On Ryabko and Ryabko asymptotically optimal perfect steganographic scheme in a noisy channel

Valeria Potapova

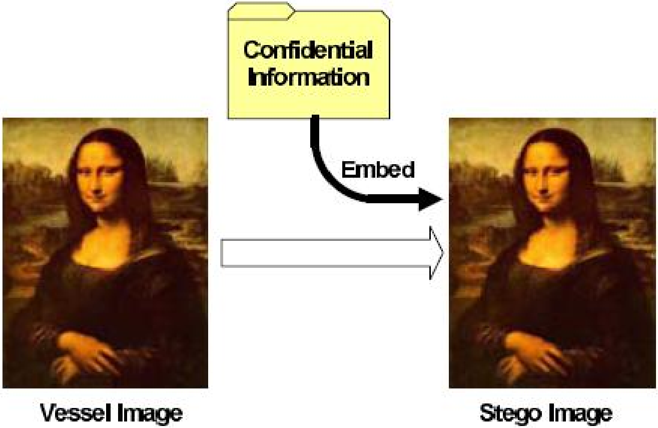
Institute for Information Transmission Problems
Russian Academy of Science

ACCT, 2016

RUSSIAN ACADEMY OF SCIENCES
INSTITUTE FOR INFORMATION TRANSMISSION PROBLEMS
(Kharkevich Institute)

Outline

The Idea of Steganography



Formal Definition

Definition

An *embedding scheme* of quality T is a pair of mappings $E : V \times X \to S$ and $D : S \to X$ such that for any message $x \in X$ and any container $v \in V$ the stegoword $s = E(v, x)$ possesses the following properties:

(1) $D(s) = x$

(2) $d(v, s) \leq T$

Ryabko and Ryabko Scheme

There is a source μ of containers v. Containers are generated as strings of symbols which are i.i.d. random variables from some finite alphabet $\mathbb{A}$. Secret binary messages are independent and generated equiprobably by a source ω. In the channel the warden can intercept and then reads all messages.

Ryabko and Ryabko Scheme. Construction for the Binary Case

The binary message $x = x_1x_2x_3\ldots$ is embedded into the container $v = v_1v_2v_3v_4\ldots,\ v_i \in \mathbb{A} = \{a, b\}$.

- The symbols of v are divided into pairs and renamed in the following way:

$$aa = u,\ bb = u,\ ab = y_0,\ ba = y_1.$$

- The pairs, corresponding to u, are idle, but the pairs y_i are changed into pairs associated with $y_{x_1}y_{x_2}y_{x_3}\ldots$ in the following way:

$$(s_{2i-1}, s_{2i}) = (\min\{v_{2i-1}, v_{2i}\}, \max\{v_{2i-1}, v_{2i}\}) \text{ if the embedded } x_k = 0 \text{ and}$$

$$(s_{2i-1}, s_{2i}) = (\max\{v_{2i-1}, v_{2i}\}, \min\{v_{2i-1}, v_{2i}\}) \text{ if the embedded } x_k = 1.$$

RUSSIAN ACADEMY OF SCIENCES
INSTITUTE FOR INFORMATION TRANSMISSION PROBLEMS
(Kharkevich Institute)

Ryabko and Ryabko Scheme. Construction for the Binary Case

Example

Let the secret message be $x = 0110\ldots$ and the container $v = aababaaaabaaaabb\ldots$. By renaming pairs we get $v = uy_1y_1uy_0y_1uuu\ldots$. We embed x and end up with the stegoword $s = uy_0y_1uy_1y_0uuu\ldots = aaabbaaabaabaaaabb\ldots$.

Single Errors on a Pair of Symbols of the Stegoword

With a single error pairs

- *aa* and *bb* turn to pairs *ab* or *ba*
- *ab* and *ba* turn to pairs *aa* or *bb*

Example

Let the secret message be $x = 0110\ldots$ and the container $v = aababaaaabaaaabb\ldots$. By renaming pairs we get $v = uy_1y_1uy_0y_1uuu\ldots$. We embed x and end up with the stegoword $s = uy_0y_1uy_1y_0uuu\ldots = aaabbaaabaabaaaabb\ldots$. Assume that two errors have occurred during the transmission and $s' = baaabaaabaabaaaabb\ldots$. The decoding algorithm extracts $x' = 1110\ldots$.

Generalized Scheme for Non-binary Case

Symbols of the container are from the alphabet $\mathbb{A} = \{0, 1, 2, ..., q-1\}$, which symbols are ordered as integers. The two stages of embedding are the same as for the binary case.

- The symbols of v are divided into pairs and renamed in the following way:

$$\alpha\alpha = u \text{ for all } \alpha \in \mathbb{A}$$
$$\alpha\beta = y_0 \text{ if } \alpha < \beta$$
$$\alpha\beta = y_1 \text{ if } \alpha > \beta.$$

- The pairs, corresponding to u, are idle, but the pairs y_i are changed into pairs associated with $y_{x_1} y_{x_2} y_{x_3} \ldots$ in the following way:

$$(s_{2i-1}, s_{2i}) = (\min\{v_{2i-1}, v_{2i}\}, \max\{v_{2i-1}, v_{2i}\}) \text{ if the embedded } x_k = 0 \text{ and}$$
$$(s_{2i-1}, s_{2i}) = (\max\{v_{2i-1}, v_{2i}\}, \min\{v_{2i-1}, v_{2i}\}) \text{ if the embedded } x_k = 1.$$

RUSSIAN ACADEMY OF SCIENCES
INSTITUTE FOR INFORMATION TRANSMISSION PROBLEMS
(Kharkevich Institute)

The Model of Errors for the Non-binary Case

- With a single error pairs $\alpha\alpha$ turns to $\alpha\beta$ or $\beta\alpha$
- If $\alpha < \beta$, a pair $\alpha\beta$ contains 0. With the conditional probability $\frac{2}{q-1}$ the pair turns into $\alpha\alpha$. If α turns into α' and $\alpha' > \beta$ or β turns into β' such that $\alpha > \beta'$, the regular reversal happens. The probability of reversal depends on the pair! Say α is k-th symbol in the alphabet and β is l-th symbol ($k < l$). The conditional probability of the reversal is $\frac{q-1-l}{q-1} + \frac{k}{q-1}$.

RUSSIAN ACADEMY OF SCIENCES
INSTITUTE FOR INFORMATION TRANSMISSION PROBLEMS
(Kharkevich Institute)

Conclusion

We have investigated the universal perfect steganographic system and its behavior during the transmission via a noisy channel or, the same, a channel with an active warden . If an error in transmitted stegoword happens during the transmission, an insertion/deletion takes place in the embedded secret message.

Thank you for your attention!

RUSSIAN ACADEMY OF SCIENCES
INSTITUTE FOR INFORMATION TRANSMISSION PROBLEMS
(Kharkevich Institute)