

The Square Root Law Requires a Linear Key



Andrew Ker

adk@comlab.ox.ac.uk

Oxford University Computing Laboratory

11th ACM Multimedia & Security Workshop
Princeton, 8 September 2009

kindly presented by Jessica Fridrich

The Square Root Law Requires a Linear Key

Outline

- *The simplest square root law (SRL)*
 - *problem with the embedding assumption*
- *SRL for fixed-size payload*
 - *problem with the secret key assumption*
- *Partial SRL with limited secret keys*
- *Conclusions*

SRL for i.i.d. covers


- Assuming
- Covers, size n , consist of independent random samples (pixels).
 - Payload, size m , affects pixels independently with probability m/n .
 - Unaltered pixels have mass function $p(x)$, pixels used for payload have mass function $q(x)$.
 - $\exists z.p(z) \neq q(z) \quad \wedge \quad p(x)=0 \Leftrightarrow q(x)=0$.

1. If $m/\sqrt{n} \rightarrow \infty$ as $n \rightarrow \infty$ then, for sufficiently large n , an arbitrarily accurate detector exists.
2. If $m/\sqrt{n} \rightarrow 0$ as $n \rightarrow \infty$ then, for sufficiently large n , every detector must have an arbitrarily high inaccuracy.

We interpret this to mean

“secure payload grows asymptotically with the square root of cover size.”

SRL for i.i.d. covers

- Assuming
- Covers, size n , consist of independent random samples (pixels).
 - Payload, size m , affects pixels independently with probability m/n .
- 

Problem

This is a slightly unrealistic model:

- “Uniform” embedding is not “independent” embedding.
- If the payload is of a certain size, embedding in location i means that embedding in location j is marginally less likely.

So even in the i.i.d. cover model, the stego images should not consist of i.i.d. pixels. This makes analysis difficult.

Modified SRL

Assuming

- Covers, size n , consist of independent random samples (pixels).

- Payload affects m locations chosen uniformly from all possible embedding paths.

- Unaltered pixels have mass function $p(x)$, pixels used for payload have mass function $q(x)$.

- $\exists z.p(z) \neq q(z) \quad \wedge \quad p(x)=0 \Leftrightarrow q(x)=0$.

1. If $m/\sqrt{n} \rightarrow \infty$ as $n \rightarrow \infty$ then, for sufficiently large n , an arbitrarily accurate detector exists.

2. If $m/\sqrt{n} \rightarrow 0$ as $n \rightarrow \infty$ then, for sufficiently large n , every detector must have an arbitrarily high inaccuracy.

i.e. the same result holds with “uniform” instead of “independent” embedding.

Modified SRL

- Assuming
- Covers, size n , consist of independent random samples (pixels).
 - Payload affects m locations chosen uniformly from all possible embedding paths.

Problem

Still unrealistic!

There are $\frac{n!}{(n-m+1)!}$ possible embedding paths (choose m ordered locations from n , without replacement).

If $m \sim \sqrt{n}$, sender and recipient need to share $\log \frac{n!}{(n-\sqrt{n})!} \sim m \log m$ bits of information to locate the payload, i.e.

they need a secret key larger than the payload transmitted!

SRL requires a linear key

- Assuming
- Covers, size n , consist of independent random samples (pixels).
 - Payload affects m locations chosen from a set of 2^k possible embedding paths (i.e. a secret key of k bits).
 - Unaltered pixels have mass function $p(x)$, pixels used for payload have mass function $q(x)$.
 - $\exists z.p(z) \neq q(z)$ ~~$\wedge p(x)=0 \Leftrightarrow q(x)=0$~~ .

Then

if $k/m \rightarrow 0$ and $m \rightarrow \infty$ as $n \rightarrow \infty$ then, for sufficiently large n , an arbitrarily accurate detector exists.

We interpret this to mean

“ k must be at least linear in m if a square root law is to hold”

(it’s actually a bit stronger than this).

SRL requires a linear key

- Assuming
- Covers, size n , consist of independent random samples (pixels).
 - Payload affects m locations chosen from a set of 2^k possible embedding paths (i.e. a secret key of k bits).
 - Unaltered pixels have mass function $p(x)$, pixels used for payload have mass function $q(x)$.
 - $\exists z.p(z) \neq q(z)$ ~~$\wedge p(x)=0 \Leftrightarrow q(x)=0$~~ .

Then

if $k/m \rightarrow 0$ and $m \rightarrow \infty$ as $n \rightarrow \infty$ then, for sufficiently large n , an arbitrarily accurate detector exists.

Problem

This is only half a theorem: we have not yet proved that a linear key suffices for the square root law...

Conclusion

We seem to have a parallel to Shannon's perfect cryptography bound:

“Perfect cryptography is impossible unless the secret key size is at least linear in the plaintext size...”

...and the minimum constant of linearity is the entropy rate of the plaintext.”

(we don't yet have a parallel to this second part).

Conclusion

We seem to have a parallel to Shannon's perfect cryptography bound:

*“Perfect cryptography is impossible unless the secret key size is at least linear in the **plaintext size**...”*

In the steganography case, it's at least linear in the **number of embedding changes** (not really the payload size), so we will need to adapt the result for matrix embedding or suchlike.

Other future work

- prove that a linear key is **sufficient** for a square root law,
 - (so far we know that $O(m \log m)$ is sufficient, $o(m)$ insufficient).
- find the constant of linearity (is it <1 ? If not, steganography is pointless!),
- extend to Markov (etc.) cover model.