Věříme, že jste se v předchozích dvou dílech našeho miniseriálu dostatečně namlsali – vždyť přinejmenším fantastické obrazy, jaké umí vyprodukovat fraktální geometrie, určitě stojí za podívání. Tentokrát už vizuální kreace opustíme a plně se věnujeme další možnosti jejího praktického využití. Možná budete překvapeni, je jí totiž šifrování.

Když rozkvetou fraktály... (3)

Šifrování je věda o utajování informace. Je stará téměř stejně jako umění písma. Už v prvopočátcích písemnictví, někdy před 4000 lety, se objevovaly tajné znaky, které byly určeny pouze pro určitou skupinu zasvěcených. Počátky šifrování v pravém slova smyslu lze datovat do 7. století př. n. l., kdy staří Řekové používali k šifrování mechanickou pomůcku – *scytalé*. Byla to hůlka určitého průměru, na kterou se (po šroubovici) těsně navinul kožený pásek. Na ten se podélně napsala zpráva a pásek se odvinul. Zpráva se pak dala přečíst jen po navinutí na hůlku o stejném průměru.

Mezi další nejstarší šifry lze zařadit i tzv. *Polybiův pochodňový dálnopis*, který byl založen na takovéto tabulce:

Vysílání probíhalo po písmenech tak, že na viditelném místě za dvěma neprůhlednými panely stála “obsluha”, která nad levý panel umístila tolik pochodní, jaké bylo pořadové číslo sloupce, ve kterém se nacházelo vysílané písmeno. Nad pravý panel se umístilo tolik pochodní, v kolikátém řádku se dané písmeno nacházelo. Tak se odvysílala celá zpráva. V době antického Říma se o pokrok v šifrování postaral sám Julius César. Jeho metoda spočívala v nahrazení každého písmene zprávy písmenem, které leželo v abecedě o tři písmena za ním.

Další vývoj byl spojen s rozvojem moderní diplomacie. Potřeba ochrany některých důležitých zpráv před nedovoleným otevřením a čtením si vynutila zaměstnávat ve státních, vojenských i církevních úřadech šifrovací úředníky.

K prudkému rozvoji kryptografie, který byl spjat s vynálezem telegrafu, pak došlo na počátku tohoto století a do konce padesátých let bylo vynalezeno velké množství mechanických šifrovacích strojů (například z 2. světové války známá *Enigma*).

Po zrodu počítačů v padesátých a šedesátých letech se kryptografie opět mění. Do té doby byla výhradní doménou diplomatických a vojenských kruhů, pro firmy a jednotlivce byla tato technologie prakticky nedostupná. To se v naší době zásadně změnilo. Kryptografie se stala veřejně používanou službou pro zajištění důvěrnosti a integrity informací. Vznikla řada šifer používajících zejména systémy s veřejným klíčem (pro potřeby bankovního sektoru apod.).

Dnes se věda o šifrování a dešifrování nazývá ***kryptologie*** a dělí se na ***kryptografii,*** zabývající se návrhem šifrovacích metod, a ***kryptoanalýzu***, která je zaměřena na studium metod luštění šifer.

Při návrhu šifrovacího systému je důležité dbát určitých zásad, která nám mohou pomoci při výběru správné šifry, protože ne vždy je vhodné použít co nejkomplikovanější systém. C. E. Shannon v r. 1940 formuloval tato nejdůležitější **kritéria pro posouzení kvality** šifrovacího systému:

spolehlivost – odolnost vůči rozluštění;

délka klíče – měla by být pokud možno co nejmenší;

složitost šifrování a dešifrování –závisí na stupni bezpečnosti;

šíření chyb – týká se systémů, u nichž zašifrování znaku závisí na zašifrování předcházejících znaků;

zvětšení zašifrovaného textu – přináší narušení statistického charakteru textu, avšak při omezené propustnosti přenosového kanálu mohou nastat problémy.

V dřívějších dobách bylo také nutno dodržovat tato pravidla:

nevysílat stejný text zašifrovaný různými klíči;

omezit používání velmi frekventovaných slov a frází;

omezit používání typických kombinací písmen, interpunkčních znamének a mezer.

Tato nejzákladnější pravidla byla vyvinuta už brzy po druhé světové válce a do dnešních dnů samozřejmě doznala značných změn. Nejsou samoúčelná, neboť při jejich nedodržení je riziko rozluštění textu velmi vysoké – zejména dnes, kdy se dešifrování zpráv svěřuje výkonným počítačům, které velmi rychle vyzkoušejí všechny známé “antišifry”. Například použije-li se jednoduchá Césarova šifra nebo jakákoliv jiná šifra, která nahradí otevřený text (originál) textem šifrovaným tak, že se přitom nepozmění statistická charakteristika jazyka, pak lze zprávu rozluštit už pomocí jednoduchých statistických analýz. Každý jazyk má totiž jistou charakteristickou četnost výskytu znaků v textech (obr. 1). Pokud se při šifrování použije pouze jednoduchá náhrada písmen otevřeného textu za šifrovaný (např. C za A, D za B, …), pak se histogram zprávy liší od histogramu otevřeného textu jen posunem sloupečků, který odpovídá posunu mezi abecedou textu otevřeného a zašifrovaného.

Tak primitivní šifrování dnes samozřejmě už nikdo prakticky nepoužívá a vznikají stále novější a sofistikovanější metody, u nichž jen pouhá logika (Césarova šifra, scytalé, …) dávno nestačí; ostatně čtenářům Chipu jistě není třeba moderní šifry zvláště představovat.

Mezi novodobé metody bezesporu patří i ***fraktální kódování*** a ***neurofraktální šifrování***. Jak už název napovídá, v obou metodách je použita fraktální geometrie; zajímavé však jistě je, že jejich pomocí lze provádět kódování a šifrování nejen obrazů, ale – na základě grafické podoby písmen – i textů. I když jde z hlediska moderní kryptologie v podstatě o **kuriozitu**, zdaleka ne tak “elegantní” jako jiné rigorózní metody, určitě stojí za zmínku.

Šifrování obrazů a textů

Jak už bylo řečeno, pomocí fraktální geometrie lze mnohé **obrázky** popsat velmi jednoduše, a to prostřednictvím několika čísel. Tato čísla (parametry *afinní transformace* – viz první část seriálu v Chipu 10/99) nám již mohou posloužit jako šifrovaná zpráva, která mimo jiné představuje i vysokou kompresi daného obrazu (např. fraktál Kapradina, který jsme rovněž představili v první části seriálu, lze popsat

pomocí 24 čísel, zatímco ve formátu BMP může jeho velikost dosahovat řádově až megabajtů; blíže o tom v další části seriálu – viz obr. 2). Výhodou takového přístupu je, že je těžko rozluštitelný – samozřejmě jen do té doby, dokud kryptoanalytik nezjistí, že k zašifrování byla použita fraktální geometrie. Ale i pak musí znát ještě další údaje, kterými lze dešifrování zpřesnit (nebo také znepřesnit). Například by musel vědět, jaké koeficienty byly ve zprávě použity (všechny, jen některé, …), zda byla použita ještě jiná metoda, která tyto koeficienty zašifrovala, musel by znát jejich pozici ve zprávě, atd.

K zakódování **textu** můžeme fraktální geometrii využít tak, že jednotlivá písmena abecedy (přesněji řečeno: jejich grafémy) popíšeme několika afinními transformacemi, čímž získáme vyjádření jednotlivých písmen prostřednictvím čísel. Základním tělesem, na něž budeme aplikovat afinní transformace, je zde černý čtverec. Například na obrázku 3 je grafická podoba písmene A, pro kterou jsme na tento čtverec aplikovali afinní transformace zmenšení a posun. Číselné vyjádření vygenerovaného písmene A (jsou to parametry **e** a **f** rovnice [1] v první části) pak vypadá takto:

0 0 0 0,2 0,2 0,4 0,4 0,6 0,6 0,8 0,8 0,8 1 1 1 1

0 0,2 0,4 0,2 0,6 0,2 0,8 0,2 0,6 0 0,2 0,4 1 1 1 1

Naše zakódované písmeno A je tedy vyjádřeno 32 čísly. Výhodou je vysoká robustnost vůči okolním vlivům, protože i při odchýlení čtverečků je písmo do určité míry stále čitelné.

Za velkou nevýhodu lze považovat redundanci (nadbytečnost) – všechna písmena musí totiž být vyjádřena pomocí vektorů o stejných rozměrech (vektory jsou doplněny jedničkami tak, aby počet prvků byl 32 v případě neurofraktálního šifrování).

Každé písmeno je takto popsáno šestnácti afinními transformacemi (32 čísel). Pak tedy např. věta *fraktaly jsou mnoziny jejichz geometricky motiv se opakuje v zakladnim telese az do nekonecna*, kterou vidite na obrázku 4, je jako zakódovaný text tvořena 2976 čísly (93 znaků x 32 čísel v transformačním vektoru).

Kódování pomocí fraktální geometrie je jednoduché a není tak časově náročné jako kódování obrazu – na zakódování textu totiž stačí použít jedinou iteraci, protože počet použitých iterací nemá rozhodující vliv na výslednou podobu zakódovaného textu. Pokud se použije iterací více, pak je text stále čitelný, jen jeho fraktální struktura vystoupí do popředí (obr. 5).

Prosté fraktální kódování má ještě jednu nevýhodu. Jedno písmeno je reprezentováno poměrně značným množstvím čísel. Na jedné straně reprezentace jednoho znaku pomocí velkého počtu čísel může být někdy výhodná (může to zdržet a zmást laického kryptoanalytika – v závislosti na jeho schopnostech, přístrojovém vybavení atd.), na straně druhé znamená redundanci, a tedy větší nároky na energii, čas a přenosové médium. Pokud nám tato redundance nevadí, můžeme kvalitu dosud popsaného kódování zvýšit následným použitím tzv. ***neurofraktálního šifrování*** (obr. 6).

Při neurofraktálním šifrování se z koeficientů afinních transformací sestaví *trénovací množina* a ta se předloží *neuronové síti* (srv. Chip 1/99) s tím, že jako výstupní vektory budou použity afinní transformace a jako vstupní vektory předem dohodnuté vektory. Neuronová síť pak veškeré informace, na které je učena, ukládá do svých vah – ty pak mohou být použity jako vlastní zpráva.

Pro lepší pochopení vezměme jednoduchý příklad. Představme si dva špiony 007 a 008. Agent 007 chce poslat zprávu agentovi 008 pomocí neurofraktálního šifrování. K tomu stačí, aby oba byli předem dohodnuti, jakou síť, strukturu a konstantní vstupní vektory použijí. Poté 007 napíše svou

zprávu, provede její fraktální zakódování a neuronová síť se naučí přiřazovat různé výstupy (nová zpráva) konstantním vstupům. Po naučení sítě vezme 007 množinu vah (na kterou může, ale také nemusí aplikovat další šifrovací mechanismus) a pošle ji 008. Ten ji prostě dosadí do svého dvojčete sítě 007 a předloží mu konstantní vstupní vektory. Síť s novými vahami (zašifrovaná informace) a dohodnutými vstupy tak dešifruje zprávu z matice vah. Tuto zprávu (výstupní vektory, tj. afinní koeficienty) je pak nutno ještě fraktálně dekódovat.

Aby takovou zprávu mohl dešifrovat nepřítel, musel by vědět, že se jedná o množinu vah neuronové sítě, musel by znát její topologii (počty neuronů v jednotlivých vrstvách, počet vrstev, typy přenosových funkcí v neuronech, způsob jejich propojení, …), vstupní vektory a také to, zda na tuto množinu vah byla použita další šifrovací metoda. Dále by musel vědět, že výstupní vektory sítě jsou koeficienty afinních transformací, a musel by znát jejich počet. Parametrů, které by musel znát, je tedy velice mnoho.

Výhodou této metody je, že je do jisté míry **tolerantní k chybám**. V klasických šifrovacích metodách je abeceda otevřeného textu nahrazována šifrovací abecedou. Tato náhrada je jednoznačná a jakákoliv odchylka znamená jinou interpretaci šifrovaného znaku, potažmo věty či celého textu.

U fraktálního kódování a neurofraktálního šifrování to – alespoň do určité míry – neplatí. I když při šifrování a dešifrování dojde k chybě (neuronová síť vždy pracuje s jistou chybou), pak po výsledném fraktálním dekódování dostaneme některá písmena třeba mírně pootočená či jinak zdeformovaná, ale pořád ještě čitelná (např. R, K na obr. 7).

Tato metoda samozřejmě není imunní proti všem stupňům možných deformací a chyb, nicméně je dostatečně robustní. Pokud by se stejná chyba vloudila do “klasického” šifrování, pak by takto poškozený kód mohl být nerozluštitelný i pro oprávněného příjemce (v závislosti na bezpečnostních algoritmech, které slouží k případné rekonstrukci poškozeného signálu).

Použití neuronové sítě na šifrování má samozřejmě také své nevýhody, například redundanci (nadbytečnost). Ta nastává, je-li počet vah v síti větší než součet všech prvků všech zakódovaných “fraktálních” vektorů. Pak dochází k tomu, že množina vah – šifrovaná zpráva – je větší než vlastní zpráva. Nicméně pokud tomu tak není, pak se nevýhoda obrací ve výhodu – dochází ke kompresi dat. To se týká hlavně textů. V případě kódování (viz další díl o fraktálech v počítačovém vidění) a šifrování obrazů dochází k mohutné kompresi objektů v obraze již při fraktálním kódování.

Jak je patrné z uvedených experimentů, fraktální kódování i neurofraktální šifrování je metoda, která by, jakkoli je kuriózní, mohla najít své uplatnění. A to navzdory tomu, že dnes existují mnohem výkonnější a odolnější metody šifrování.

Příště už náš krátký výlet do světa fraktálů ukončíme, a to možnostmi jejich využití v počítačovém vidění.

Ivan Zelinka (zelinka@zlin.vutbr.cz)