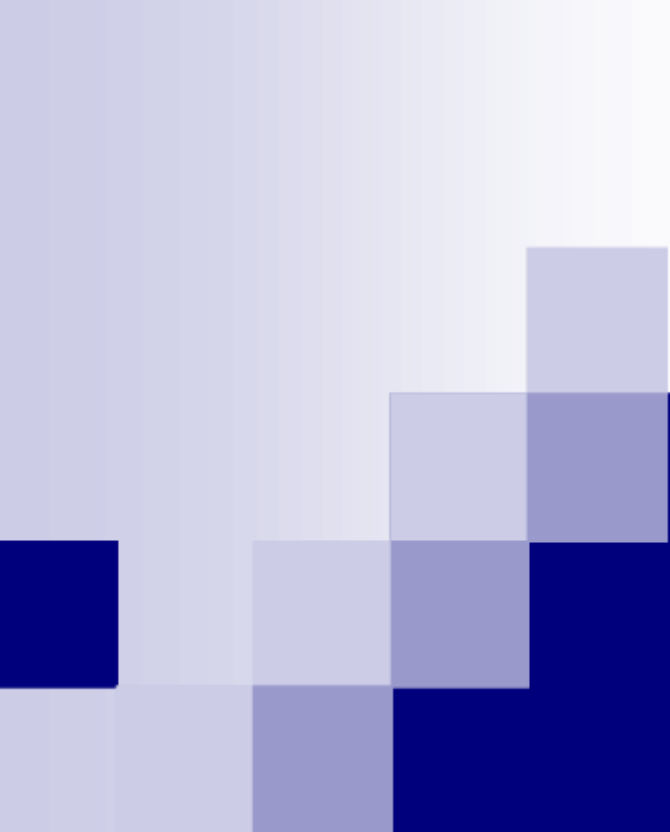




Obrazová steganografia – ukrývanie informácií v obrazoch



Ústav informatiky
Slovenská akadémia vied
Bratislava



Radoslav Forgáč

Týždeň vedy a techniky, Bratislava, 10.11.2020



1. Základné pojmy steganografie
2. Kryptografia vs. steganografia
3. Použité metódy a prostriedky
4. Požiadavky na obrazovú steganografiu
5. Neurónové siete a steganografia
 - ☐ Neurónová sieť OM-PCNN ako generátor pozičnej matice
6. Ukážka výstupov
 - ☐ Odozva neurónovej siete OM-PCNN na obrazy s rôznou entropiou
 - ☐ Odozva neurónovej siete na veľkosť ukrývanej správy
7. Využitie obrazovej steganografie

Steganografia – základné pojmy



Steganós - schovaný, skrytý; graphia - písanie

- ❑ **Steganografia** – vedná disciplína, ktorá sa zaoberá metódami ukrývania dát v krycích médiách
- ❑ **Krycie médium** – médium vhodné na ukrývanie informácií
- ❑ **Ukrývaná správa** – akákoľvek informácia, ktorá je vkladaná do krycieho média (text, obraz, video, audio, ...)
- ❑ **Stego médium** - krycie médium s ukrytou správou

Prehľad krycích médií



Audio súbory



Video súbory



Dokumenty



Súborové systémy



Spustiteľné súbory

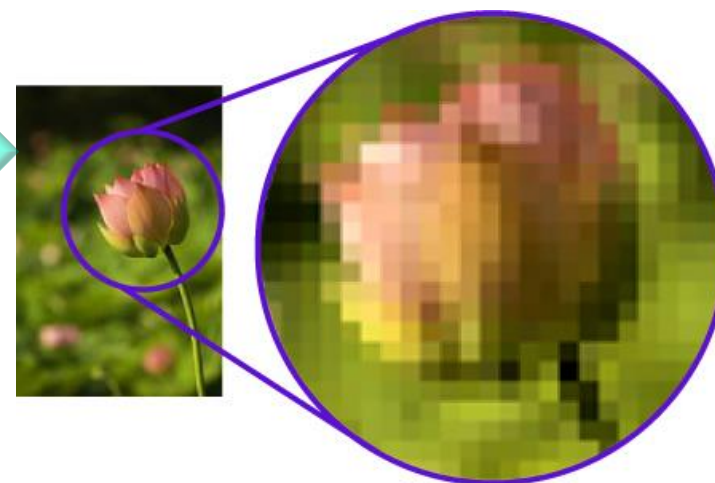


Rastrová grafika

Obrazové súbory



Vektorová grafika

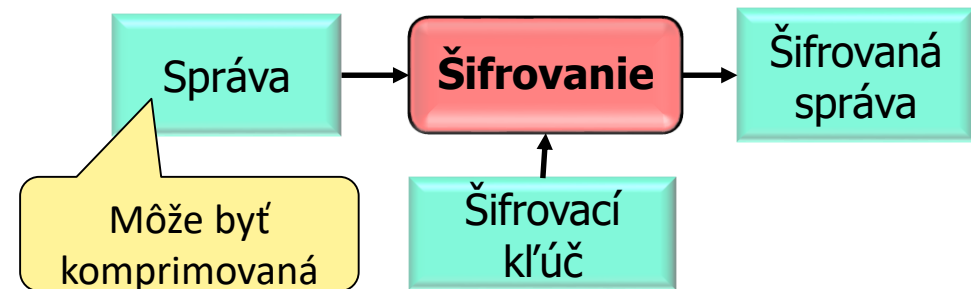


Kryptografia *VS* Steganografia



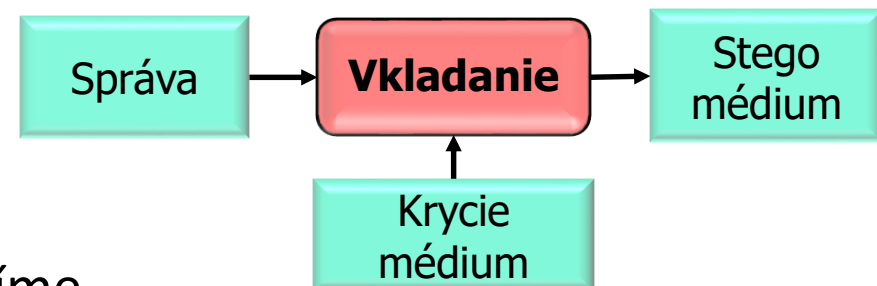
Kryptografia

- Zabezpečuje nečitateľnosť obsahu správy
- Vidíme na „prvý pohľad“, že správa je šifrovaná

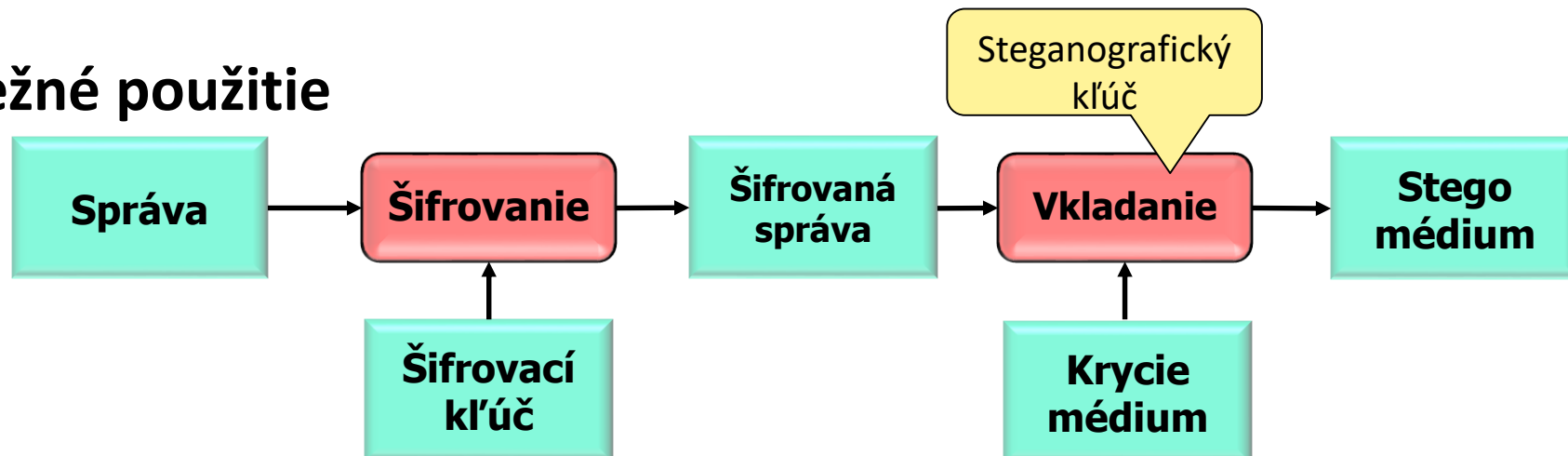


Steganografia

- Zabezpečuje utajenosť existencie správy
- Rozdiel medzi krycím médiom a stego médiom na „prvý pohľad“ nevidíme



Bežné použitie





- ❑ ***Obrazová steganografia***
 - *Časovo priestorová doména obrazov*
 - *Metóda pozičných matíc*
 - *Metóda substitúcie najmenej významného bitu (Least Significant Bit, LSB)*

- ❑ ***Šifrovanie***
 - *AES-256 na šifrovanie vkladanej správy*

- ❑ ***Neurónové siete***
 - *Optimalizovaný model Pulzne viazanej neurónovej siete (OM-PCNN) na generovanie pozičných matíc*

Metóda substitúcie najmenej významného bitu



Least Significant Bit method (LSB) a jej modifikácie

- Človek nedokáže spozorovať rozdiel intenzity pixelu, ak je zmena urobená na pozícii najmenej významného bitu

Hodnota pôvodného
i-teho pixelu

$$y_i = \begin{cases} x_i + 1 \\ x_i - 1 \\ x_i \end{cases}$$

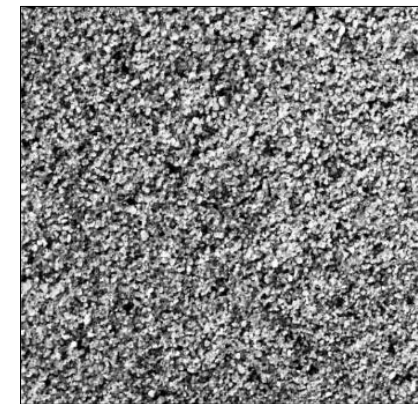
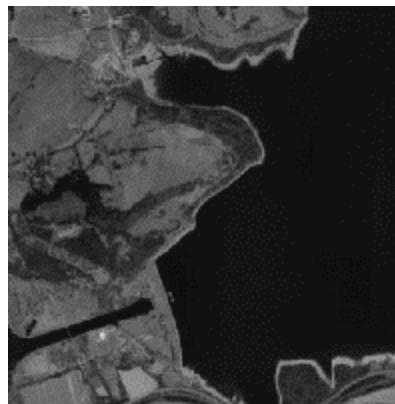
Hodnota
upraveného i-teho
pixelu

Entropia (H) – fyzikálna veličina, ktorá reprezentuje stupeň neurčitosti v obraze

$$H(x) = - \sum_{k=0}^{255} p_k \log_2 p_k$$

p_i - pravdepodobnosť výskytu k -tej farebnej zložky v obraze

1100 1000



Hodnoty pixelov:
Entropia:

200
 $H_{\min} = 0$

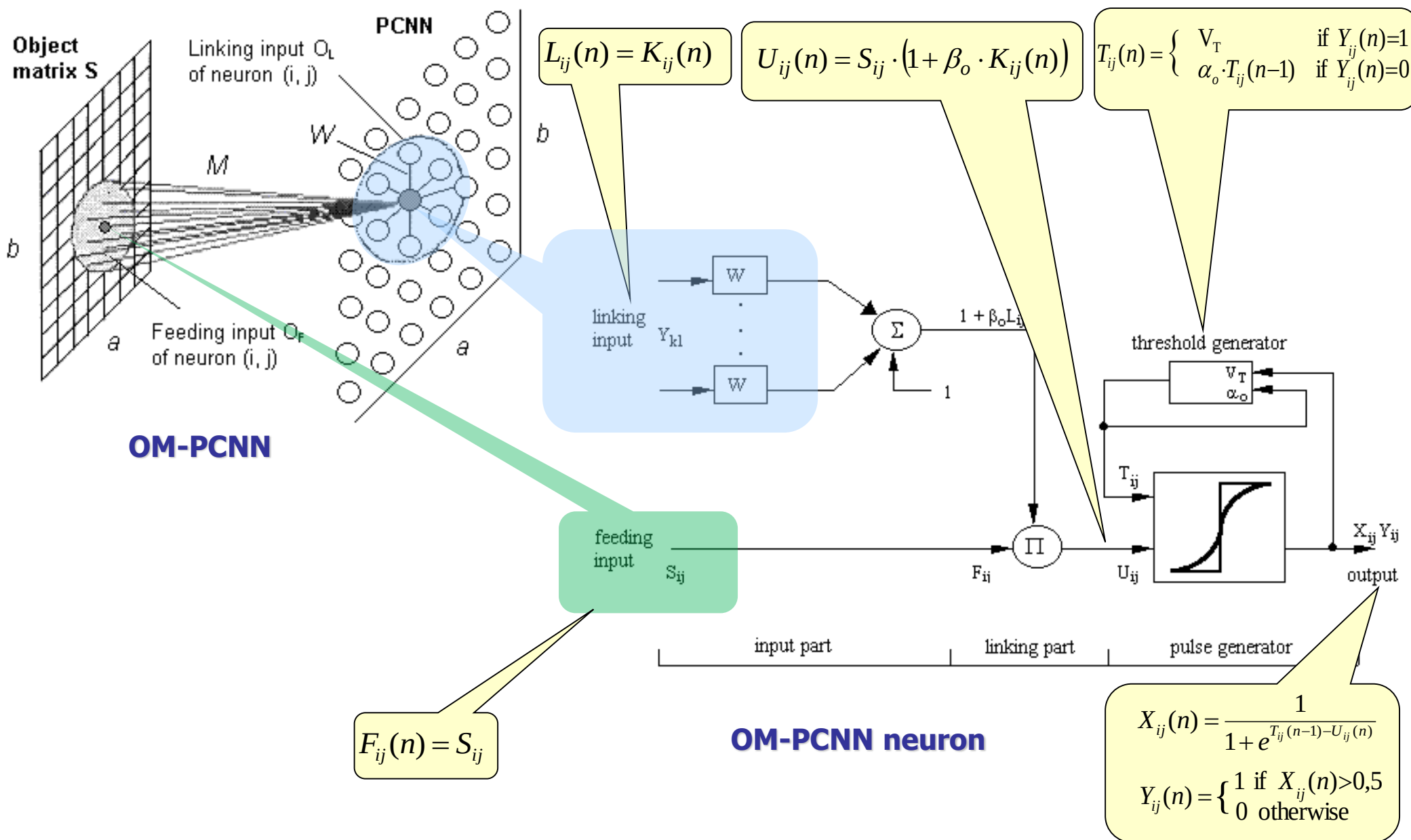
0 – 255
 $0 < H < 8$

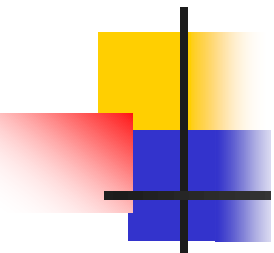
0 – 255
 $H_{\max} = 8$



- ❑ ***Nedetekovateľnosť*** – minimalizácia akéhokoľvek podozrenia, že je v obraze ukrytá správa
- ❑ ***Bezpečnosť*** – odolnosť steganografickej metódy voči stegoanalýze a stego útokom
- ❑ ***Robustnosť*** – odolnosť steganografickej metódy voči transformáciám v obraze a iným operáciám (zmena formátu súboru, pridávanie šumu, zmena mierky, rotácia, stratová kompresia, atď.)
- ❑ ***Kapacita*** – množstvo dát, ktoré možno ukryť v krycom obraze
 - závisí od veľkosti krycieho obrazu a použitej STG metódy

Optimalizovaný model PCNN (OM-PCNN)

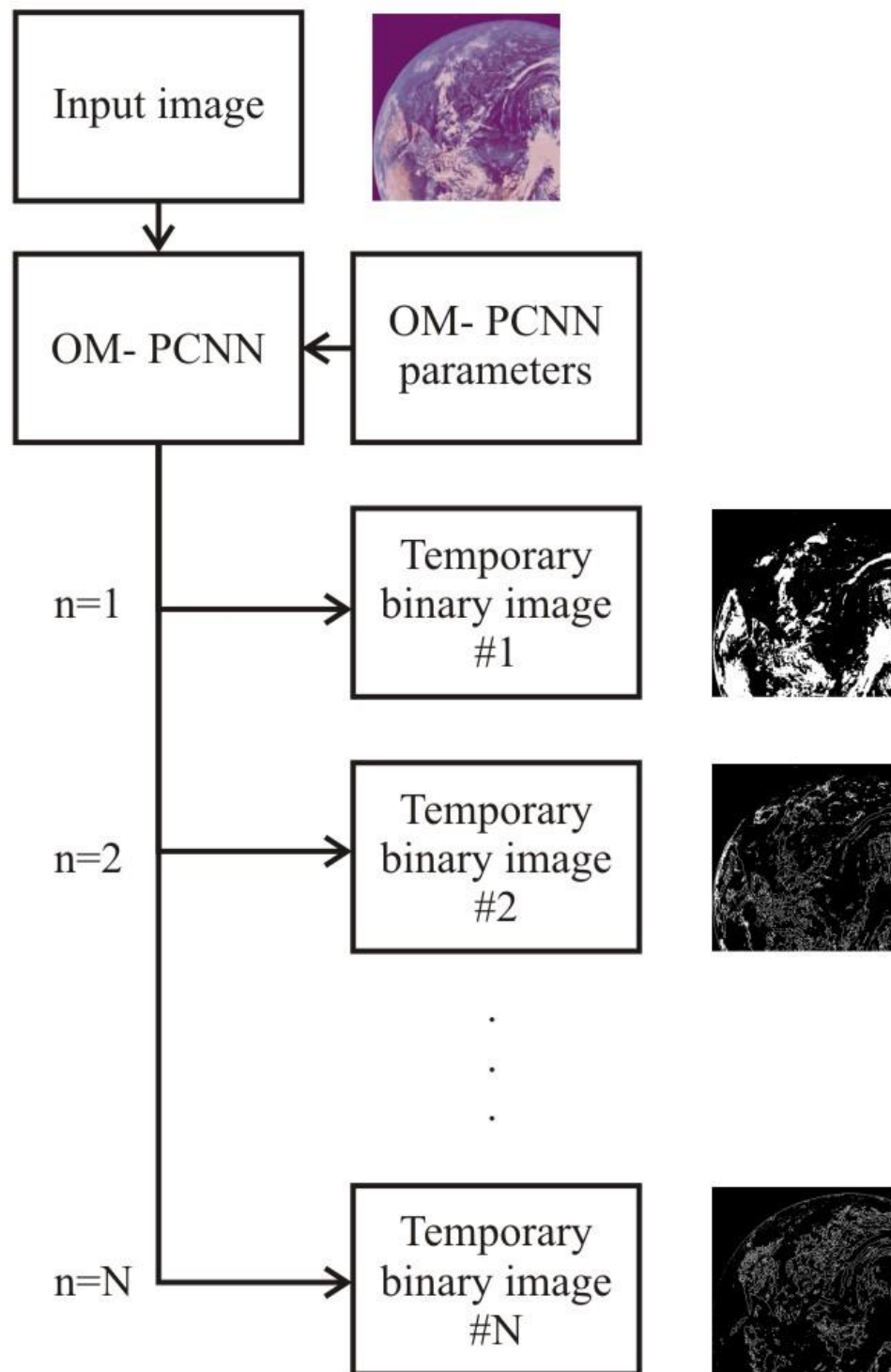
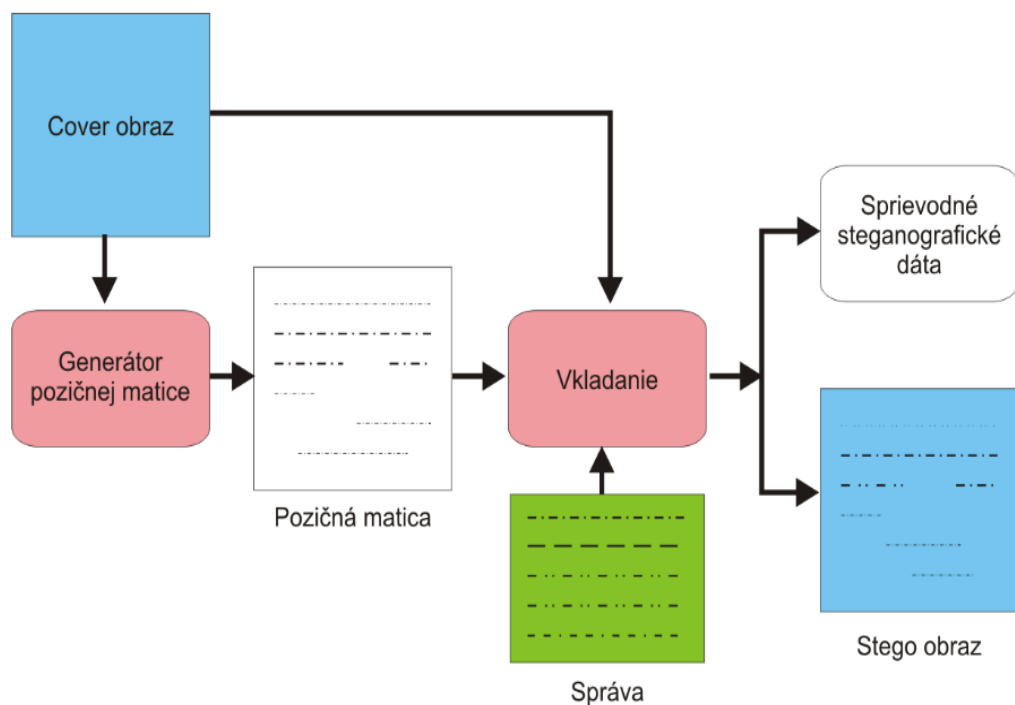




Neurónová sieť OM-PCNN ako generátor pozičnej matice

Pozičná matica

- šablóna na vkladanie ukrývanej správy

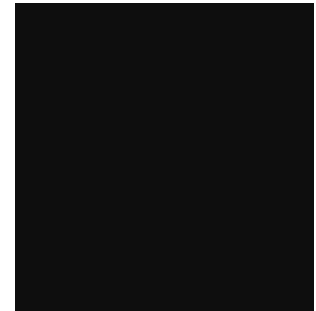
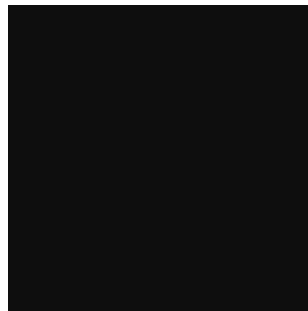
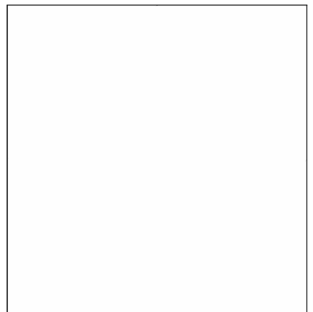
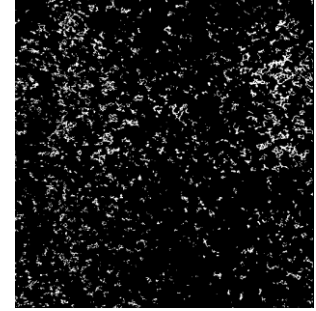
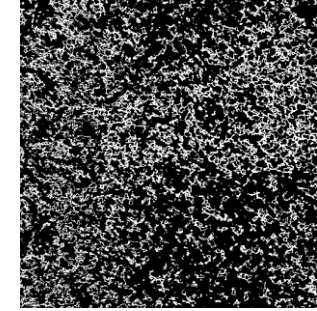
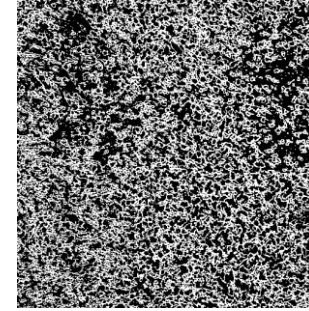
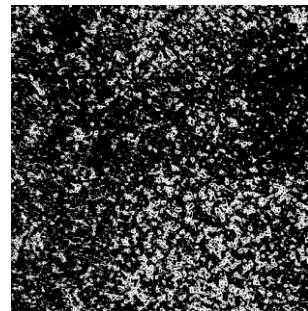
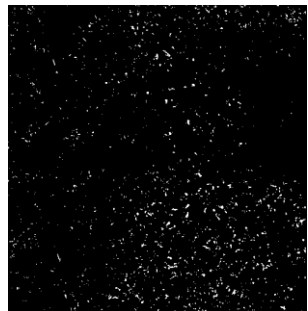
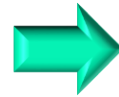
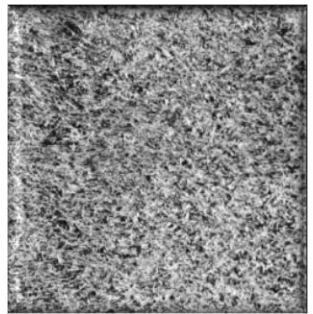
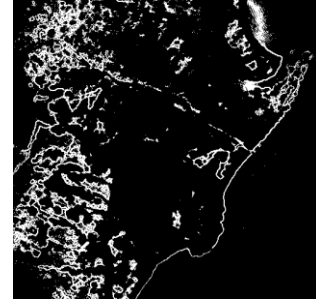
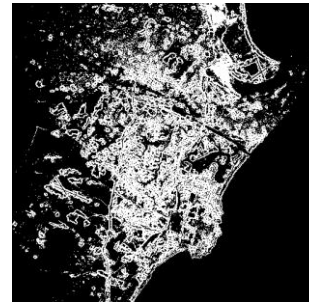
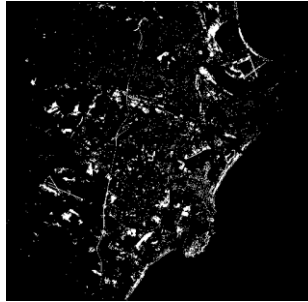
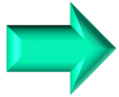


Odozva neurónovej siete OM-PCNN na obrazy s rôznou entropiou



Vstupné
krycie obrazy

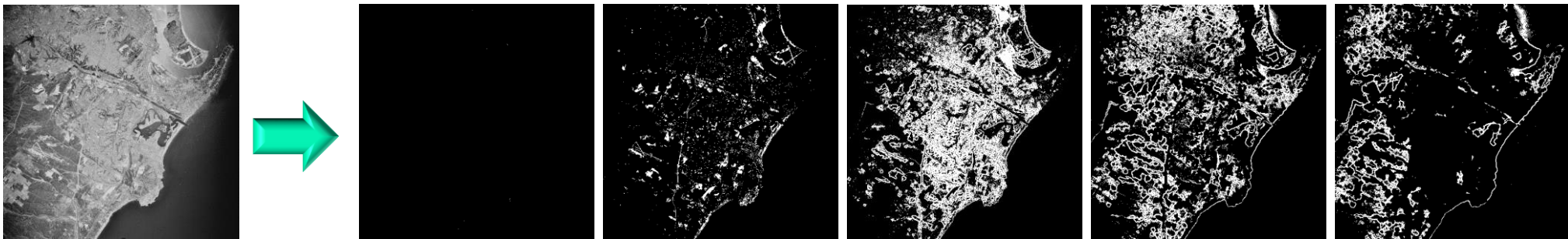
Výstupné binárne obrazy



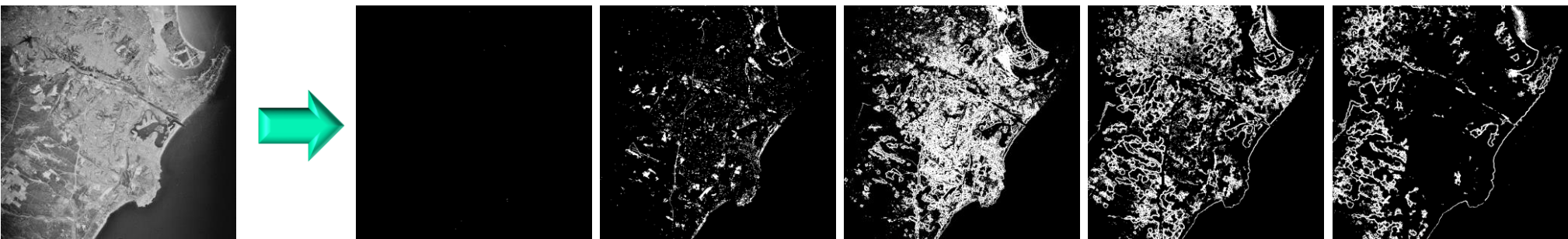
Odozva neurónovej siete OM-PCNN na veľkosť ukrývanej správy



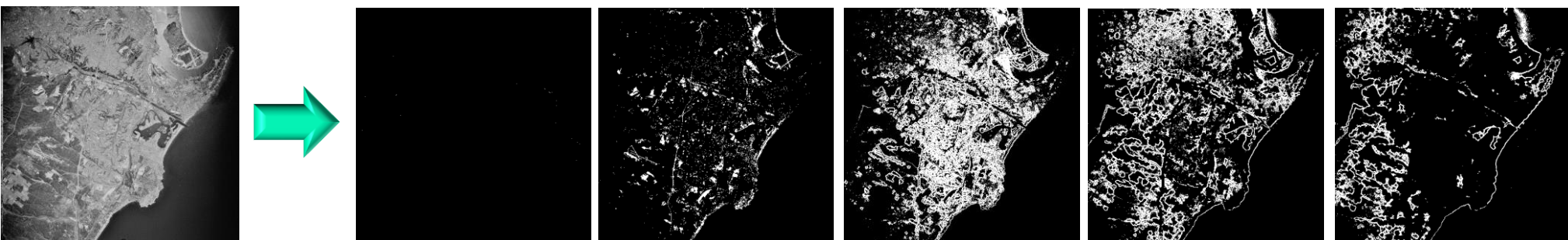
Krycí obraz 512x512 Prvých 5 binárných obrazov generovaných pomocou OM-PCNN

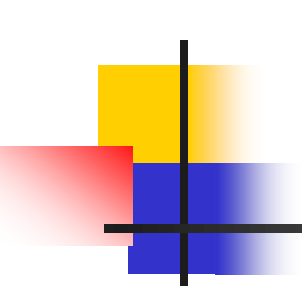


Stego obraz, do kt. bola vložená 30 bajtová správa (potrebná kapacita 240 pixelov)



Stego obraz, v ktorom boli „obsadené“ všetky pixely (veľkosť správy = 32 768 bajtov)





Význam obrazovej steganografie



Využitie

- ☐ Overovanie autenticity obrazov
- ☐ Overovanie autorstva
- ☐ Anotovanie obrazov
- ☐ Uchovávanie citlivých informácií v obrazoch
- ☐ ...
- ☐ ***Zdravotníctvo, armáda, ...***

Zneužitie

- ☐ utajená komunikácia teroristických a iných nežiaducich skupín
- ☐ šírenie detskej pornografie
- ☐ ...



Ďakujem za pozornosť