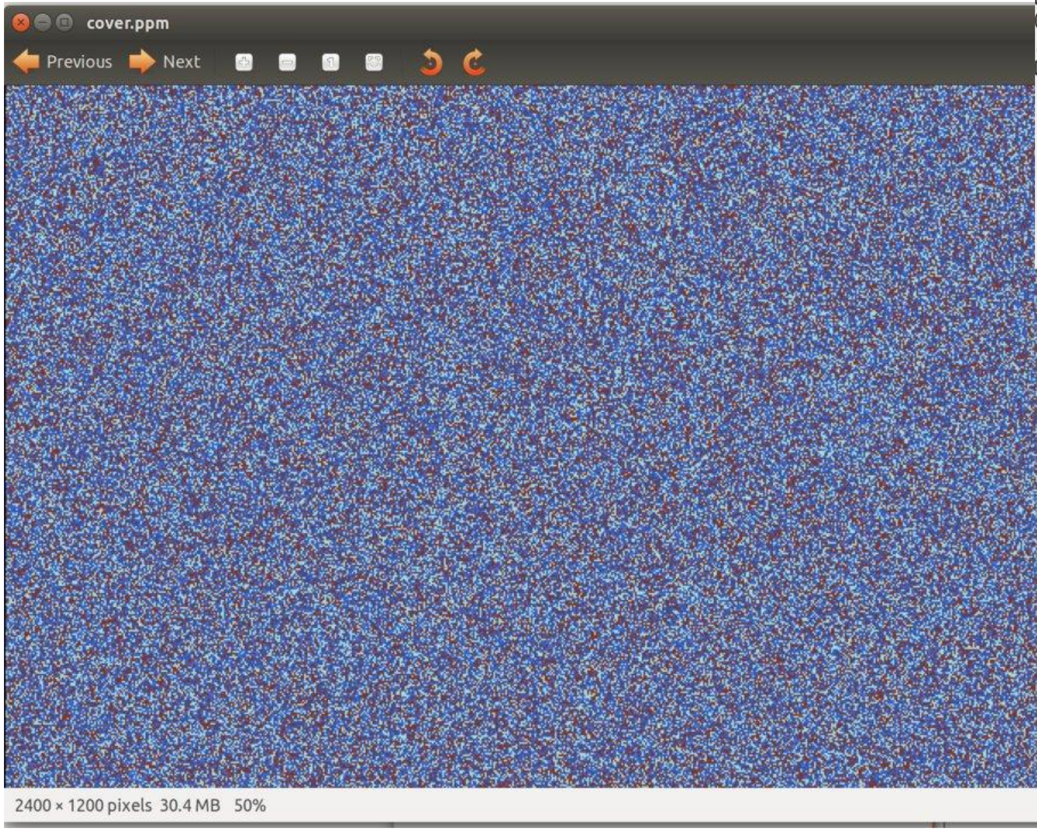
Random Padding

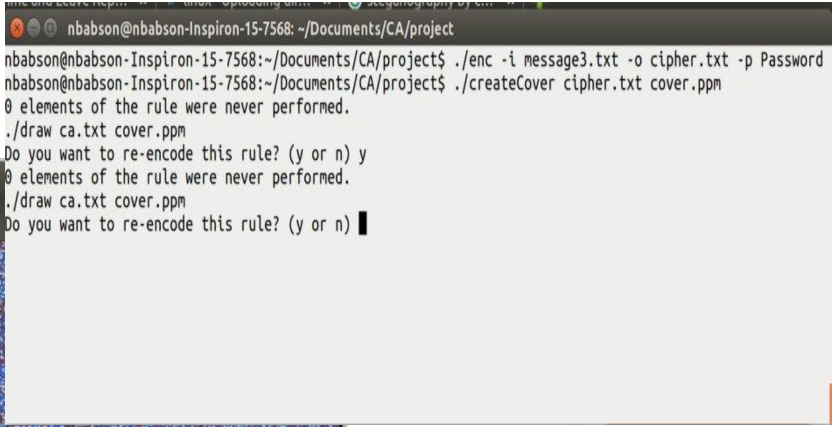




```
nbabson@nbabson-Inspiron-15-7568:~/Documents/CA/project$ ./enc -i message3.txt -o cipher.txt -p Password
nbabson@nbabson-Inspiron-15-7568:~/Documents/CA/project$ ./createCover cipher.txt cover.ppm
0 elements of the rule were never performed.
./draw ca.txt cover.ppm
Do you want to re-encode this rule? (y or n)
```

Random Padding





```
nbabson@nbabson-Inspiron-15-7568:~/Documents/CA/project$ ./enc -i message3.txt -o cipher.txt -p Password
nbabson@nbabson-Inspiron-15-7568:~/Documents/CA/project$ ./createCover cipher.txt cover.ppm
0 elements of the rule were never performed.
./draw ca.txt cover.ppm
Do you want to re-encode this rule? (y or n) y
0 elements of the rule were never performed.
./draw ca.txt cover.ppm
Do you want to re-encode this rule? (y or n) 
```

Each state number is encoded in the randomly selected colors.

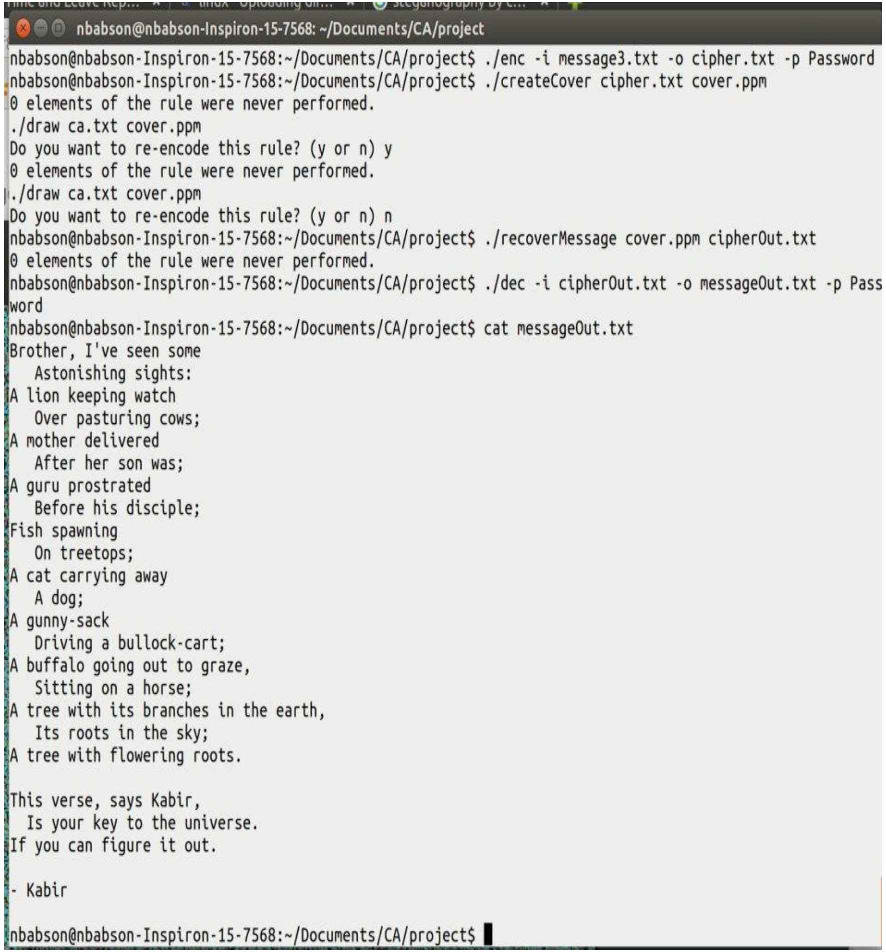
Each generated CA has a different random generation 0.

Extraction

It is possible some elements of the rule will not be expressed in the CA.

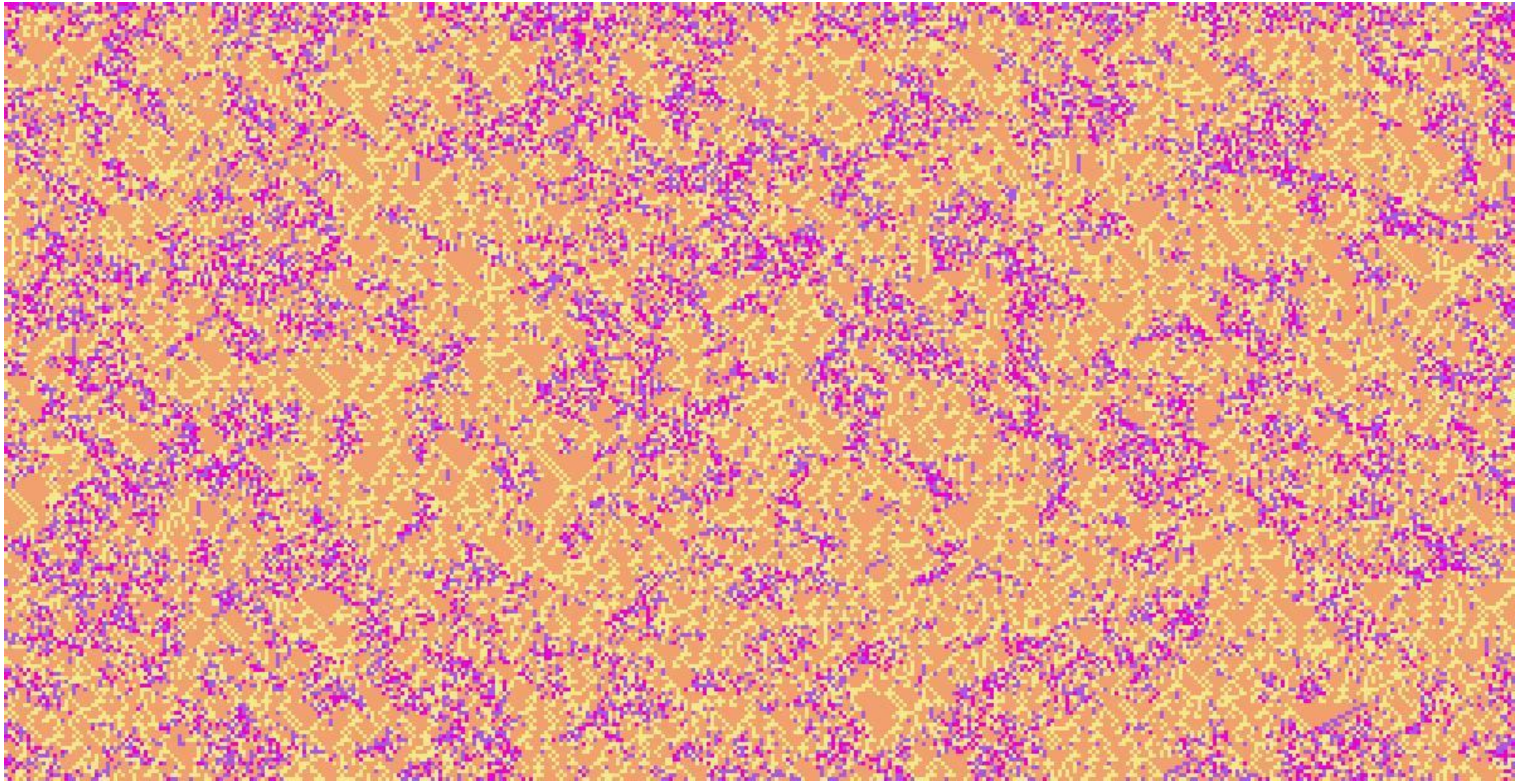
If there is room in the rule, the message is embedded twice.

The redundancy helps recover missing message characters.

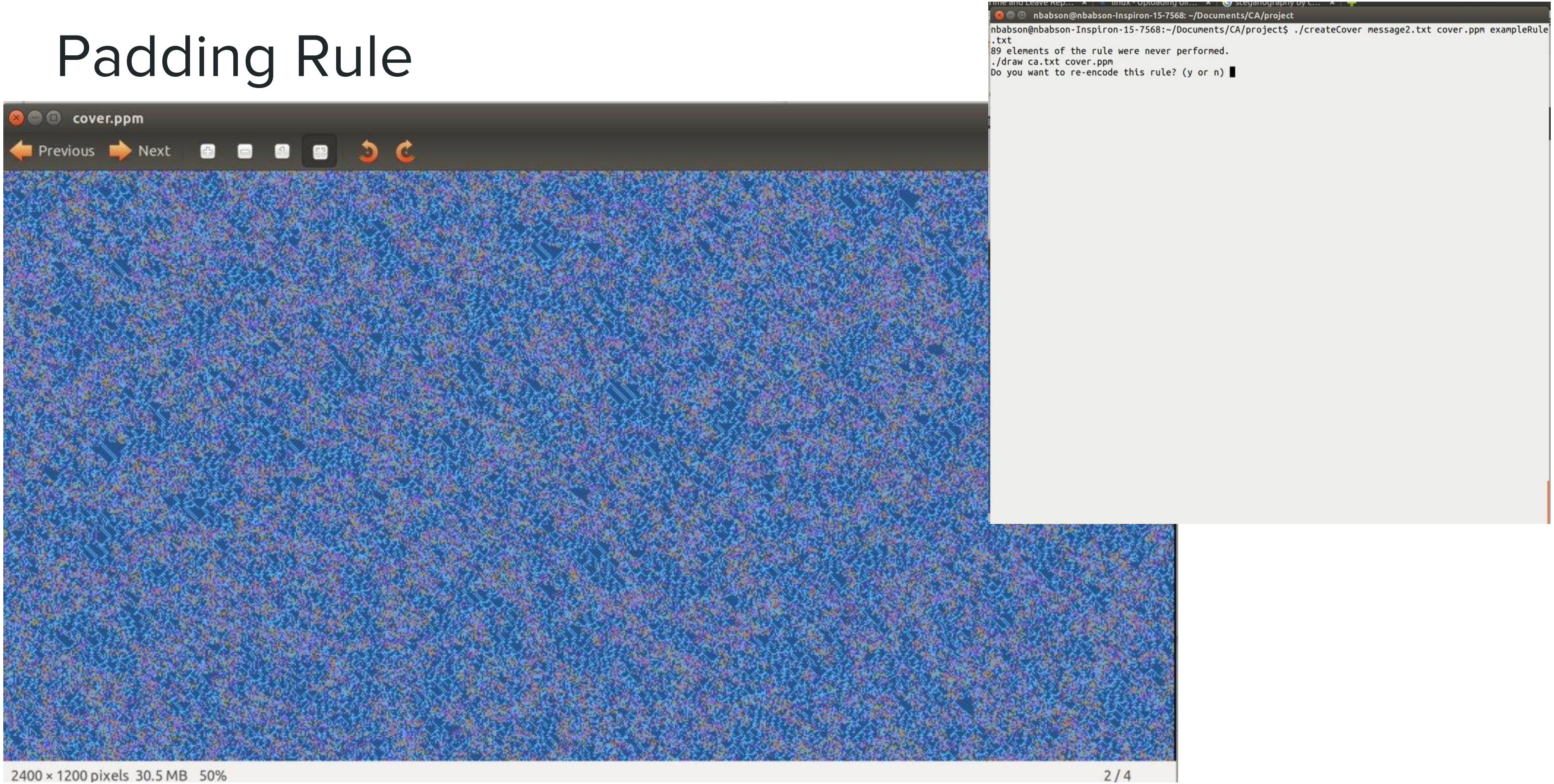


```
nbabson@nbabson-Inspiron-15-7568:~/Documents/CA/project$ ./enc -i message3.txt -o cipher.txt -p Password
nbabson@nbabson-Inspiron-15-7568:~/Documents/CA/project$ ./createCover cipher.txt cover.ppm
0 elements of the rule were never performed.
./draw ca.txt cover.ppm
Do you want to re-encode this rule? (y or n) y
0 elements of the rule were never performed.
./draw ca.txt cover.ppm
Do you want to re-encode this rule? (y or n) n
nbabson@nbabson-Inspiron-15-7568:~/Documents/CA/project$ ./recoverMessage cover.ppm cipherOut.txt
0 elements of the rule were never performed.
nbabson@nbabson-Inspiron-15-7568:~/Documents/CA/project$ ./dec -i cipherOut.txt -o messageOut.txt -p Pass
word
nbabson@nbabson-Inspiron-15-7568:~/Documents/CA/project$ cat messageOut.txt
Brother, I've seen some
   Astonishing sights:
A lion keeping watch
   Over pasturing cows;
A mother delivered
   After her son was;
A guru prostrated
   Before his disciple;
Fish spawning
   On treetops;
A cat carrying away
   A dog;
A gunny-sack
   Driving a bullock-cart;
A buffalo going out to graze,
   Sitting on a horse;
A tree with its branches in the earth,
   Its roots in the sky;
A tree with flowering roots.

This verse, says Kabir,
  Is your key to the universe.
If you can figure it out.

- Kabir

nbabson@nbabson-Inspiron-15-7568:~/Documents/CA/project$ █
```

Padding Rule

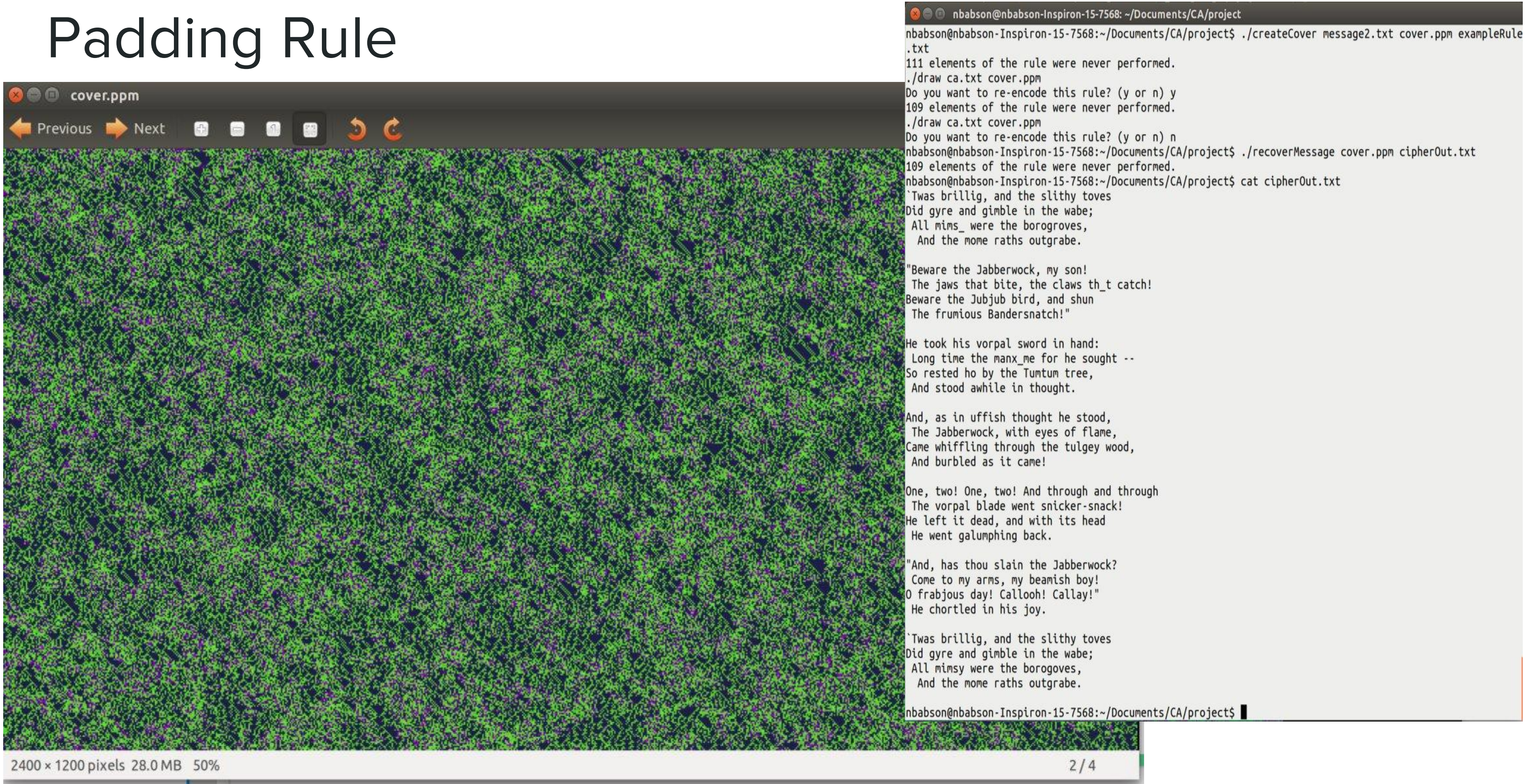


Padding Rule


cover.ppm
Previous
Next
2400 × 1200 pixels 30.5 MB 50%
2 / 4
nbabson@nbabson-Inspiron-15-7568: ~/Documents/CA/project

```
nbabson@nbabson-Inspiron-15-7568:~/Documents/CA/project$ ./createCover message2.txt cover.ppm exampleRule
.txt
89 elements of the rule were never performed.
./draw ca.txt cover.ppm
Do you want to re-encode this rule? (y or n)
```

Padding Rule


cover.ppm
Previous
Next
2400 × 1200 pixels 28.0 MB 50%
2 / 4
nbabson@nbabson-Inspiron-15-7568: ~/Documents/CA/project

```
nbabson@nbabson-Inspiron-15-7568:~/Documents/CA/project$ ./createCover message2.txt cover.ppm exampleRule
.txt
111 elements of the rule were never performed.
./draw ca.txt cover.ppm
Do you want to re-encode this rule? (y or n) y
109 elements of the rule were never performed.
./draw ca.txt cover.ppm
Do you want to re-encode this rule? (y or n) n
nbabson@nbabson-Inspiron-15-7568:~/Documents/CA/project$ ./recoverMessage cover.ppm cipherOut.txt
109 elements of the rule were never performed.
nbabson@nbabson-Inspiron-15-7568:~/Documents/CA/project$ cat cipherOut.txt
`Twas brillig, and the slithy toves
Did gyre and gimble in the wabe;
 All mims_ were the borogroves,
  And the mome raths outgrabe.

"Beware the Jabberwock, my son!
 The jaws that bite, the claws th_t catch!
Beware the Jubjub bird, and shun
 The frumious Bandersnatch!"

He took his vorpal sword in hand:
 Long time the manx_me for he sought --
So rested ho by the Tumtum tree,
 And stood awhile in thought.

And, as in uffish thought he stood,
 The Jabberwock, with eyes of flame,
Came whiffling through the tulgey wood,
 And burbled as it came!

One, two! One, two! And through and through
 The vorpal blade went snicker-snack!
He left it dead, and with its head
 He went galumphing back.

"And, has thou slain the Jabberwock?
 Come to my arms, my beamish boy!
O frabjous day! Callooh! Callay!"
 He chortled in his joy.

`Twas brillig, and the slithy toves
Did gyre and gimble in the wabe;
 All mimsy were the borogoves,
  And the mome raths outgrabe.

nbabson@nbabson-Inspiron-15-7568:~/Documents/CA/project$ 
```

LSB Histogram Detection

The least significant bit of each color is set so that there are an equal number of 0s and 1s.

Since the CA blocks are 3 x 3 pixels, hopefully the least significant bit distribution will resemble that of a natural image, in which neighboring pixels are likely to resemble each other.

Results with HW2 detector:

n = 2 → 0.32 DIFFERENT

n = 3 → 0.008 DIFFERENT

n = 4 → 0.81 DIFFERENT

n = 5 → 0.97 SAME