A Curiosity Regarding Steganographic Capacity of Pathologically Nonstationary Sources

Andrew Ker

adk@comlab.ox.ac.uk

Oxford University Computing Laboratory

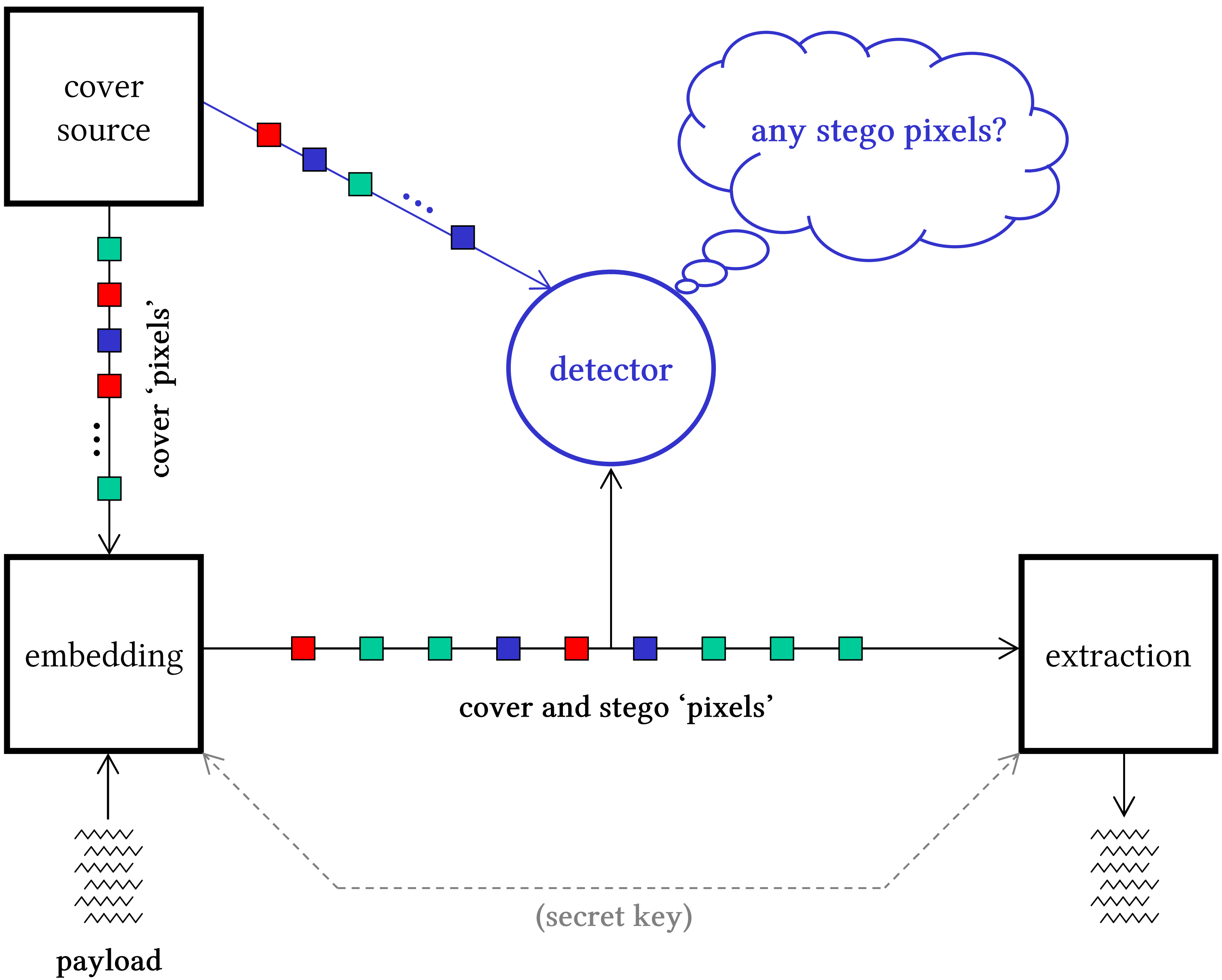
SPIE/IS&T Electronic Imaging, San Francisco

24 January 2011

A Curiosity
Regarding Steganographic Capacity
of Pathologically Nonstationary Sources

Outline

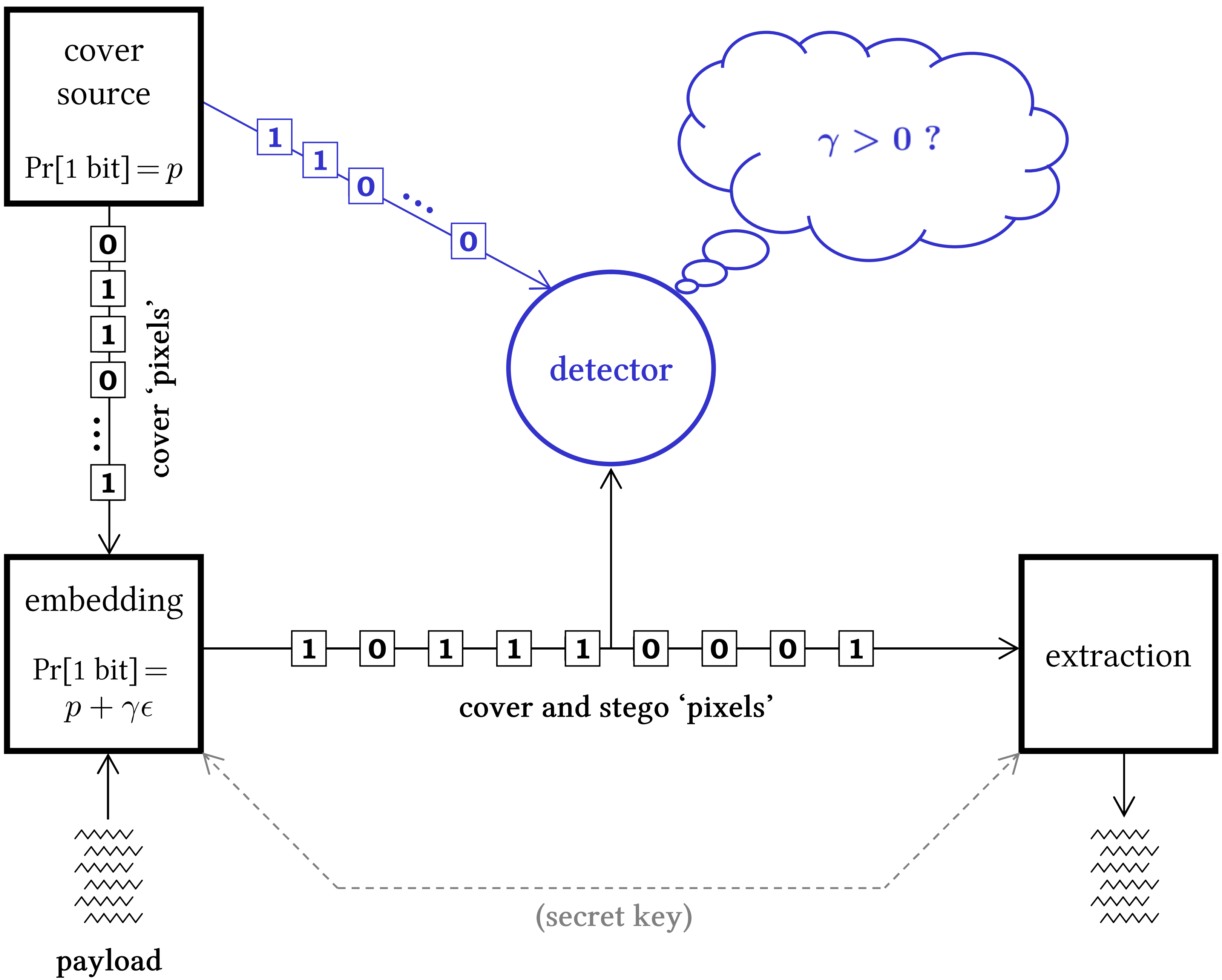
- Stationary i.i.d. bit streams:
  - *square root capacity law*
- The most horrible nonstationary source:
  - *linear capacity law (if...)*
- The next most horrible nonstationary source:
  - *a curious result*


cover
source
any stego pixels?
cover 'pixels'
detector
embedding
cover and stego 'pixels'
extraction
(secret key)
payload

Ultimate aim

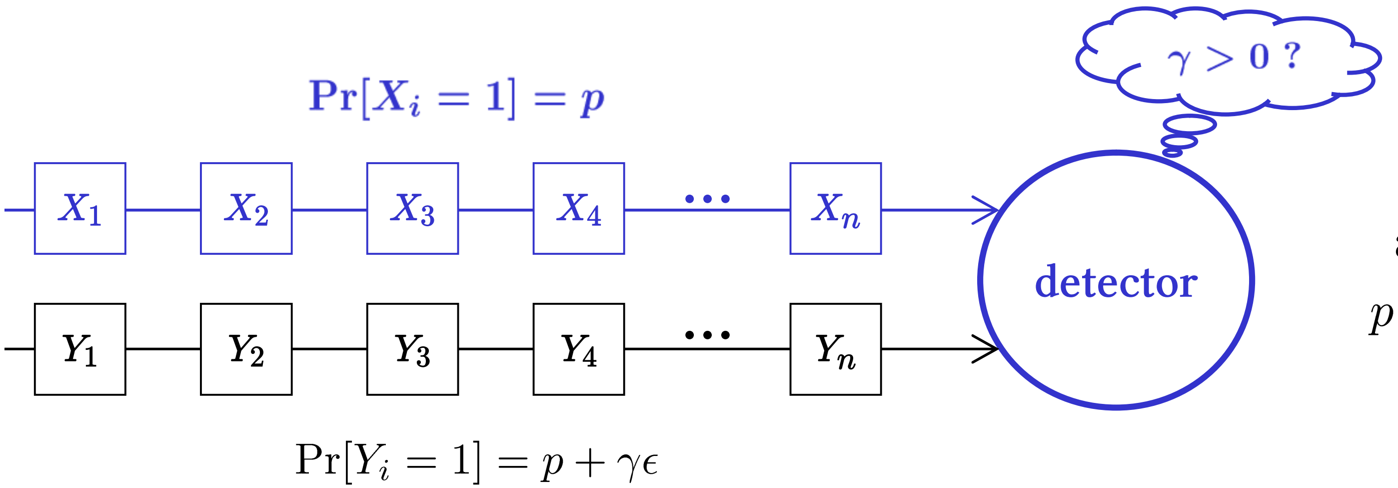
Want to prove capacity laws for realistic cover models with minimal assumptions.

> ‘If there is a problem you can’t solve, then there is an easier problem you can solve: find it.’
>
> George Pólya



cover
source
Pr[1 bit] = p
1
1
0
...
0
0
1
1
0
...
1
cover 'pixels'
γ > 0 ?
detector
embedding
Pr[1 bit] =
p + γε
1
0
1
1
1
0
0
0
1
cover and stego 'pixels'
extraction
payload
(secret key)

A simple square root law

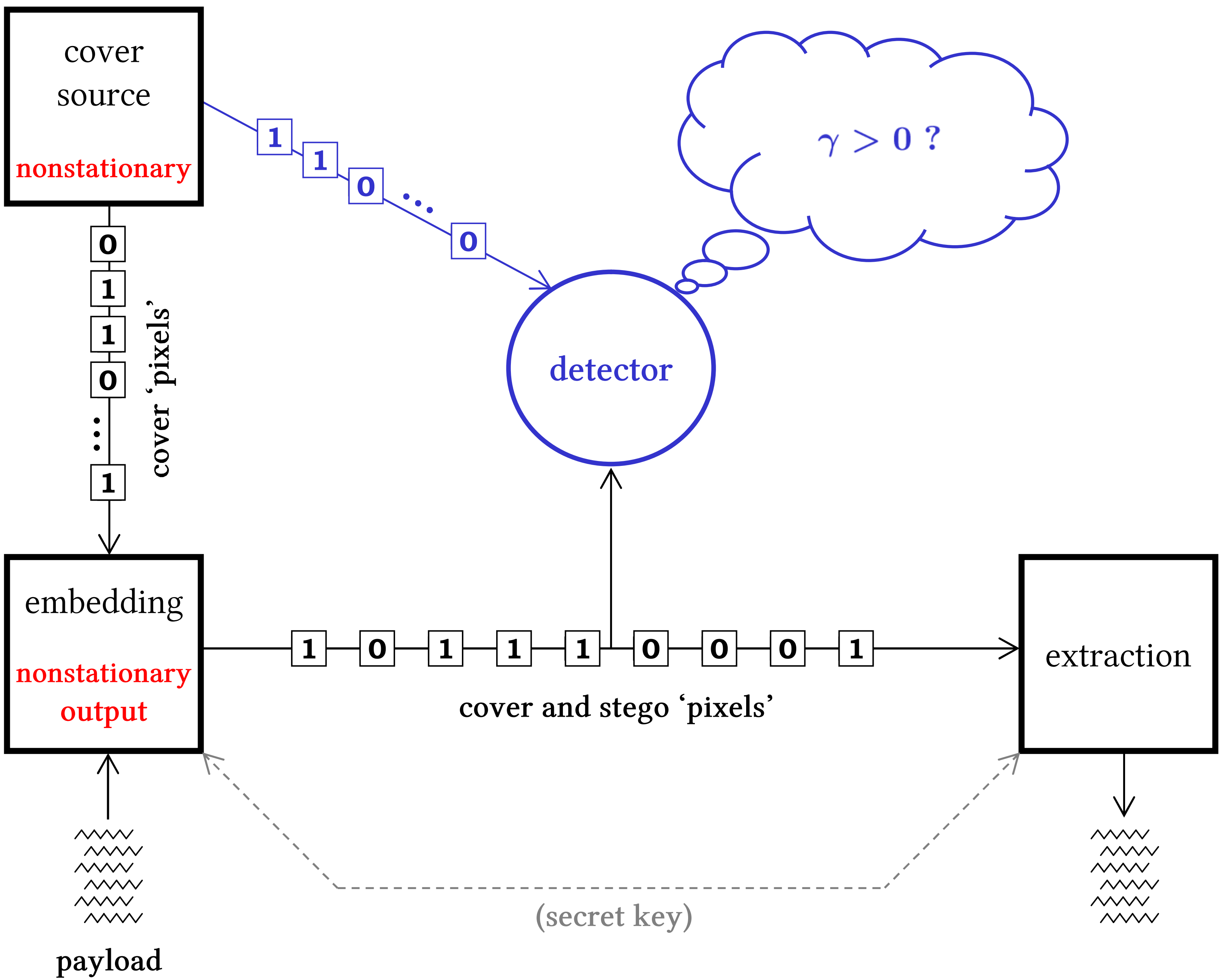


assumptions:
$p \neq 0, 1, \ |\epsilon| > 0$

As $n \to \infty$,

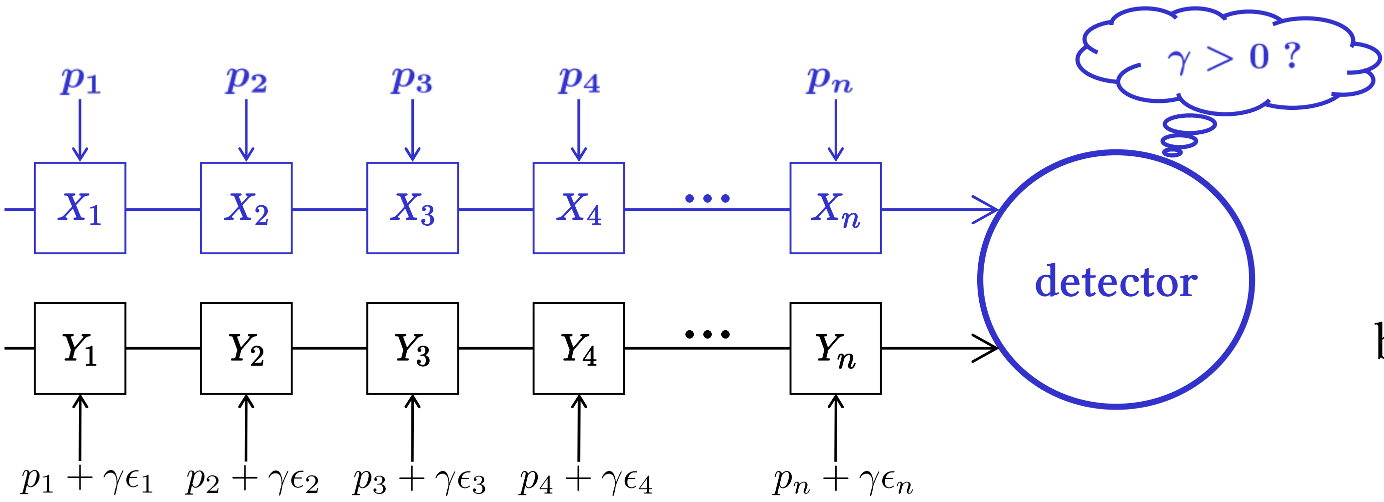
1. If $\gamma^2 n \to \infty$, an asymptotically perfect detector exists.
2. If $\gamma^2 n \to 0$, there is asymptotic perfect security.

The critical payload size $\propto n\gamma = O(\sqrt{n})$.



cover
source
nonstationary
1
1
0
0
$\gamma > 0$?
0
1
1
0
1
cover 'pixels'
detector
embedding
nonstationary
output
1
0
1
1
1
0
0
0
1
extraction
cover and stego 'pixels'
(secret key)
payload

Pathological nonstationarity



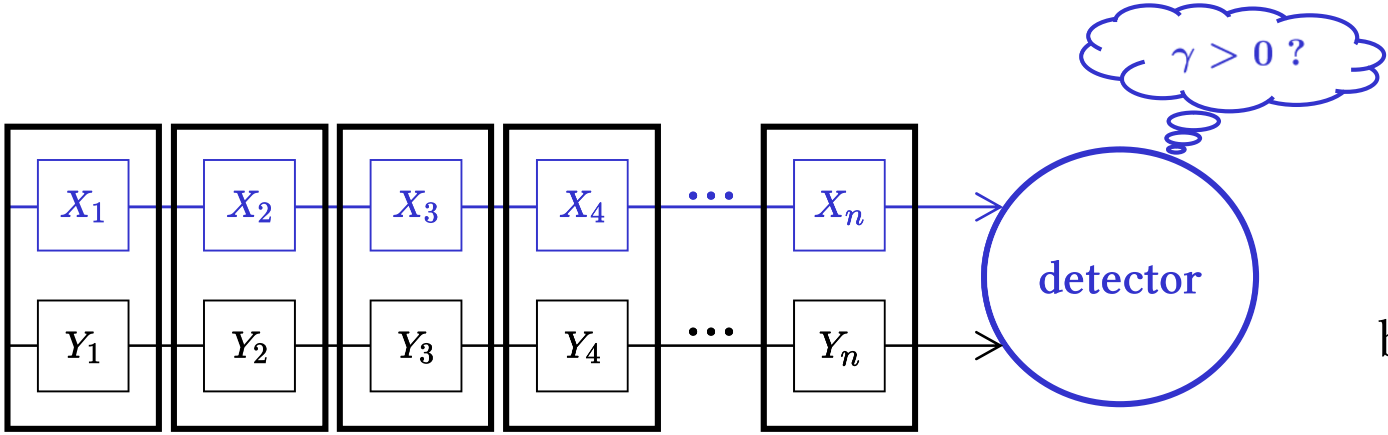
assumptions:
$p_i,\ 1-p_i,\ |\epsilon_i|$
bounded away from 0.

Even when γ is fixed, there is no asymptotic perfect detector as $n \to \infty$,

if and only if

- the detector is ignorant of the p_i, and
- $\sum \epsilon_i = 0$ (first-order statistics are preserved).

Pathological nonstationarity



assumptions:
$p_i,\ 1-p_i,\ |\epsilon_i|$
bounded away from 0.

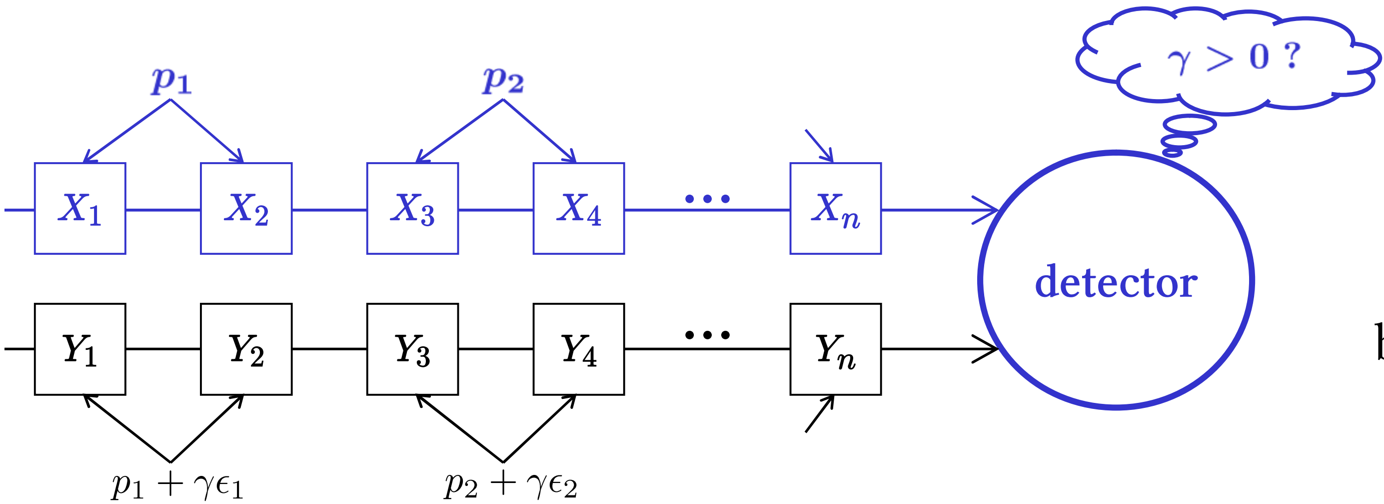
Even when γ is fixed, there is no asymptotic perfect detector as $n \to \infty$,

if and only if
- the detector is ignorant of the p_i, and
- $\sum \epsilon_i = 0$ (first-order statistics are preserved).

Detector must be invariant under permutations, so forced to rely on

$$\begin{pmatrix} \#(X_i{=}0, Y_i{=}0) \\ \#(X_i{=}0, Y_i{=}1) \\ \#(X_i{=}1, Y_i{=}0) \\ \#(X_i{=}1, Y_i{=}1) \end{pmatrix} \dot\sim \mathbf{N}(n\mu, n\Sigma(\gamma))$$

Pair stationarity

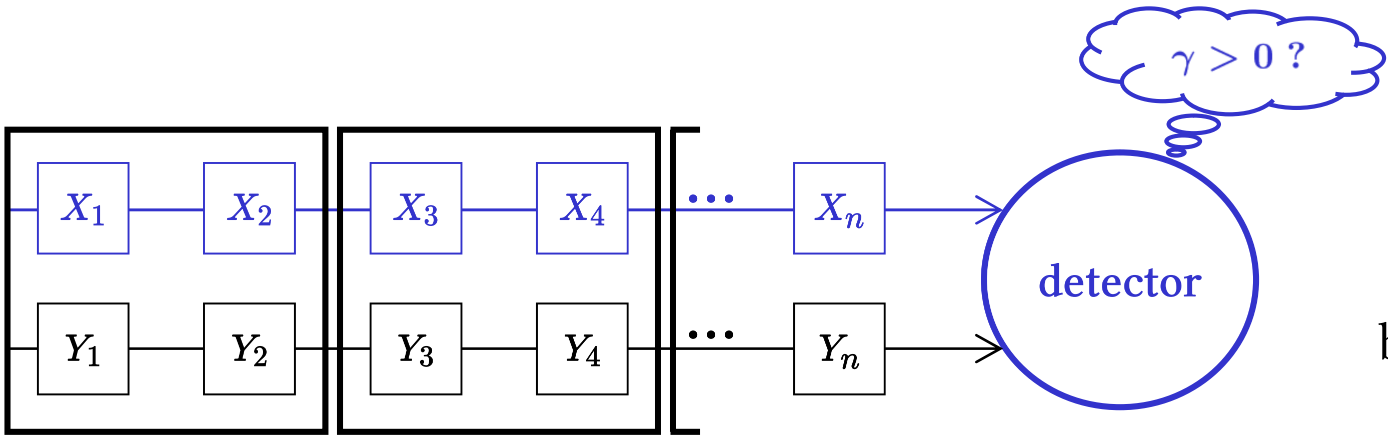


assumptions:

$p_i,\ 1-p_i,\ |\epsilon_i|$

bounded away from 0.

Pair stationarity



assumptions:

$p_i,\ 1-p_i,\ |\epsilon_i|$

bounded away from 0.

$$\Pr\left[\begin{smallmatrix} 0 & 0 \\ 1 & 1 \end{smallmatrix}\right] = (1-p_i)^2(p_i+\gamma\epsilon_i)^2$$

$$-$$

$$\Pr\left[\begin{smallmatrix} 0 & 1 \\ 0 & 1 \end{smallmatrix}\right] = (1-p_i)p_i(1-p_i-\gamma\epsilon_i)(p_i+\gamma\epsilon_i)$$

$$-$$

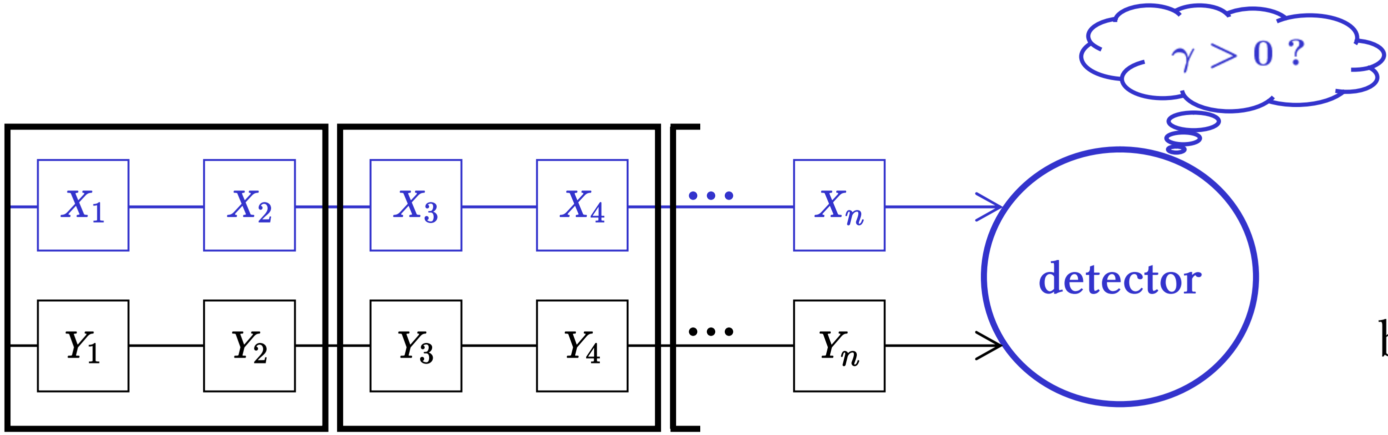
$$\Pr\left[\begin{smallmatrix} 1 & 0 \\ 1 & 0 \end{smallmatrix}\right] = (1-p_i)p_i(1-p_i-\gamma\epsilon_i)(p_i+\gamma\epsilon_i)$$

$$+$$

$$\Pr\left[\begin{smallmatrix} 1 & 1 \\ 0 & 0 \end{smallmatrix}\right] = p_i^2(1-p_i-\gamma\epsilon_i)^2$$

$$= \gamma^2\epsilon_i^2$$

Pair stationarity



assumptions:

$p_i,\ 1-p_i,\ |\epsilon_i|$

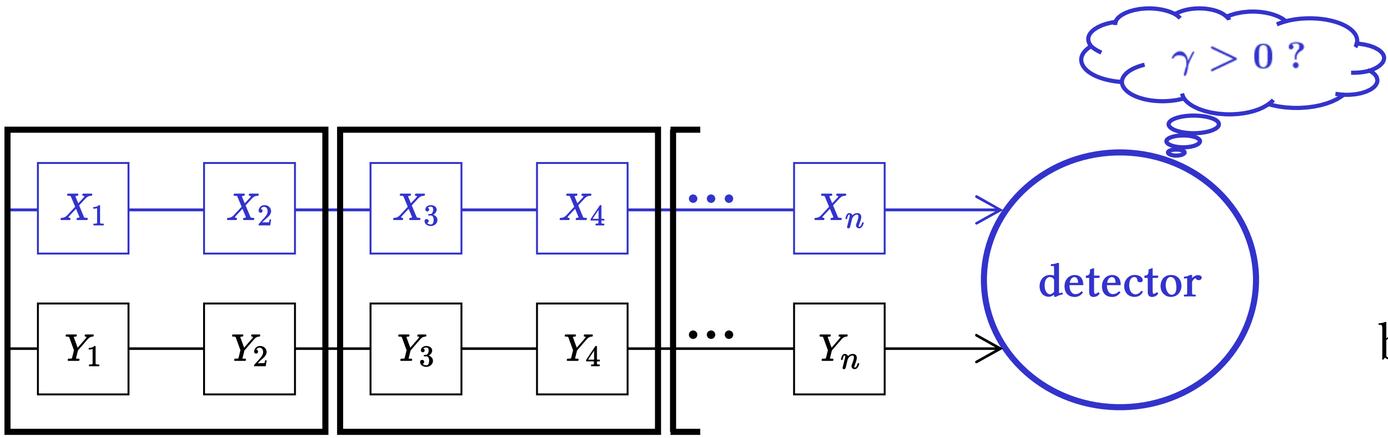
bounded away from 0.

if
- the detector is ignorant of the p_i, and
- $\sum \epsilon_i = 0$ (first-order statistics are preserved).

Detector must be invariant under permutations, so forced to rely on

$$\begin{pmatrix} \#(X_{2i}{=}0, X_{2i+1}{=}0, Y_{2i}{=}0, Y_{2i+1}{=}0) \\ \#(X_{2i}{=}0, X_{2i+1}{=}0, Y_{2i}{=}0, Y_{2i+1}{=}1) \\ \vdots \end{pmatrix} \dot{\sim} \mathrm{N}(n\mu + n\gamma^2\nu, n\Sigma(\gamma))$$

Pair stationarity



assumptions:

p_i, $1-p_i$, $|\epsilon_i|$

bounded away from 0.

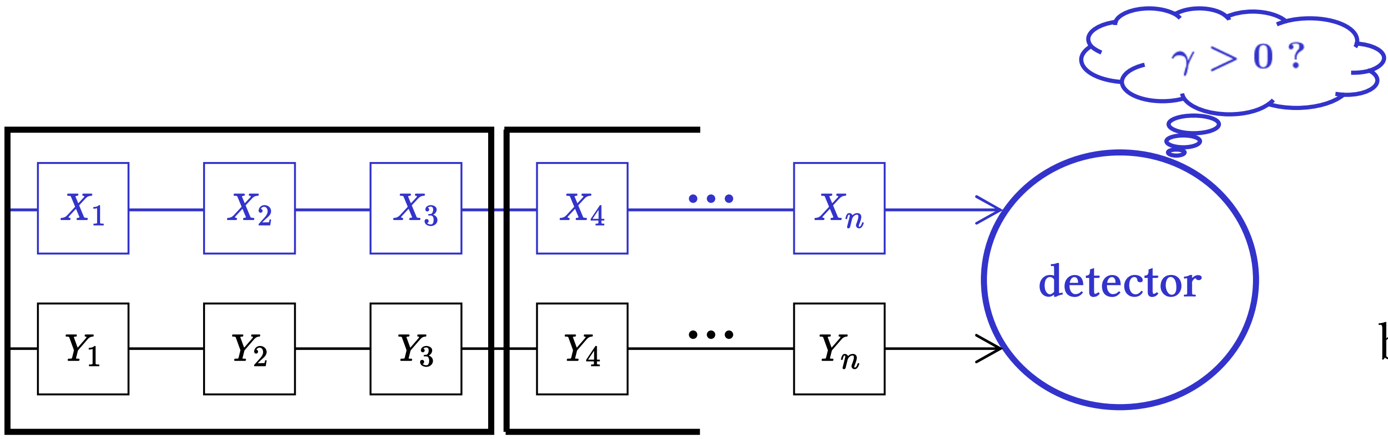
if
- the detector is ignorant of the p_i, and
- $\sum \epsilon_i = 0$ (first-order statistics are preserved).

As $n \to \infty$,

1. If $\gamma^4 n \to \infty$, an asymptotically perfect detector exists.
2. If $\gamma^4 n \to 0$, no asymptotically perfect detector exists.

The critical payload size $\propto n\gamma = O(n^{3/4})$.

Triple stationarity



assumptions:
p_i, $1-p_i$, $|\epsilon_i|$
bounded away from 0.

if
- the detector is ignorant of the p_i, and
- $\sum \epsilon_i = 0$ (first-order statistics are preserved).

As $n \to \infty$,

1. If $\gamma^4 n \to \infty$, an asymptotically perfect detector exists.
2. If $\gamma^4 n \to 0$, no asymptotically perfect detector exists.

The critical payload size $\propto n\gamma = O(n^{3/4})$.

Conclusions

- These cover models are not supposed to be realistic.
  - *This work pushes the boundaries of the square root law.*

- The square root law fails for completely nonstationary sources…

  … as long as the detector is ignorant of the bit probabilities.

  … and the embedding is first-order secure.

- Stationarity for two bits at a time leads to an $O(n^{3/4})$ capacity law.

- Stationarity for any pattern of bits has the same conclusion.
  - *This is very curious.*