On secrecy of two algorithms for embedding a halftone image into grayscale image

North-West Institute of Printing Arts of St. Petersburg State University of Technology and Design

Elena Kainarova, Julia Poberezhnaya, Elena Iakovleva, Lev Denisov

Plan

1. Steganographic system
2. Two embedding algorithms
3. Secrecy

Modern steganography

Modern steganography it is a art of protection of information.

The main goal is embedding of digital data named as watermarks into digital media.

By watermarking numerous problems of copy prevention can be achieved, particulary:

1. Proof of ownership;
2. Owner identification;
3. Copy control.

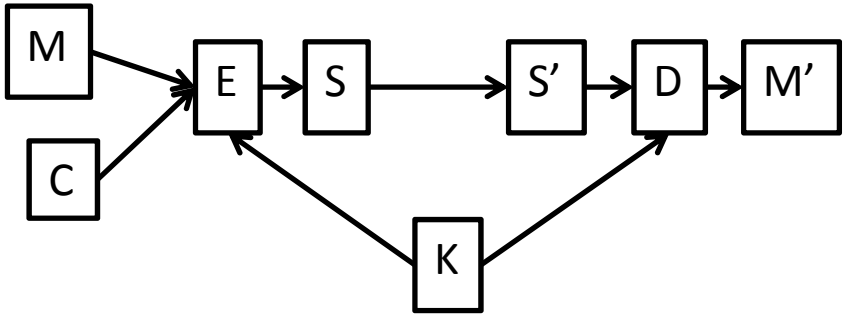
etc

A steganographic system

C	M	K	S	E	D

C	cover work	halftone image
M	digital watermark	grayscale or binary image
K	secrete key	random pattern
S	stego work	
E	embedding	
D	extracting	

E: C⊗M⊗K → S	embedding
T: S → S’	Transformation (sending through the channel)
D: C ⊗ K ⊗ S’ → M’	extracting



C≈ S

Two algorithms

The first algorithm

$C = 2^7 B_8 + \ldots + 2^{V-1} B_V + \ldots + 2^0 B_1$

E: $B_V \rightarrow S_V = K \oplus M \oplus B_V \mod(2)$

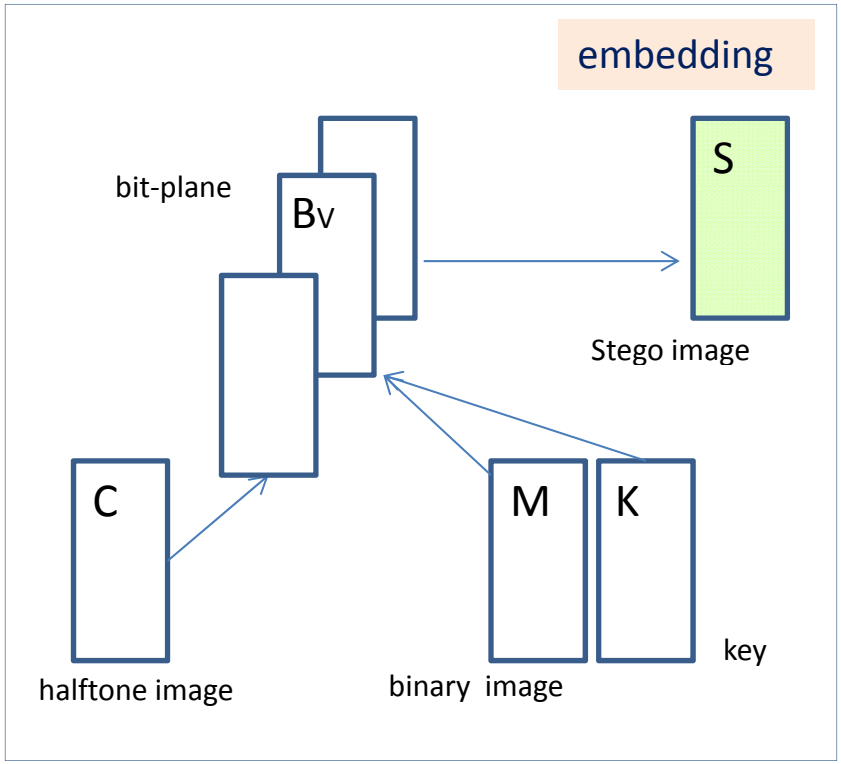
$S = 2^7 B_8 + \ldots + 2^{V-1} S_V + \ldots + 2^0 B_1$

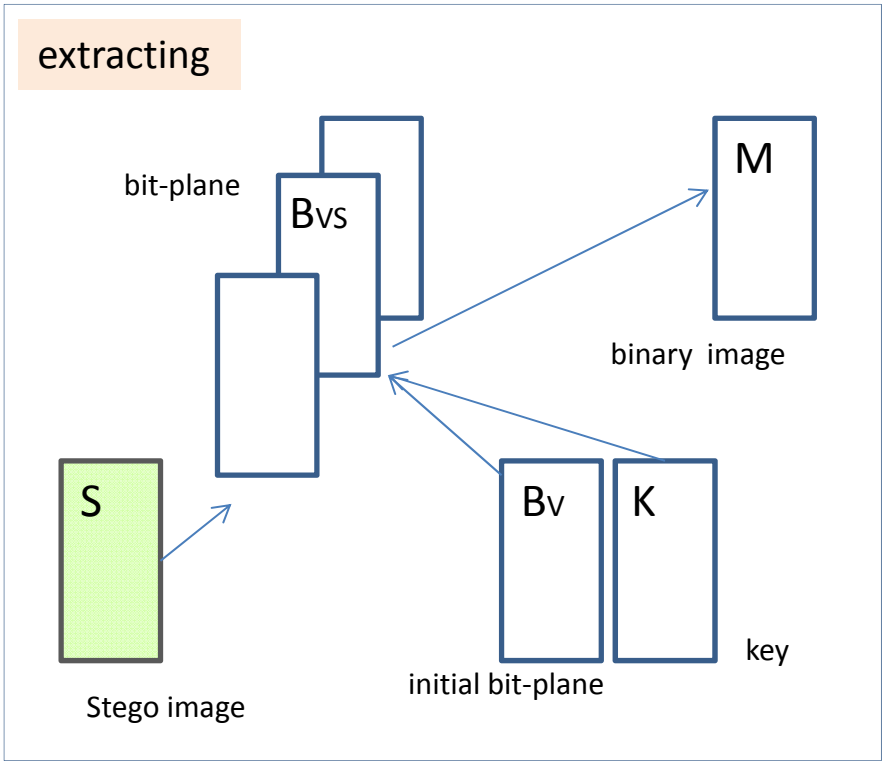
The second algorithm

E: $C \rightarrow S = C + \beta(1 - 2M)K$

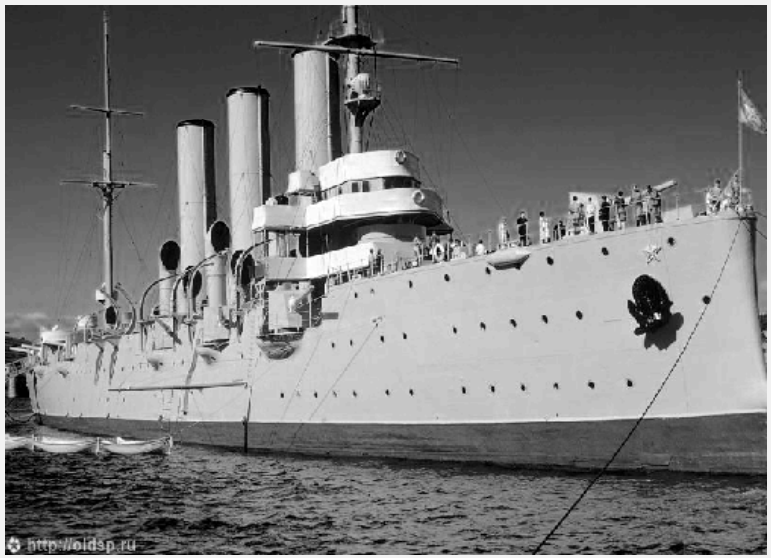
The algorithm is embedded in the bit-plane

$C \rightarrow S=C-B_V 2^{V-1}+(M+K+B_V)2^{V-1}$	embedded in the bit-plane V=1,2,…
$C \rightarrow B_v$	initial the bit-plane
$S \rightarrow B_{VS}= M+K+B_V$	bit-plane with a watermark
$M= B_{VS}+K+B_V$	extracting



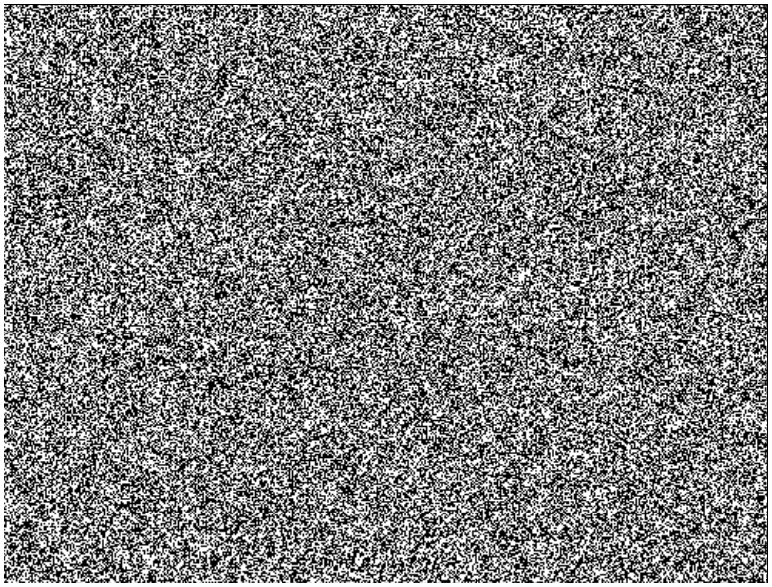


Work of the first algorithm

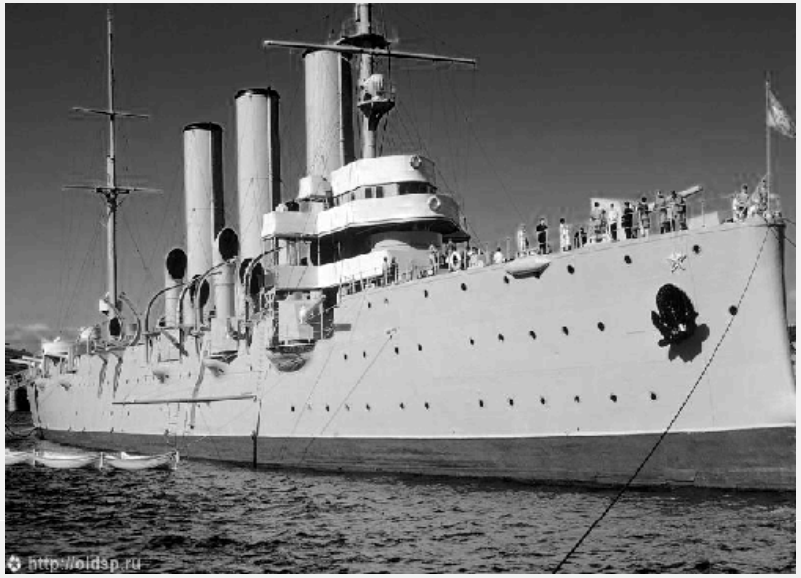


Grayscale image, Cover work

Binary image, Watermark



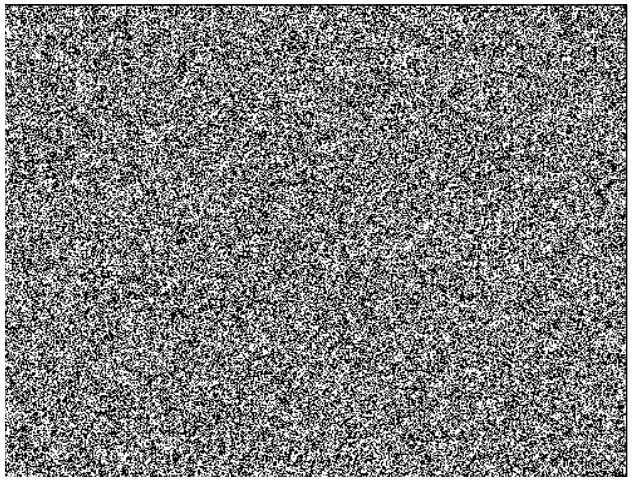
Random pattern, Secrete key



Stego work, Watermark in the second bit plain

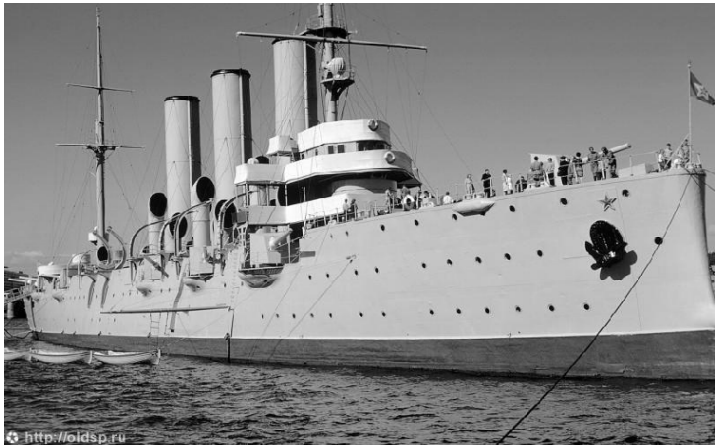
Work of the second algorithm

Grayscale image, Cover work

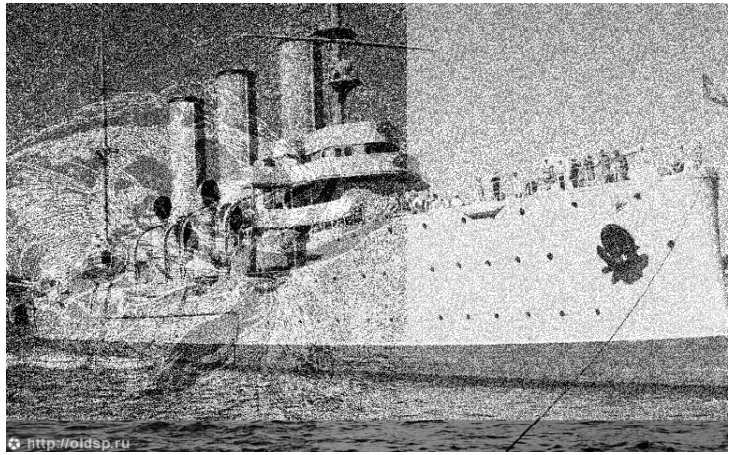


Random pattern, Secrete key

Binary image,
Watermark



b=0.1



b=100

secrecy

Problem.
Both algorithms have secrete key. Which of them is more secure?

epsilon-secrecy

The system is epsilon secure, if $Q(C|S) \leq \varepsilon$.

The system is perfect secrecy , if $Q(C|S)=0$. (Cachin, 1998).

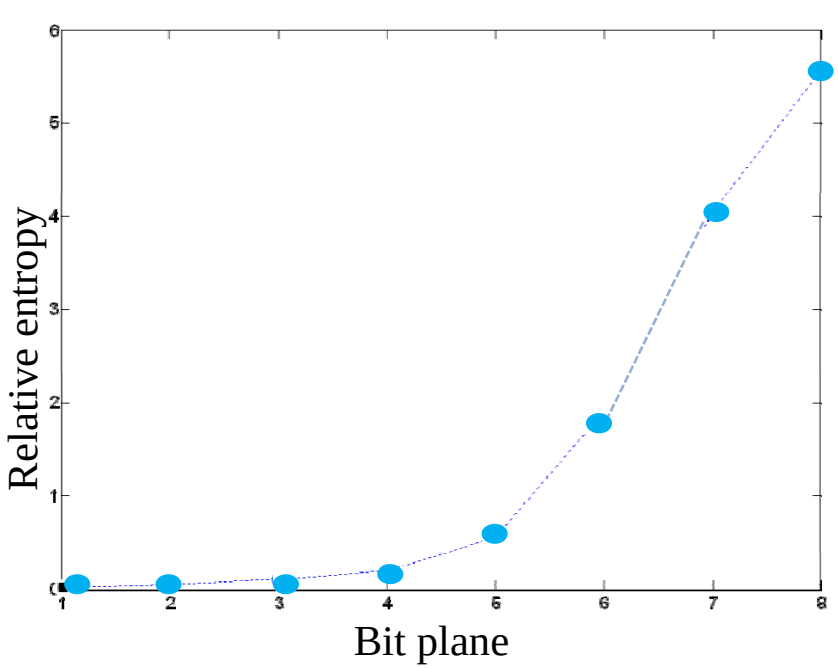
The criterion is based on the relative entropy, that describes deference between two histograms

$$Q(p_C \,\|\, p_S) = \sum_i p_C[i](\log p_C[i] - \log p_S[i])$$

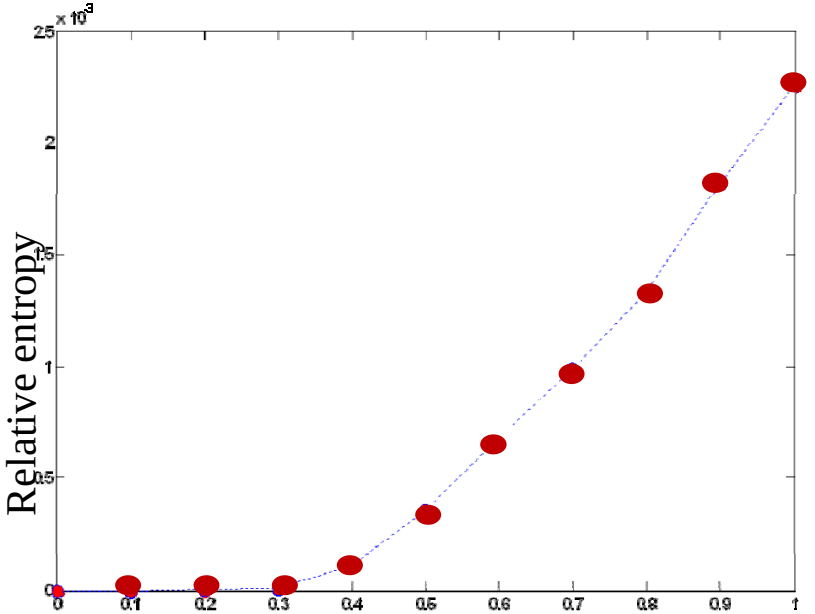
The histograms are identical $Q(C|S) \approx 0$.
It means $C \approx S$.

Relative entropy of two algoritms

First algorithm



Second algorithm



We use a base of 2000 digital images

Conclusion.
The second algorithm is more secure.

Thank you for your attention!

Our contacts:

Website Uprint Image Processing Group

http://uipg.ru

e-mail: helenkainarova@gmail.com

Saint-Petersbourg University of Technology and Design
North-West Institute of Printing