VRNITEV ARNOLDOVE MAČKE

MITJA LAKNER[1], PETER PETEK[2], MARJETA ŠKAPIN RUGELJ[1]

[1]Fakulteta za gradbeništvo in geodezijo, Univerza v Ljubljani
[2]Pedagoška fakulteta, Univerza v Ljubljani

Math. Subj. Class. (2010): 37D45, 94A60

Hiperbolična matrika določa preslikavo na torusu, vendar jo lahko opazujemo tudi na $N \times N$ rastru, kot je to napravil V. I. Arnold [2]. Opazoval je sliko mačke, ki se je po določenem številu iteracij vrnila. Zanima nas povezava med gostoto rastra in periodo vrnitve. To lastnost lahko uporabimo tudi za šifriranje in prikrivanje informacij.

RECURRENCE OF ARNOLD'S CAT

A hyperbolic matrix yields a mapping on the torus. However we can, as V. I. Arnold [2] did, consider the picture of the cat on $N \times N$ raster. After a certain number of iterations the cat returns. We are interested in the dependence of the period of return on the density of the raster net. The property of return can be used for coding and covering up information.

Uvod

V klasični mehaniki nastopajo posebni sistemi diferencialnih enačb – hamiltonski sistemi. Pojavljajo se npr. pri nebesni mehaniki ali pri dvojnem nihalu. Standardna obravnava [1] nas pripelje do prostorov v obliki večdimenzionalnih torusov. Lokalne rešitve sistema opišemo z matriko, ki ohranja ploščino. Matrika v eno smer razteguje, v drugo stiska in je *hiperbolična*, kar pomeni, da nima lastnih vrednosti dolžine ena. V nekem smislu ta hiperboličnost zagotavlja dobro mešanje slike. Ruski matematik V. I. Arnold je obravnaval take sisteme, posebej na dvodimenzionalnem torusu. Opazoval je zanimive lastnosti, kaj se zgodi na neki ekvidistantni mreži – rastru – na torusu. Točk na mreži je končno mnogo, matrika jih zgolj premeša, permutira med sabo. Po končnem številu korakov vsaka permutacija spet pripelje stvari v prvotno stanje.

Arnold, ki je imel rad slikovite prispodobe, je vzel sliko mačke, jo rastriral in iteriral preslikavo na torusu [2]. In mačka se je spet pojavila po določenem končnem številu korakov. Seveda je perioda odvisna od gostote rastra in to precej misteriozno.

Vsaj teoretično se da uporabiti to metodo za prikrivanje podatkov, steganografijo. Pri tem ni treba slediti prvotni Arnoldovi matriki, vsaka iz splošne linearne grupe nad celimi števili je dobra. In kot je navada že v kriptografiji, kjer si želijo velikih praštevil, si tukaj želimo dolgo periodo.

Sicer pa je, če jo opazujemo na celem torusu in ne le na rastrski mreži, preslikava *kaotična*. A o tem v prihodnjem članku.

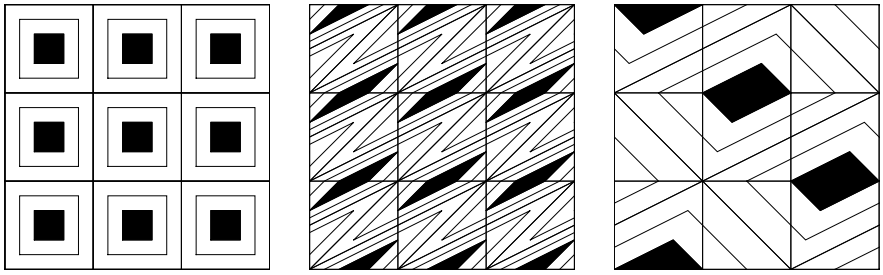
Hiperbolični avtomorfizmi torusa

Torus dobimo, če enotski kvadrat zlepimo po dveh vzporednih stranicah in isto naredimo še z nastalima krožnicama. To je vsebina naslednje definicije:

Definicija 1. Če v ravnini $\mathbb{R}^2$ identificiramo vse točke, katerih koordinate se razlikujejo za celo število, dobimo torus T.

Identifikacija definira ekvivalenčno relacijo na $\mathbb{R}^2$, kjer je $(x_1, y_1) \sim (x_2, y_2)$ natanko tedaj, ko sta $x_2 - x_1$ in $y_2 - y_1$ celi števili. Ta ekvivalenčna relacija določa projekcijo $\pi : \mathbb{R}^2 \to T$, $\pi(x, y) = [x, y]$.

Poglejmo si, kaj dobimo, če tlakovano celoštevilsko ravninsko mrežo preslikamo s celoštevilsko matriko dimenzije 2×2. Na sliki 1 na sredini vidimo, da pri množenju z matriko z determinanto 1 dobimo tlakovanje mreže s skladnimi »ploščicami«. Če pa ima matrika determinanto 2, so »ploščice« tlakovanja različne. Iz slike intuitivno sklepamo, da se je smiselno omejiti na matrike z determinanto ± 1.



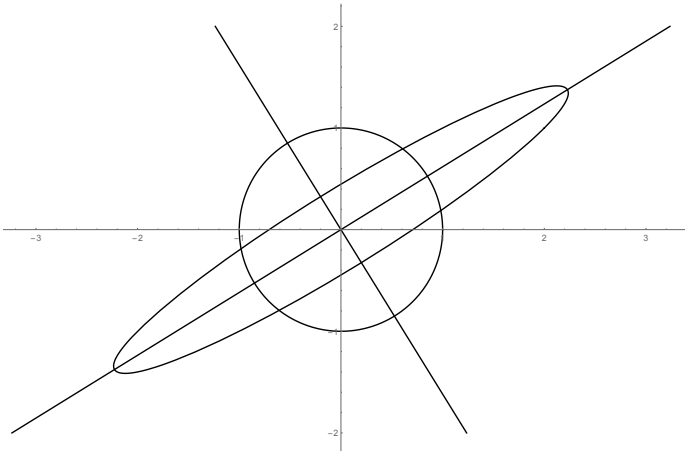
Slika 1. Tlakovanje ravninske mreže (na levi) in sliki mreže, če uporabimo matriki z determinanto 1 (na sredi) oz. 2 (na desni).

Definicija 2. Naj bo $A = (a_{ij})$ matrika dimenzije 2×2 z lastnostmi

(a) A je hiperbolična (lastni vrednosti ne ležita na enotski krožnici v kompleksni ravnini);

(b) $a_{ij} \in \mathbb{Z}$, $1 \leq i, j \leq 2$;

(c) $\det A = \pm 1$.



Slika 2. Slika krožnice pri množenju z matriko A.

Matrika A inducira tako preslikavo $L_A\colon T \to T$, da je $L_A \circ \pi = \pi \circ A$. To preslikavo imenujemo **hiperbolični avtomorfizem torusa**:

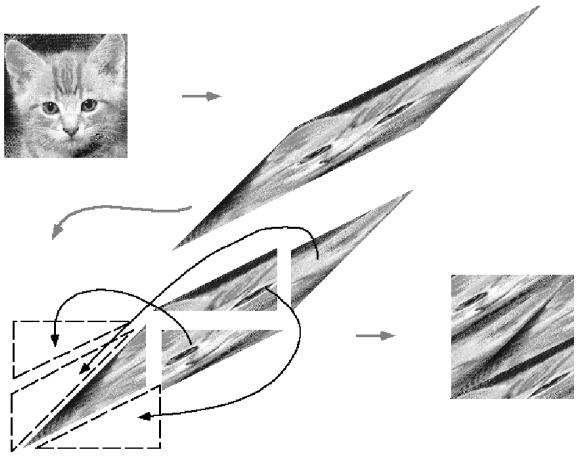
$$L_A([x,y]) \equiv A \begin{bmatrix} x \\ y \end{bmatrix} \pmod 1.$$

Opomba 1. Ker je $\det A = \pm 1$, je A^{-1} tudi hiperbolična in elementi matrike so cela števila. Torej A^{-1} tudi inducira hiperbolični avtomorfizem torusa $(L_A)^{-1}$.

Primer. Preslikavo L_A torusa, inducirano z matriko $A = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$, imenujemo preslikava Arnoldove mačke C_A [2]. Lastni vrednosti matrike A sta $\lambda_1 = \frac{3+\sqrt{5}}{2}$ in $\lambda_2 = \frac{3-\sqrt{5}}{2}$. Na sliki 2 vidimo, kam se pri množenju z matriko A preslika krožnica s središčem v izhodišču. Ker je $\det A = 1$, je C_A hiperbolični avtomorfizem torusa. Poglejmo, kam A preslika enotski kvadrat. Ker je

$$A \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 2 \\ 1 \end{bmatrix}, \quad A \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \quad A \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 3 \\ 2 \end{bmatrix},$$

se enotski kvadrat preslika v paralelogram enake ploščine (glej sliko 3). Na sliki 4 vidimo, kako se slika mačke, ki jo predstavimo s 124×124 točkami, razmaže po paralelogramu in po 15 iteracijah ponovno pojavi.



Slika 3. Avtomorfizem.

Izhodišče je edina negibna točka preslikave C_A. Bralec se lahko z uporabo popolne indukcije prepriča, da za potenco matrike A velja

$$A^n = \begin{bmatrix} F_{2n+1} & F_{2n} \\ F_{2n} & F_{2n-1} \end{bmatrix},$$

kjer je (F_n) Fibonaccijevo zaporedje s $F_0 = 0$, $F_1 = 1$ in $F_{n+1} = F_{n-1} + F_n$.

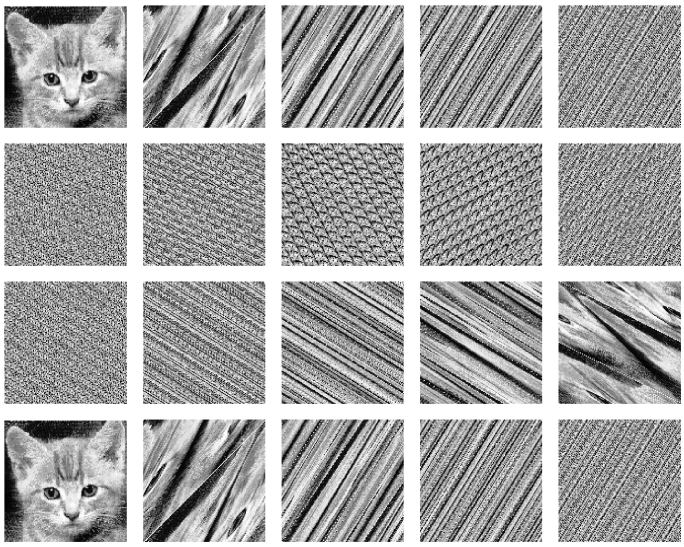
Resnično sliko predstavimo z $N \times N$ slikovnimi točkami, enakomerno razporejenimi v kvadratno mrežo. Naj bo $\Pi(N)$ najmanjše tako število, da je $A^k \equiv I \pmod N$. Potem se po $\Pi(N)$ iteracijah preslikave C_A vrne prvotna slika. Najbolj znan raster je $N = 124$, ko je $\Pi(124) = 15$ (slika 4).

Diskretna preslikava Arnoldove mačke

Diskretna preslikava Arnoldove mačke je podana s predpisom

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} \equiv A \begin{bmatrix} x_n \\ y_n \end{bmatrix} \pmod N, \tag{1}$$

kjer je $A = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$, in deluje na kvadratni mreži z $N \times N$ točkami, katerih koordinate so cela števila $0, 1, \ldots, N-1$. Naj točke pomenijo slikovne točke slike mačke. Vsaka iteracija točke pomeša med sabo. To vidimo takole: preslikava $(x, y) \mapsto (\frac{x}{N}, \frac{y}{N})$ preslika kvadrat $[0, N)^2$ bijektivno na $[0, 1)^2$. Ker π preslika kvadrat $[0, 1)^2$ bijektivno na torus T, kjer je L_A bijekcija, je diskretna preslikava Arnoldove mačke res permutacija.



Slika 4. Iteracija avtomorfizma.

Vprašanje pa je, koliko iteracij je treba, da zopet dobimo prvotno sliko. V matričnem zapisu to pomeni, da iščemo tako število $P = P(N)$, da bo $A^P \equiv I \pmod N$ (glej sliko 4). Število $P(N)$ imenujemo perioda, s $\Pi(N)$ pa označimo minimalno periodo, ko se slika ponovi. V primeru na sliki 4 je $\Pi(124) = 15$. Izkaže se, da minimalna perioda ni naraščajoča funkcija N ([6, 3, 4]). Slika 5 prikazuje minimalno periodo do vključno $N = 5000$.

Ker velja

$$A^n = \begin{bmatrix} F_{2n+1} & F_{2n} \\ F_{2n} & F_{2n-1} \end{bmatrix}, \tag{2}$$

kjer je (F_n) Fibonaccijevo zaporedje za $F_0 = 0$, $F_1 = 1$, sta perioda in minimalna perioda preslikave (1) odvisni od deljivosti Fibonaccijevih števil. Iz enačbe (2) sledi, da je število T perioda $P(N)$ preslikave (1), če in samo če velja

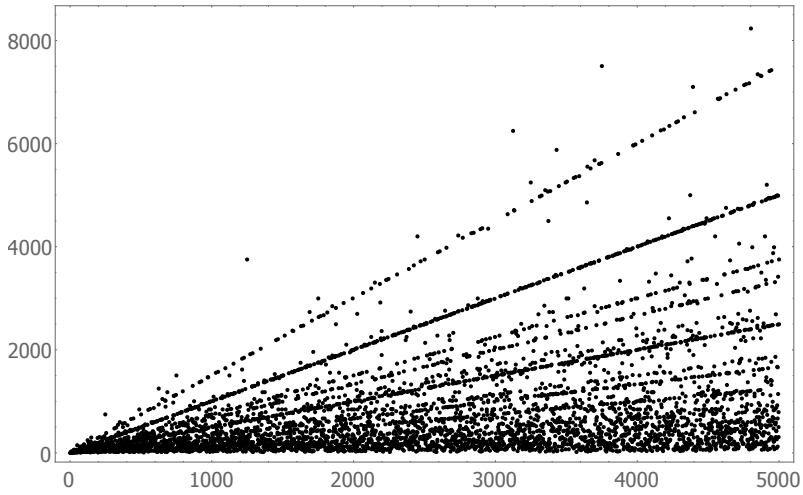
$$F_{2T-1} \equiv 1 \pmod N \text{ in } F_{2T} \equiv 0 \pmod N. \tag{3}$$

Pokažimo zelo grobo oceno za minimalno periodo.

Izrek 1. *Za poljubno sliko velikosti $N \times N$, kjer je $N \geq 3$, velja $\Pi(N) \leq \frac{N^2}{2}$.*

Za dokaz izreka potrebujemo tri kratke leme. Naj bo Φ_n najmanjši nenegativni ostanek F_n pri deljenju z N:

$$F_n \equiv \Phi_n \pmod N.$$



Slika 5. Minimalna perioda $\Pi(N)$. Na sliki opazimo premice, opisane v izrekih 6 in 7.

Primer. **(a)** Za $N = 2$ je zaporedje Φ_n periodično z minimalno periodo 3,

$$(0, 1, 1, 0, 1, 1, \ldots).$$

(b) Za $N = 7$ je zaporedje Φ_n periodično z minimalno periodo 16, $(0, 1, 1, 2, 3, 5, 1, 6, 0, 6, 6, 5, 4, 2, 6, 1, 0, 1, 1, 2, 3, 5, 1, 6, 0, 6, 6, 5, 4, 2, 6, 1, \ldots)$.

(c) Za $N = 11$ je zaporedje Φ_n periodično z minimalno periodo 10,

$$(0, 1, 1, 2, 3, 5, 8, 2, 10, 1, 0, 1, 1, 2, 3, 5, 8, 2, 10, 1, \ldots).$$

Lema 2. *Prvi par, ki se ponovi v zaporedju parov* $\langle \Phi_1, \Phi_2 \rangle, \langle \Phi_2, \Phi_3 \rangle, \ldots, \langle \Phi_n, \Phi_{n+1} \rangle, \ldots,$ *je par* $\langle 1, 1 \rangle$.

Dokaz. Ker je največ N^2 različnih parov, poljubna množica $N^2 + 1$ parov vsebuje vsaj dva enaka para. Pa recimo, da je prvi par, ki se ponovi, enak $\langle \Phi_k, \Phi_{k+1} \rangle$, kjer je $k > 1$. Poiščimo torej v zaporedju tak par $\langle \Phi_r, \Phi_{r+1} \rangle$, kjer je $r > k$, da velja $\Phi_k = \Phi_r$ in $\Phi_{k+1} = \Phi_{r+1}$. Iz definicije Fibonaccijevih števil sledi

$$\Phi_{r-1} = \Phi_{r+1} - \Phi_r$$

in

$$\Phi_{k-1} = \Phi_{k+1} - \Phi_k,$$

torej

$$\Phi_{r-1} = \Phi_{k-1}.$$

To pa pomeni, da je

$$\langle \Phi_{r-1}, \Phi_r \rangle = \langle \Phi_{k-1}, \Phi_k \rangle.$$

Toda $\langle \Phi_{k-1}, \Phi_k \rangle$ se v zaporedju pojavi pred $\langle \Phi_k, \Phi_{k+1} \rangle$. To pa je v nasprotju z našo predpostavko, da je $k > 1$. Torej je $k = 1$. ∎

Lema 3. *Za poljubno pozitivno celo število N obstaja med prvimi N^2 Fibonaccijevimi števili vsaj eno, ki je deljivo z N.*

Dokaz. Iz leme 2 sledi, da je $\langle 1, 1 \rangle$ prvi par v zaporedju, ki se ponovi. Torej je $\langle \Phi_t, \Phi_{t+1} \rangle = \langle 1, 1 \rangle$ za neko celo število t, $1 < t \leq N^2 + 1$. Potem je

$$F_t \equiv 1 \pmod{N}$$

in

$$F_{t+1} \equiv 1 \pmod{N}.$$

Toda

$$F_{t-1} = F_{t+1} - F_t$$

in zato je

$$F_{t-1} \equiv 0 \pmod{N}.$$

Naj bo $B = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$. Potem je $A = B^2$ in $B^n = \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix}$. ∎

Lema 4. *Naj bo $N > 2$. Če velja $F_n \equiv 0 \pmod{N}$ in $F_{n+1} \equiv 1 \pmod{N}$, potem je število n sodo.*

Dokaz. Lema je ekvivalentna trditvi, da za $N > 2$ iz $B^n \equiv I \pmod{N}$ sledi, da je n sodo število. Ker je $\det B = -1$, je $\det B^n = (\det B)^n = (-1)^n \equiv 1 \pmod{N}$. Torej je n sodo število. ∎

Dokaz izreka 1. Iz leme 2 in leme 3 sledi, da se vzorec $0, 1, 1$ v zaporedju

$$\Phi_0, \Phi_1, \Phi_2, \ldots, \Phi_n, \Phi_{n+1}, \ldots$$

prvič ponovi za $\Phi_{t-1}, \Phi_t, \Phi_{t+1}$, kjer je $0 < t - 1 \leq N^2$. Iz leme 4 sledi, da je $t - 1$ sodo število. Iz definicije minimalne periode pa dobimo, da velja $2\Pi(N) \leq 2\Pi(N) = t - 1$, kar dokazuje izrek. ∎

Za preslikavo (1) iz pogoja (3) in leme 4 sledi naslednja trditev:

Trditev 5. *Naj bo $N > 2$. Potem velja:*

(a) *T je perioda preslikave (1), če in samo če je $2T$ perioda zaporedja (Φ_n).*

(b) *T je minimalna perioda preslikave (1), če in samo če je $2T$ minimalna perioda zaporedja (Φ_n).*

Dyson in Falk [6] sta dokazala, da veljajo bistveno bolj stroge meje kot v izreku 1.

Izrek 6. **(a)** *$\Pi(N) = 3N$, če in samo če je $N = 2 \times 5^k$, kjer je $k = 1, 2, \ldots$*

(b) *$\Pi(N) = 2N$, če in samo če je $N = 5^k$ ali $N = 6 \times 5^k$, kjer je $k = 0, 1, 2, \ldots$*

(c) *$\Pi(N) \leq \frac{12N}{7}$ za vse preostale N.*

Primer. $\Pi(10) = 30$, $\Pi(5) = 10$, $\Pi(6) = 12$, $\Pi(30) = 60$, $\Pi(2) = 3$, $\Pi(3) = 4$.

Lastnosti, ki jih je Wall v članku [11] dokazal za periode zaporedij (Φ_n), sta Bao in Yang [3] z uporabo trditve 5 združila v naslednje izreke:

Izrek 7. *Naj bo N praštevilo, večje od 5. Potem za preslikavo (1) velja:*

(a) *Če je N oblike $10m \pm 3$, potem je $N + 1$ neka perioda preslikave (1).*

(b) *Če je N oblike $10m \pm 1$, potem je $\frac{N-1}{2}$ neka perioda preslikave (1).*

Primer. Minimalna perioda pa je lahko še bistveno manjša:
$\Pi(29) = 7$, $\Pi(47) = 16$, $\Pi(521) = 13$, $\Pi(9349) = 19$.

Izrek 8. *Če ima N praštevilsko faktorizacijo $N = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, potem je $\Pi(N)$ najmanjši skupni večkratnik števil $\Pi(p_1^{\alpha_1}), \ldots, \Pi(p_k^{\alpha_k})$.*

Se pravi, da moramo določiti $\Pi(N)$ le še za potence praštevil $N = p^M$. Pri tem je $p = 2$ poseben primer.

Izrek 9. *Če je $p = 2$, potem je $\Pi(2) = \Pi(4) = 3$. Za $M \geq 2$ pa je $\Pi(2^M) = 3 \times 2^{M-2}$.*

Primer. $\Pi(8) = 6$, $\Pi(16) = 12$, $\Pi(32) = 24$.

Za praštevila, večja od 2, računi kažejo, da je $\Pi(p^2) > \Pi(p)$. Velja pa

Slika 6. Skrivno sporočilo in njegov deseti iterat s preslikavo Arnoldove mačke.

Izrek 10. *Naj za praštevilo p velja $\Pi(p^2) \neq \Pi(p)$. Potem za $N = p^M$ velja $\Pi(N) = p^{M-1}\Pi(p)$. Če je k največje tako celo število, da velja $\Pi(p^k) = \Pi(p)$, potem je $\Pi(N) = p^{M-k}\Pi(p)$ za $M > k$.*

Primer. $\Pi(3) = 4$, $\Pi(9) = 12$, $\Pi(27) = 36$, $\Pi(7) = 8$, $\Pi(49) = 56$, $\Pi(343) = 392$.

Posplošena diskretna preslikava Arnoldove mačke

Če v enačbi (1) vzamemo matriko

$$A = \begin{bmatrix} 1+ab & a \\ b & 1 \end{bmatrix},$$

kjer sta a in b naravni števili, dobimo avtomorfizem torusa, saj sta lastni vrednosti različni realni števili, katerih produkt je enak 1. Tako dobljeno preslikavo imenujemo posplošena diskretna preslikava Arnoldove mačke. Posplošena preslikava se uporablja v kriptografiji in steganografiji.

Cilj kriptografíje (grško kryptós – skrit in gráphein – pisati) je narediti podatke neberljive, medtem ko je cilj kriptoanalize razkrivanje šifriranih podatkov [7]. Osnovno sporočilo po navadi imenujemo čistopis (cleartext, plaintext), zašifrirano pa šifropis ali tajnopis (kriptogram, ciphertext). Sporočilo po nekem algoritmu spremenimo v kriptirano sporočilo. Določene vrednosti parametrov, ki jih uporabimo v algoritmu, imenujemo ključ. Sogovornika se morata torej dogovoriti o algoritmu in ključu, da si lahko pošiljata šifrirana sporočila. V stari Grčiji so Špartanci sporočilo zakodirali tako, da

so na valj navili ozek trak in sporočilo napisali pravokotno na smer traku. Naslovniku so potem poslali odvit trak in če je želel sporočilo prebrati, je moral trak naviti na valj z enakim premerom. Ključ tega postopka je bil torej premer valja. Julij Cezar je sporočila svojim vojskovodjem zakodiral tako, da je vsako črko zamenjal s črko, ki je bila po abecedi nekaj mest za njo. Matematično tak način kodiranja lahko opišemo kot $f(a) \equiv (a + k) \pmod{n}$, kjer je n število črk v abecedi, k pa ključ. Takih sporočil ni težko dešifrirati, če uporabimo statistično analizo črk, značilnih za določen jezik. Iz daljšega besedila ugotovimo frekvenco določenih črk v jeziku in s primerjavo frekvenc črk v kodiranem besedilu lahko relativno hitro ugotovimo, katera črka pomeni določeno črko, in tako razšifriramo sporočilo. Skozi zgodovino so z uporabo matematike razvili različne postopke šifriranja. Pri moderni kriptografiji je algoritem kodiranja velikokrat znan, torej je poudarek kriptoanalize na odkrivanju ključa. Na Fakulteti za računalništvo v Ljubljani prof. dr. Aleksandar Jurišić vodi Laboratorij za kriptografijo in računalniško varnost in na strani `http://lkrv.fri.uni-lj.si/` je kar nekaj literature s tega področja.

Cilj steganografije (grško steganos – prikrit in gráphein – pisati) je prikrivanje obstoja podatkov [10]. Stari Kitajci so npr. sporočilo napisali na ozek svilen trak, ga tesno zvili, potopili v vosek in tako dobili voščene kroglice, ki jih je nato pogoltnil sel. Med najbolj znanimi metodami steganografije je zapis sporočila s črnilom, ki je pri normalni sobni temperaturi nevidno. Ko list papirja segrejemo, pa se sporočilo obarva rjavo. Kot črnilo lahko uporabimo na primer limonin sok, kis ali mleko.

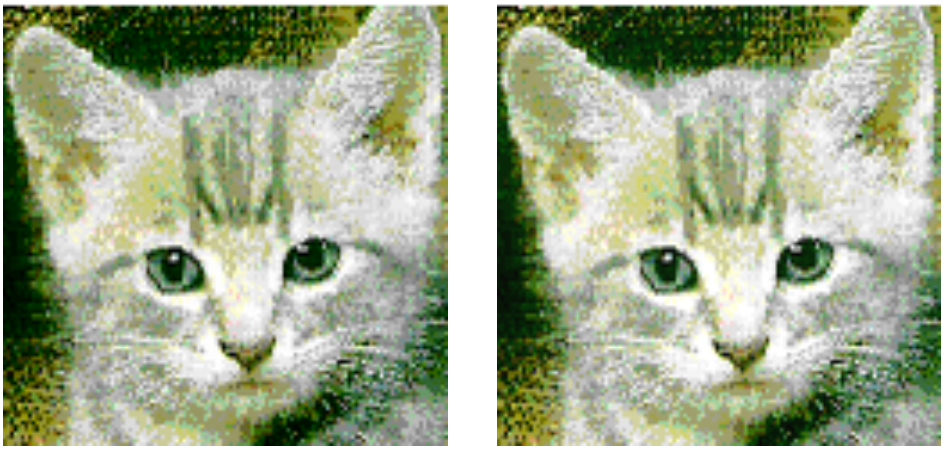
Ena od možnosti uporabe posplošene preslikave Arnoldove mačke v steganografiji je, da vzamemo sliko, ki ji dodamo skrivno sporočilo, ki ga pred tem transformiramo z eno ali več različnimi preslikavami [8], [9].

Spremenjeno sliko nato pošljemo tistemu, ki mu želimo sporočiti skrivno sporočilo. Z ustreznim ključem lahko naslovnik loči sliko od šifriranega sporočila. Pri tem je pomembno, da s prostim očesom ne ločimo originalne slike od slike z dodanim sporočilom, tako da slika ni sumljiva.

Ker je ranljivost algoritmov večja, če je perioda preslikave kratka, je zelo pomembno poznavanje periode v odvisnosti od parametrov a, b in N [4,5].

Primer. Na sliki 6 je skrivno sporočilo »OMF« in njegov deseti iterat.

Na sliki 7 je na levi originalna slika muce, na desni pa je slika muce z dodanim skrivnim sporočilom. Na vseh slikah je raster enak 124, zato je minimalna perioda $\Pi(124) = 15$. Če ima naslovnik, ki mu je sporočilo namenjeno, originalno sliko muce, lahko dobi šifrirano skrivno sporočilo. Če pozna še ključ, ki je v našem primeru zaporedna številka iterata, lahko dobi originalno skrivno sporočilo. Ker smo sliki dodali deseti iterat sporočila s preslikavo Arnoldove mačke, izračunamo peti iterat šifriranega sporočila.



Slika 7. Muca brez in s skrivnim sporočilom.

Nekaj nalog

1. Vzemimo za A osnovno Arnoldovo matriko in raster $N = 50$.
   (a) Koliko je $\Pi(50)$?
   (b) Kaj pa, če se vprašamo po minimalni potenci p, da je

$$A^p + I \equiv \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \pmod{N},$$

   seveda če tak p sploh obstaja?

2. Naj bo A posplošena Arnoldova matrika $A = \begin{bmatrix} 7 & 3 \\ 2 & 1 \end{bmatrix}$ in raster $N = 26$. Koliko je $\Pi(26)$? Kaj pa, če je raster $N = 124$?

3. Ali najdete še kakšno hiperbolično matriko, ki ni oblike $A = \begin{bmatrix} 1+ab & a \\ b & 1 \end{bmatrix}$?

4. Katera celoštevilska matrika dimenzije 2×2 ustreza enačbi $A^3 \equiv I \pmod 5$?

Rešitve:

1. (a) $\Pi(50) = 150$.
   (b) 75.
2. $\Pi(26) = 14$, $\Pi(124) = 14$.
3. Primera takih matrik: $\begin{bmatrix} 3 & 5 \\ 1 & 2 \end{bmatrix}$ in $\begin{bmatrix} 3 & 4 \\ 2 & 3 \end{bmatrix}$.
4. Primera takih matrik: $\begin{bmatrix} 1 & 1 \\ 2 & 3 \end{bmatrix}$ in $\begin{bmatrix} 2 & 1 \\ 3 & 2 \end{bmatrix}$.

LITERATURA

[1] V. I. Arnold, *Mathematical Methods of Classical Mechanics*, Springer, 1989.

[2] V. I. Arnold in A. Avez, *Ergodic problems in Classical Mechanics*, Benjamin, New York, 1968.

[3] J. Bao in Q. Yang, *Period of the discrete Arnold cat map and general cat map*, Nonlinear Dynam. **70** (2012), 1365–1375.

[4] F. Chen, K. Wong, X. Liao in T. Xiang, *Period distribution of generalized discrete Arnold cat map for $N = p^e$*, IEEE T. Inform. Theory **58** (2012), 445–452.

[5] F. Chen, X. Liao, K. Wong, T. Xiang, Q. Han in Y. Li, *Period distribution of some linear maps*, Commun. Nonlinear Sci. Numer. Simulat. **17** (2012), 3848–3856.

[6] F. Dyson in H. Falk, *Period of a Discrete Cat Mapping*, Amer. Math. Monthly **99** (1992), 603–614.

[7] *Kriptografija*, dostopno na: `http://www.egradiva.net/moduli/upravljanje\_ik/14\_kriptiranje/01\_datoteka.html`, ogled 3. 6. 2015.

[8] M. Mishra, A. R. Routray in S. Kumar, *High Security Image Steganography with Modified Arnold's Cat Map*, Int. J. Comput. Appl. **37** (2012), 16–20.

[9] S. Rawat in B. Raman, *A chaotic system based fragile watermarking scheme for image temper detection*, Int. J. Electron. Commun. **65** (2011), 840–847.

[10] *Steganografija*, dostopno na: `http://www.monitor.si/clanek/skrivanje-podatkov-steganografija/123365/?xURL=301`, ogled 3. 6. 2015.

[11] D. Wall, *Fibonacci series modulo m*, Amer. Math. Monthly **67** (1960), 525–532.