Šifrovací metoda založená na fraktální kompresi

Tomáš Grísa

ÚM FSI VUT v Brně

1.2.2012

Osnova

1. Základní matematické principy
   - Banachova věta o pevném bodu kontraktivního zobrazení
   - IFS, PIFS
2. Fraktální komprese obrazu
3. Šifrovací metoda založená na fraktální kompresi
   - Definice
   - Algoritmus
   - Jednoznačnost
   - Příklad
   - Výhody a nevýhody

Základní matematické principy

Definice: Nechť $(\mathcal{M}, d)$ je metrický prostor a $T : \mathcal{M} \to \mathcal{M}$. Zobrazení T nazveme kontraktivní právě tehdy, když existuje konstanta $c < 1$ taková, že:

$$d\left(T\left(x\right), T\left(y\right)\right) \leq c \cdot d\left(x, y\right) \qquad \forall x, y \in \mathcal{M}$$

Definice: Metrický prostor $(\mathcal{M}, d)$ nazveme úplným, jestliže každá Cauchyovská posloupnost je konvergentní.

Definice: Bod $x^* \in \mathcal{M}$ se nazývá *pevným bodem zobrazení* $T : \mathcal{M} \to \mathcal{M}$, jestliže $T\left(x^*\right) = x^*$.

Věta: Banachova věta o pevném bodu kontraktivního zobrazení
Buď $\mathcal{M}$ úplný metrický prostor a T kontraktivní zobrazení z $\mathcal{M}$ do $\mathcal{M}$. Potom T má právě jeden pevný bod.

Kolážová věta, IFS

Věta: Kolážová věta
Buď T kontraktivní zobrazení s koeficientem kontrakce c, a x^* pevným bodem zobrazení T. Potom platí:

$$d(x, x^*) \leq \frac{1}{1-c} \cdot d(x, T(x))$$

Definice: Buď $(\mathcal{M}, d)$ úplný metrický prostor, potom *iterujícím funkčním sytémem (IFS)* nazýváme konečnou množinu kontraktivních transformací $F = \{w_1, w_2, ..., w_n\}$ definovaných na $\mathcal{M}$.

Tvrzení: *Buď $(\mathcal{M}, d)$ úplný metrický prostor, potom $H(\mathcal{M})$ s* Hausdorffovou vzdáleností *d_h je úplným metrickým prostorem.*

IFS Věta

Věta: IFS věta

Je-li $(\mathcal{M}, F)$ *iterující funkční sytém, potom transformace* $\mathcal{W} : H(\mathcal{M}) \to H(\mathcal{M})$, *definovaná:*

$$\mathcal{W}(B) = \bigcup_{i=1}^{n} w_i(B)$$

pro všechna $B \in H(\mathcal{M})$ *je kontraktivním zobrazením na* $(H(\mathcal{M}), d_h)$ *s konstantou kontrakce* $c = \max\{c_1, ..., c_n\}$. *Pak tato transformace má jediný pevný bod* $A \in H(\mathcal{M})$, *který vyhovuje rovnici*

$$A = \mathcal{W}(A)$$

a je dán limitou

$$A = \lim_{i \to \infty} \mathcal{W}^i(B)$$

pro libovolné $B \in H(\mathcal{M})$.

PIFS

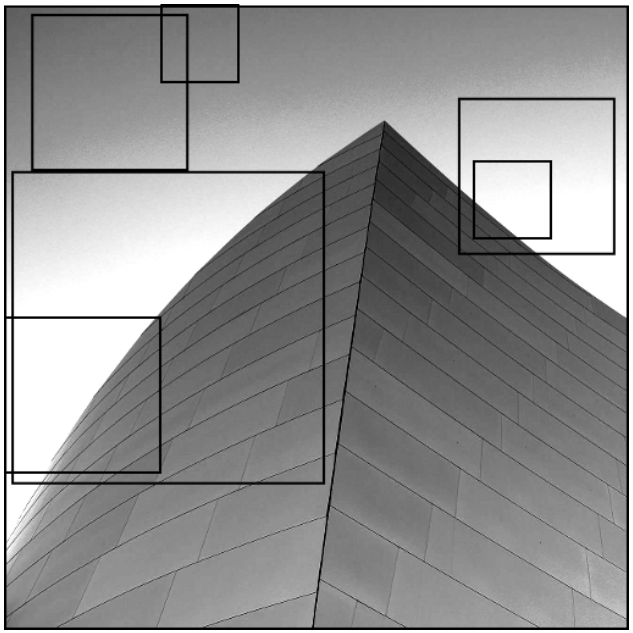
Definice: Buď X úplný metrický prostor, dále buď $D_i \subset X$ pro $i = 1, ..., n$. PIFS (*Partitioned Iterated Function Systems*) nazýváme množinu kontraktivních zobrazení $w_i : D_i \to X$, pro $i = 1, ..., n$.

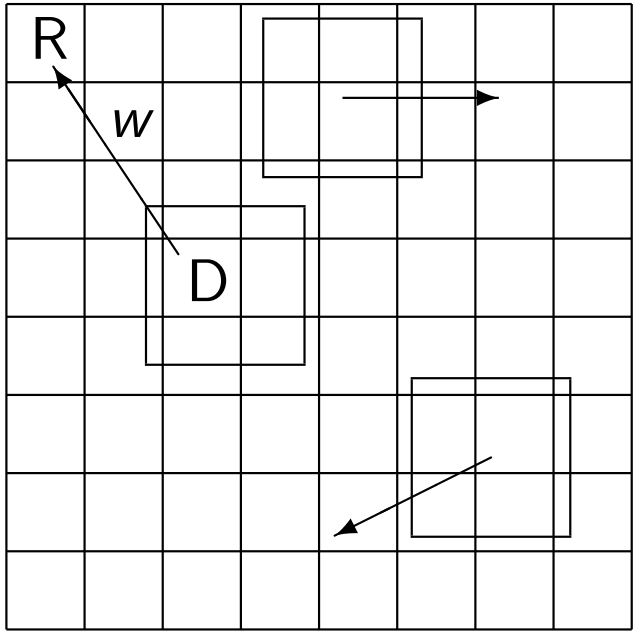
Poznámka: PIFS má také právě jeden pevný bod.

Fraktální komprese obrazu

Ztrátová kompresní metoda rastrové grafiky založená na hledání soběpříbuzných částí obrazu.

Využití kolážové věty: *Pokud vhodně pokryjeme množinu I obrazy sebe sama, které dostaneme pomocí transformací PIFS, potom atraktor tohoto PIFS vhodně aproximuje I.*





Šifrovací metoda založená na fraktální kompresi

Tvrzení: *Mějme následující celočíselné dělení*

$$a \ div \ b, a \in \mathbb{N}_0, b \in \mathbb{N} - \{1\}.$$

Potom v $\mathbb{N}_0$ *s klasickou metrikou je toto celočíselné dělení neexpanzivní, a podmíněně kontraktivní.*

Definice: Definujme zprávu $\mathcal{M}$ jako konečnou posloupnost čísel z intervalu přirozených čísel. Délku zprávy (počet prvků této posloupnosti) označme $|\mathcal{M}|$. $N - tý$ prvek zprávy označme m_n.

Definice: Definujme klíč $\mathcal{K}$ jako konečnou posloupnost celočíselných dvojic $[\delta, \kappa]$, kde δ je z intervalu přirozených čísel, a $\kappa \in \{2, 3, ..., 11\}$. Délku klíče (počet celočíselných dvojic této posloupnosti) označme $|\mathcal{K}|$. První prvek $n - té$ celočíselné dvojice klíče označme δ_n, druhý prvek této dvojice potom κ_n.

Algoritmus - šifrování

Buď $\mathcal{A}$ zpráva o délce $|\mathcal{A}|$, a $\mathcal{K}$ klíč délky $|\mathcal{K}|$. Buď $\mathcal{B}$ libovolná zpráva délky $|\mathcal{B}| = |\mathcal{A}|$.

1. Vytvoř novou (pomocnou) zprávu $\mathcal{E}$ o délce $|\mathcal{E}| = |\mathcal{A}|$ tak, že

$$e_n = \left(\left(b_{((n+\delta_j-1) \bmod |\mathcal{E}|)+1} \right) \operatorname{div} \kappa_j \right) + a_n,$$

$$j = ((n-1) \bmod |\mathcal{K}|) + 1.$$

2. Pokud

$$\sum_{i=1}^{|\mathcal{A}|} |b_i - e_i| = 0,$$

vrať $\mathcal{E}$ a ukonči výpočet. V opačném případě $\mathcal{B} = \mathcal{E}$ a jdi na bod #1.

Algoritmus - dešifrování, jednoznačnost

Nyní jsme schopni rekonstruovat zprávu $\mathcal{A}$ podle následujícího předpisu:

$$a_n = b_n - \left(\left(b_{\left(n+\delta_j\right) \bmod |\mathcal{E}|} \right) \operatorname{div} \kappa_j \right)$$

Tvrzení: *Nechť $\mathcal{A}$ je zpráva, $\mathcal{K}$ je klíč, a $\mathcal{E}$ je odpovídající zašifrovaná zpráva. Potom pro daný klíč $\mathcal{K}$ je zašifrovaná zpráva $\mathcal{E}$ jednoznačně určena, a je možno jí dosáhnout pouze z $\mathcal{A}$.*

Příklad

Zpráva: *CRYPTOGRAPHY IS THE PRACTICE AND STUDY OF TECHNIQUES FOR SECURE COMMUNICATION*

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
P	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**				
16	17	18	19	20	21	22	23	24	25	26	27			

Tabulka: Tabulka pro převod textu do číselné reprezentace.

$\mathcal{A} = \{3, 18, 25, 16, 20, 15, 7, 18, 1, 16, 8, 25, 27, 9, 19, 27, 20, 8, 5, 27, 16, 18, 1, 3, 20, 9, 3, 5, 27, 1, 14, 4, 27, 19, 20, 21, 4, 25, 27, 15, 6, 27, 20, 5, 3, 8, 14, 9, 17, 21, 5, 19, 27, 6, 15, 18, 27, 19, 5, 3, 21, 18, 5, 27, 3, 15, 13, 13, 21, 14, 9, 3, 1, 20, 9, 15, 14\}$

Příklad

Klíč: $\mathcal{K} = \{[11,2], [8,4], [19,3], [15,6]\}$

$\mathcal{E} = \{23, 21, 27, 21, 39, 21, 10, 19, 19, 19, 13, 26, 41, 11, 27, 28, 39, 10, 15, 31, 36, 22, 8, 6, 29, 15, 9, 6, 39, 8, 17, 6, 40, 24, 26, 24, 19, 29, 31, 18, 24, 29, 22, 6, 26, 12, 19, 14, 30, 24, 11, 21, 37, 8, 19, 19, 47, 23, 14, 6, 26, 22, 8, 30, 20, 18, 17, 16, 40, 20, 18, 7, 10, 22, 14, 19, 34\}$

Příklad

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**
P	Q	R	S	T	U	V	W	X	Y	Z		A	B	C
31	**32**	**33**	**34**	**35**	**36**	**37**	**38**	**39**	**40**	**41**	**42**	**43**	**44**	**45**
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
46	**47**	**48**	**49**	**50**	**51**	**52**	**53**							
S	T	U	V	W	X	Y	Z							

Tabulka: Tabulka pro převod zašifrované zprávy do textové reprezentace.

Zašifrovaná zpráva: *PVDRHRLTPRJZDMACXKNCSSLHDOFIIGWGC WVI HSQF FMJUKS KVOKXUHXJEXVPCKVRPIRSFGAQQS*

Výhody a nevýhody

Nevýhody:

- *rozsah znaků v zašifrované zprávě*
- *opakující se části u konstantních zpráv*

Výhody:

- *modifikace Vigenèrovy šifry*
- *soběpodobnost*

Šifrovací metoda založená na fraktální kompresi

Děkuji za pozornost...