Masarykova univerzita
Fakulta informatiky

Extraktor entropie z mikrofonu a kamery pro mobilní telefon

Bakalářská práce

Roman Konečný

Brno, jaro 2013

Prohlášení

Prohlašuji, že tato bakalářská práce je mým původním autorským dílem, které jsem vypracoval samostatně. Všechny zdroje, prameny a literaturu, které jsem při vypracování používal nebo z nich čerpal, v práci řádně cituji s uvedením úplného odkazu na příslušný zdroj.

Roman Konečný

Vedoucí práce: Ing. Mgr. Zdeněk Říha, Ph.D.

Poděkování

Rád bych poděkoval vedoucímu své práce Ing. Mgr. Zdeňku Říhovi, Ph.D. za jeho pomoc při řešení této práce. Dále bych chtěl poděkovat rodině a přátelům za jejich podporu při studiu a v životě.

Shrnutí

Cílem této bakalářské práce je analýza zdrojů entropie, které má k dispozici mobilní telefon s operačním systémem Windows Phone 8. Součástí práce je aplikace, která demostruje získávání náhodných dat z dostupných zdrojů entropie.

Klíčová slova

extraktor entropie, Windows Phone 8, mobilní telefon, náhodná čísla

Obsah

Seznam obrázků

Seznam tabulek

Kapitola 1

Úvod

Potřeba generování náhodných čísel se objevila dávno před vznikem prvních počítačů, většinou šlo o hazard, např. hru v kostky. Postupem času, především s nástupem výpočetní techniky, se se rozšířila oblast, ve které se náhodná čísla uplatňují. Je však třeba vyřešit problém, kde náhodná data získat. Existují sice specializovaná zařízení, která jsou schopna registrovat a zaznamenat náhodné fyzikální jevy (atmosférický šum, rozklad radioaktivních prvků), jsou ovšem relativně drahá a rychlost, jakou jsou schopna náhodná čísla dodávat, nemusí být vždy pro potřeby dané aplikace uspokojivá. Proto byly vyvinuty speciální algoritmy, které dovedou generovat takzvaná pseudonáhodná čísla. Algoritmus na vstupu dostane semínko, což je malý vzorek náhodných dat, a z něj generuje posloupnost pseudonáhodných čísel. Kvalita posloupnosti je ovlivněna jak použitým algoritmem, tak kvalitou samotného semínka. S příchodem chytrých mobilních telefonů se potřeba generování náhodných čísel pro další použití rozšířila i na tyto přístroje.

Většina operačních systémů, které mobilní telefony v dnešní době používají, má v sobě zabudovanou funkci, obvykle se označuje jako Random(), která dokáže generovat pseudonáhodná data a kterou mohou programátoři ve svých programech použít. Kvalita takto získaných dat ovšem nemusí vyhovovat některým aplikacím (jako příklad se dají uvést kryptografické programy) a může se tedy stát, že se funkce ze systémových knihoven nemůže použít. V tom případě je nutné napsat vlastní generátor vyhovující podmínkám, jež jsou na něj kladeny. Důležité je především získání náhodných dat pro potřeby semínka generátoru. Podobné téma bylo několikrát řešeno pro operační systém Symbian [1, 2], ne však pro platformu Windows Phone 8, kterou se zabývá tato bakalářská práce.

Cílem práce je tedy analyzovat dostupné zdroje entropie (náhodnosti), jež nabízí mobilní telefony s operačním systémem Windows Phone 8, a získat z nich data, jež mohou být použita pro semínko generátoru pseudonáhodných čísel. Jelikož se jedná o velmi mladou platformu, která byla představena teprve v říjnu roku 2012, práce se jednou kapitolou věnuje systému Windows Phone 8, především jeho srovnání s konkurenčními mobilními operačními systémy a způsobu, jakým se pro tento systém vyvíjí aplikace. Těžištěm práce jsou pak kapitoly, které se zabývají popisem programu pro sběr náhodných dat a jejich následnou analýzou. V následujícím odstavci je naznačen způsob, z jakých fází se celý proces skládá i se stručným popisem.

Nejdříve je třeba získat informace o tom, jaké zdroje náhodnosti se u zařízení se systémem Windows Phone 8 nachází a jsou k dispozici. Seznam dostupných zdrojů je pak použit k vytvoření programu, který data z těchto zdrojů sbírá a následně je ukládá do textových souborů. Pro každý zdroj je vytvořeno více souborů, data jsou totiž zpracovávána za různých podmínek, např. mikrofonem se dají získávat data za úplného ticha, při běžné úrovni hluku nebo při velmi nahlas puštěné hudbě, obdobným způsobem se vytváří soubory s daty i pro ostatní zdroje. Poté se soubory zkopírují do počítače, kde se programem určí míra entropie jednotlivých případů. Je nutné podotknout, že program musí být pro každý zdroj upraven, ne všechna data jsou totiž ve stejném formátu, velmi se liší např. výstupy senzoru pohybu a kamery.

Kapitola 2

Platforma Windows Phone 8

2.1 Úvod

Windows Phone 8 je druhá generace operačního systému pro chytré mobilní telefony (anglicky smartphones) Windows Phone od společnosti Microsoft. Je nástupcem populárního Windows Mobile a Windows Phone 7, avšak ani s jedním z těchto systémů není zpětně kompatibilní. Aplikace napsané pro Windows Phone 7 ovšem bez problémů běží i na verzi 8 [3]. Přístroje s tímto operačním systémem na trh dodává několik renomovaných výrobců mobilních telefonů, např. finská Nokia, tchajwanské HTC či jihokorejský Samsung.

2.2 Ostatní mobilní OS

V následujících odstavcích se pokusím trochu přiblížit i jiné mobilní platformy. Jedná se spíše o informativní výčet než vyčerpávající popis. Nejsou zde uvedeny všechny mobilní operační systémy, chybí např. webOS, Maemo nebo Firefox OS[1].

2.2.1 Windows Mobile

Mobilní operační systém od společnosti Microsoft, jedná se o předchůdce platformy Windows Phone. Jeho vznik se datuje k roku 1999 a ve vývoji byl až do roku 2010, kdy ho nahradil Windows Phone 7. Windows Mobile je založen na Windows CE, což je operační systém pro přenosná zařízení, zejména PDA[2]. Ačkoliv by se dal Windows Mobile označit za předchůdce Windows Phone 8, jedná se o naprosto odlišný systém s odlišným jádrem, ovládáním[3] i uživatelským rozhraním. To má evokovat vzhled starších verzí operačního systému Windows, zejména ve verzích 2000 a XP, zatímco Windows Phone využívá tzv. Modern UI, dříve označované jako Metro, které je využíváno i v nejnovějším operačním systému pro osobní počítače a tablety, Windows 8. Programy pro Windows Mobile jsou napsány v C++ (případně na platformě .Net).

1. K dubnu 2013 ovšem ještě nebyl na trh uveden žádný telefon s tímto systémem.
2. Personal Digital Assistant.
3. Windows Mobile nepodporuje ovládání více prsty, tzv. multitouch, obvyklé je též ovládání zařízení pomocí speciální tužky, označované jako stylus.

2.2.2 Symbian

V minulosti velmi populární operační systém, používaný zejména v mobilních telefonech značky Nokia. Jedná se o otevřený systém s velkou komunitou, kterou zastupoval Symbian Limited, v roce 2008 odkoupen Nokií, která se stala hlavním propagátorem a inovátorem Symbianu. Na podzim roku 2011 však Nokia ohlásila, že přechází na Windows Phone [4] a i díky nástupu zařízení s operačním systémem Android se Symbian postupně propadal v prodejnosti a nyní je vnímán spíše jako obstarožní platforma bez vyhlídky na lepší budoucnost. Programovat pro Symbian je možno v jazyce C++, Java, Python nebo C#.

2.2.3 Bada

Operační systém, užívaný mobilními telefony značky Samsung. Na trh se tento systém dostal v roce 2010 a stal se poměrně populárním, neboť byl určen pro běžného uživatele. Jelikož však Samsung nabízí i telefony s jinými operačními systémy, jmenovitě Android a Windows Phone, chytré telefony se systémem Bada jsou spíše zaměřeny na levnější segment trhu. V roce 2012 byl navíc ohlášen konec vývoje systému s příslibem vzniku nového operačního systému s názvem Tizen [5], který by měl být schopný spouštět i aplikace pro OS Bada. Žádné další informace však nejsou známé. Aplikace pro Badu se vyvíjí v jazyce C++.

2.2.4 BlackBerry OS

Mobilní operační systém vyvíjený firmou BlackBerry Limited[4], určený pouze pro mobilní telefony řady BlackBerry. První telefon s tímto systémem byl uveden v roce 1999, poslední aktualizace BlackBerry OS pak byla v roce 2012. Na začátku roku 2013 se objevil nový operační systém, BlackBerry 10, který má původní systém nahradit. Telefony BlackBerry byly populární zejména ve firmách a zejména u manažerů, neboť nabízely šifrovanou komunikaci a fyzickou QWERTY klávesnici. S uvedením nového operačního systému BlackBerry 10 však společnost cílí i na běžné uživatele a konkuruje tak výrobcům telefonů s operačními systémy Android, iOS a Windows Phone. Aplikace se píší v jazyce Java.

2.2.5 Android

Mobilní operační systém od společnosti Google Inc., známý především kvůli své otevřenosti a nasazení na velké množství různých zařízení [5]. První telefon s tímto operačním systémem byl uveden v roce 2008 a od té doby se Android stává stále populárnějším [6], především díky tomu, že se vyskytuje jak v drahých telefonech, tak i v levných zařízeních. Aplikace pro Android se mohou psát v jazycích C, C++ nebo Java.

4. Dříve Research in Motion.
5. Android není pouze operační systém pro chytré telefony a tablety, je možné na něj narazit i v TV boxech, digitálních fotoaparátech nebo GPS navigacích.

2.2.6 iOS

Operační systém společnosti Apple Inc. pro telefony iPhone, mp3 přehrávače iPod Touch, tablety iPad a iPad Mini a digitální mediální přijímač Apple TV. Jedná se o uzavřený systém, vyvíjí se v C, C++ nebo Objective-C, pro vývoj je třeba vývojové prostředí XCode, dostupné pouze pro operační systém Mac OS X. Distribuce aplikací probíhá výhradně přes oficiální Apple App Store. Představen byl v roce 2007, tehdy se ještě jmenoval iPhone OS, v roce 2010 byl pak systém přejmenován na iOS. Ačkoliv se jedná o uzavřený systém určený pouze pro výše uvedené zařízení, iOS je velmi rozšířený a populární. Hlavní podíl na tom má velmi příjemné uživatelské rozhraní a jistá exkluzivita produktů firmy Apple. Spolu s Androidem soupeří o první místo v operačních systémech určených pro mobilní zařízení, poslední dobou však Android získává přesvědčivé vedení, hlavně díky velké nabídce zařízení, které operační systém od Googlu používají [7].

2.3 Historie Windows Phone

Windows Phone 8 je přímým nástupcem Windows Phone 7, jehož vývoj začal v roce 2008 jako nástupce systému Windows Mobile 6 a který měl být vydán v roce 2009, avšak nakonec byl po několika odkladech představen až v roce 2010 (v mezičase vyšla poslední aktualizace Windows Mobile, verze 6.5). Tento systém je z grafického hlediska velmi podobný WP 8, avšak mají odlišné jádra, zatímco tedy Windows Phone 8 používá jádro Windows NT, předchůdce v sobě obsahuje starší jádro Windows CE. V květnu 2011 byla uvedena aktualizace Windows Phone 7 s kódovým označením „Mango“ neboli Windows Phone 7.5, která přinesla některá důležitá vylepšení, jako např. podporu více najednou běžících aplikací třetích stran nebo integraci služby Skydrive. S další verzí s označením „Tango“ se kromě opravy chyb snížily nároky na zařízení (jednojádrový procesor o taktu 800 MHz a 256 MB RAM), což zapříčinilo vydání nových telefonů, které mířily do nižších cenových kategorií[6]. Systém Windows Phone 8 byl na trh uveden na konci října roku 2012, první aktualizace „Portico“ pak byla vydána v říjnu toho roku a kromě opravy chyb přinesla několik vylepšení, z nichž nejvýznamnější je možnost být připojen na WiFi i při zamknutém telefonu. Windows Phone 7 se pak zpětně dočkal verze 7.8, která se ve vlnách začala dostávat k uživatelům od ledna 2013. Tato aktualizace přináší některé funkce, které byly přeneseny z Windows Phone 8. Do budoucna se pak plánuje větší aktualizace pro WP8 s označením Blue s tím, že se systém před vydáním této verze dočká několika menších opravných a vylepšujících balíčků.

2.4 Technologický přehled

Na rozdíl od iOS, kde je jediným výrobcem přístrojů s tímto systémem sám Apple, Windows Phone je dodáván na vícero zařízeních různých výrobců. Tím je spíše podobný operačnímu systému Android, od kterého se ovšem liší tím, jak moc je restriktivní k výrobcům. Zatímco

6. Např. Nokia Lumia 610.

tedy telefony s Androidem mohou být velmi odlišné jak ve výkonu, tak v rozlišení obrazovky a velikosti, základní kostra pro WP 8 je pevně dána. Je však nutno podotknout, že na rozdíl od iOS a Androidu není platforma Windows Phone určena k použití na tabletech. Zde jsou uvedeny minimální požadavky na zařízení s Windows Phone 8 [8]:

- Qualcomm Snapdragon S4 dvojjádrový procesor;
- minimálně 512 MB RAM pro telefony s WVGA rozlišením (480 x 800 px), minimálně 1024 MB RAM pro telefony s rozlišením 720p (720 x 1280 px) nebo WXGA (768 x 1280 px);
- minimálně 4 GB flash paměti;
- geolokační služby (GPS a A-GNSS, popř. GLONASS);
- podpora micro-USB verze 2.0;
- 3,5 mm stereofonní výstup na sluchátka s podporou rozpoznávání až tří tlačítek (předchozí, pauza, další);
- zadní kamera s automatickým ostřením a bleskem, volitelná přední kamera (obě s minimálně VGA rozlišením, tedy 640 x 480 pixelů), samostatné tlačítko spouště fotoaparátu;
- akcelerometr, světelný senzor a senzor přiblížení (kompas a gyroskop jsou volitelné senzory);
- 802.11b/g WiFi (volitelně také 802.11n) a Bluetooth;
- grafická karta podporující DirectX s hardware akcelerací Direct3D;
- kapacitní dotyková obrazovka s rozpoznáváním minimálně čtyř dotyků zároveň.

Windows Phone 8 v současnosti podporuje tři rozlišení obrazovky, a to sice 480 x 800 px[7], 720 x 1280 px a 768 x 1280 px. Liší se tedy jak počtem obrazových bodů, tak i poměrem stran, není ovšem zapotřebí aplikace přepisovat pro každé rozlišení zvlášť, systém dokáže program napsaný pro jakékoliv rozlišení správně překreslit do rozlišení jiného.

Mezi zajímavosti systému patří podpora SD karet. Ta je totiž velmi sporná, z karty je možno číst, pokud to aplikace umožňuje, není ale možné na ni cokoliv zapsat s výjimkou fotek a videí. Není tedy možné např. nainstalovat aplikaci na paměťovou kartu nebo z ní číst podklady pro offline navigaci.

7. Jediné podporované rozlišení Windows Phone 7 [9].

Obecně se dá říct, že vybavenost systému je standardní, většina funkcí je podporována i ostatními mobilními operačními systémy. Za zmínku stojí absence FM rádia, naopak vyzdvihnout by se dala podpora NFC[8] a vzhledem k jádru Windows NT 128b šifrování pomocí technologie Bitlocker.

2.5 Vývoj aplikací pro Windows Phone 8

Aplikace pro Windows Phone 8 se dají vyvíjet v několika jazycích, a to sice ve Visual Basicu, C, C++ a C#. Pro popis grafického uživatelského rozhraní se používá jazyk XAML[9]. Ten je používán i při tvorbě okenních aplikací pro novější operační systémy z rodiny Microsoft Windows (od verze Vista výše), konkrétně při použití WPF[10]. Místo XAML se dá využít knihovna Direct3D, která je využívána zejména programátory v jazyce C++ a je vhodná především pro tvorbu her.

K vývoji programů pro platformu Windows Phone 8 se používá vývojové prostředí Microsoft Visual Studio 2012, k návrhu grafického uživatelského rozhraní se pak kromě vestavěného návrháře Visual Studia může použít nástroje Blend, který má rozšířenou nabídku funkcí. Tyto nástroje jsou dostupné pouze pro operační systém Microsoft Windows. Visual Studio se nabízí ve vícero verzích, pro vývoj aplikací pro Windows Phone 8 pak postačí základní edice Express, která je k dispozici zdarma i pro komerční použití. Tato verze je pak obsažena spolu s programem Blend a dalšími pomocnými nástroji, jakými jsou například Isolated Storage Explorer (program pro procházení souborů na paměťovém úložišti telefonu), či Windows Phone Emulator (emulátor fyzického zařízení, určené pro testování) v balíku Windows Phone 8 SDK tools. K použití emulátoru je zapotřebí vlastnit procesor podporující mimo jiné i technologii Hyper-V [10]. Pokud procesor Hyper-V nepodporuje, veškeré ladění aplikací musí probíhat na fyzickém zařízení.

Distribuce programů je u Windows Phone 8 zajišťována speciálním kanálem, který se nazývá Windows Phone Store. Tento kanál je podobně jako u systému iOS kontrolovaný, to znamená, že každá aplikace musí před zveřejněním projít kontrolou, kterou provádí samotná firma Microsoft. Tím je zajištěno, že aplikace neobsahuje škodlivý kód a splňuje normy, které jsou na ni kladeny. Pro publikování programů je třeba vlastnit vývojářskou licenci (Developer License), která stojí 99 dolarů na rok. Studenti pak mají tuto licenci zadarmo, pokud jsou přihlášení v programu Microsoft Dreamspark.

8. Near Field Communication.
9. Extensible Application Markup Language.
10. Windows Presentation Foundation.

Kapitola 3

Náhodná čísla

3.1 Obecně

Rozlišují se dva druhy náhodných čísel, tzv. skutečně náhodná a pseudonáhodná. Zatímco skutečně náhodná čísla využívají ke svému generování fyzikální jev, vykazující náhodnost, pro tvorbu pseudonáhodných čísel je využíván deterministický algoritmus, který z malého množství náhodných vstupních dat[11] vygeneruje posloupnost čísel, která se jeví jako náhodná [11].

Náhodná čísla se užívají v mnoha oblastech, mimo jiné například v kryptografii, při simulacích, vzorkování, matematické analýze nebo programování [12]. Hrají významnou roli v některých hrách a jsou používána i v umění. Nyní následuje podrobnější popis využití náhodných čísel v konkrétních oblastech.

3.2 Užití náhodných čísel

3.2.1 Šifrování

Šifrování je metoda, díky které vzniká z běžně čitelného textu nesrozumitelná sekvence znaků, jejíž význam může odhalit pouze osoba vlastnící příslušný klíč. Náhodná čísla jsou důležitá pro samotné šifrování, neboť jsou základem většiny šifer. Kvůli neustále stoupajícímu výkonu počítačů, které se snaží šifry prolomit, se zvyšují i nároky na šifry samotné, je proto důležité zajistit, aby náhodná čísla, užívaná pro potřeby šifrování, byla co nejkvalitnější.

3.2.2 Simulace

Simulací se rozumí umělé vytvoření zkoumaného prostředí a jeho analýza. Náhodná čísla jsou zde velmi důležitá, neboť vytváří podmínky co nejvíce podobné realitě. Simulace je využívána v mnoha oblastech, např. při studiu fyzikálních jevů, předpovědi počasí nebo při modelování ekosystémů.

11. Tzv. semínka, anglicky seed.

3.2.3 Vzorkování

Není vždy možné prozkoumat všechny případy, které mohou nastat. V těchto případech je tedy praktičtější vybrat pouze vzorek a náhodná čísla umožňují spravedlivý výběr vzorku.

3.2.4 Matematická analýza

Nejen zde se využívá metoda Monte Carlo, která pracuje s pseudonáhodnými čísly. Používá se např. k řešení integrálů a parciálních diferenciálních rovnic, k hledání kořenů rovnic nebo v Rabin-Millerově testu prvočíselnosti [13].

3.2.5 Programování

Náhodné hodnoty tvoří dobrá vstupní data pro testování efektivnosti algoritmů a počítačových programů.

3.2.6 Hry

Ať už se jedná o pouhou hru v kostky, ruletu nebo loterii, vždy hraje velkou roli náhoda. Náhodné rozestavení herních tyčinek u mikáda zajišťuje zábavnost, hody kostkou pak jsou nedílnou součástí většiny deskových her a her na hrdiny (např. populární Dungeons and Dragons či české Dračí doupě). Tato potřeba náhodnosti se pak přenesla i do počítačových her.

3.2.7 Umění

První zaznamenané užití náhodnosti se v hudbě datuje do počátku 16. století, využívalo se především hodu kostkou. Tuto metodu skládání hudby používal i Mozart, Bach, Haendel nebo Haydn [14]. V moderní hudbě pak náhodnost může ovlivňovat např. zvuk syntetizátoru. Náhoda samozřejmě nehraje roli pouze v hudbě, má své místo i v malířství nebo literatuře, kde je kupříkladu využívána ve formě Dadaistického klobouku, při kterém se z klobouku postupně táhnou slova a skládají se tak básně, byť nemusí dávat žádný smysl [15].

3.3 Skutečně náhodná čísla

Pro generování skutečně náhodných čísel je třeba využít speciálních zařízení, která dokážou zpracovat náhodné fyzikální jevy a převést je do počítačem zpracovatelné podoby. Jedním z příkladů je Geiger-Müllerův detektor, který měří radioaktivní rozpad zdroje záření. Detektor je pak připojen k PC a takto získávaná data pak mohou být dále použita. Tento způsob generování náhodných čísel využívá například HotBits, webová služba umožňující získávání náhodných čísel pro další použití [16]. Výstup je možný si jednak nechat vypsat přímo ve webovém prohlížeči, další variantou je pak využití volně dostupných zdrojových

kódů pro vlastní implementaci. Výhodou je podpora zabezpečené komunikace mezi serverem a příjemcem dat, nevýhodou je potřeba připojení k internetu.

Dalším zdrojem náhodnosti je pak atmosférický šum, kterého využívá například random.org. Výhodou je, že atmosférickým šum může být poměrně jednoduše zpracováván radiopřijímačem.

Zajímavým způsobem získávání náhodných čísel byl projekt Lavarand, který využíval snímání lávových lamp, a následná náhodná data extrahovaná ze snímků byla podkladem pro generátor pseudonáhodných čísel. Projekt byl v roce 2001 ukončen a nástupce LavaRnd již tuto techniku generování náhodných čísel nepoužívá.

Poměrně běžnou variantou získávání náhodných dat je pak specializované zařízení, měřící šum polovodičového přechodu. Předností je zabudování USB výstupu v mnoha těchto zařízeních, které dovoluje snadnější sběr náhodných čísel. Velkým plusem je taktéž nezávislost na internetovém připojení. Dalšími zdroji, které se dají využít při generování skutečně náhodných čísel, především kameře a mikrofonu, se budu v práci věnovat v dalších kapitolách.

3.4 Pseudonáhodná čísla

Získávání skutečně náhodných čísel je náročný proces, při kterém je nutné použít specializované zařízení, je pomalý a může omezovat program, který náhodná data vyžaduje. Na druhou stranu, ne všechny aplikace mají stejně vysoké nároky na náhodnost a preferují rychlost generování před kvalitou. Pro tyto účely je vhodné použít místo skutečně náhodných čísel čísla pseudonáhodná.

Pseudonáhodná čísla se tvoří pomocí generátorů pseudonáhodných čísel. Jedná se o deterministické algoritmy, které z iniciálních náhodných hodnot vytváří dlouhé náhodné posloupnosti. Tyto posloupnosti jsou periodické, po určité době se začne generovaná posloupnost opakovat.

Generátory můžeme rozdělit do dvou skupin, a to na generátory lineární a nelineární. Mezi ty lineární patří např. kongruentní generátory, zpožděné Fibonnaciho generátory, generátory založené na rekurenci modulo 2, či generátory užívající bit „carry“ nebo „borrow“. U nelineárních generátorů se pak rozlišuje mezi inverzivními a kvadratickými kongruentními generátory [17].

Kapitola 4

Program pro sběr dat

4.1 Obecně

Program, který jsem pro potřebu bakalářské práce vyvinul, získává data z rozličných zdrojů. Tyto zdroje se mohou lišit podle použitého zařízení, v mém případě je to model od tchajwanské firmy HTC s označením Windows Phone 8X, kterému chybí gyroskop. Výčet všech povinných a volitelných zdrojů je uveden v kapitole Windows Phone 8, konkrétně v podkapitole Technické specifikace (u nižšího modelu, Windows Phone 8S by HTC, pak kromě gyroskopu chybí i přední kamera). Blíže se této problematice věnuji v podkapitole Nedostupné zdroje, stejně tak i ostatním potenciálním zdrojům entropie, které ovšem nelze kvůli chybějícím programovacím rozhraním[12] využít.

Program je napsán v jazyce C#, grafické uživatelské rozhraní je pak napsáno v jazyce XAML, což je jazyk pro popis grafického rozvržení prvků, vyvinutý firmou Microsoft. Vzhledem k tomu, že procesor počítače, na kterém jsem aplikaci vyvíjel, nepodporuje technologii Hyper-V, musel jsem veškeré testování a ladění aplikace provádět na fyzickém zařízení. Hlavní nabídka aplikace je složena z odkazů na obrazovky určené pro jednotlivé zdroje (obrázek 4.1). Pro návrat zpět do hlavního menu či pro ukončení aplikace slouží senzorové tlačítko „←“ (Zpět). Získávaná data se jednak v reálném čase zobrazují na displeji zařízení (obrázek 4.2), po ukončení sběru dat z konkrétního zdroje se pak vytvoří v paměti telefonu textový soubor, který tato data obsahuje. Problematikou přenesení souborů z telefonu na pevný disk počítače, kde se data dále analyzují, se věnuji na konci této kapitoly.

4.2 Dostupné zdroje

4.2.1 Zadní kamera

Obraz, získávaný kamerou přístroje, je možno do digitální podoby zachytit ve třech barevných modelech, a to sice ARGB[13], YCbCr[14] a Y[15]. Na displeji přístroje se pak zobrazuje řada čísel, která tento obraz reprezentuje, stejně tak se tato posloupnost ukládá do sou-

12. API - Application Programming Interface.
13. Alpha, Red, Green, Blue.
14. Y - jas, Cb - modrá komponenta, Cr - červená komponenta.
15. Jas.

boru. Program vytváří pro každý barevný model vlastní soubor, nedochází tedy ke sloučení do jednoho souboru při přepnutí modelu.

4.2.2 Přední kamera

Přední kamera se chová prakticky identicky jako zadní, většinou však není tak kvalitní, například HTC 8X má osmimegapixelovou zadní kameru, kdežto přední má rozlišení pouze 1,2 Mpix. Je to dáno zejména tím, že přední kamera neslouží u chytrých mobilních telefonů primárně k focení, ale je používána zejména pro videohovory. Důležité je taktéž poznamenat, že přední kamera není uvedena v povinné výbavě mobilních telefonů s Windows Phone 8 a tudíž není zastoupena ve všech modelech.

4.2.3 Mikrofon

Analogová data z mikrofonu se do digitální podoby převádí pulzně kódovou modulací (PCM). Uživateli se pak získané hodnoty reprezentují jako posloupnost čísel od 0 do 255, jedná se tedy o osmibitovou PCM. V průběhu sbírání dat se hodnoty zobrazují na displeji přístroje, po ukončení sběru se pak ukládají do souboru k dalšímu zpracování.

4.2.4 Geopozice

Pozice zařízení je získávána ze tří zdrojů: GPS, Wi-Fi a mobilní síť. Jednotlivé zdroje poskytují odlišnou míru přesnosti, kde určování polohy pomocí GPS je nejpřesnější, nejméně přesná je pak lokalizace mobilní sítí. Aplikace se pak vždy snaží určit polohu co nejlépe. Pro přístup k těmto datům je třeba v nastavení telefonu zapnout služby pro určování polohy[16].

4.2.5 Akcelerometr

Akcelerometr měří zrychlení ve třech osách, X, Y a Z. Hodnoty měření jsou ovlivněny jak gravitační silou, tak i pohybem zařízení. V ukládaných datech se mezi jednotlivými složkami rozlišuje, lze tedy analyzovat změny v každé ose zvlášť.

4.2.6 Kompas

Jiným označením magnetometr, kompas je zařízení, které slouží k určení úhlu, který zařízení svírá se severním magnetickým pólem. Dále snímá magnetické pole okolo přístroje a hodnoty vyjadřuje v trojrozměrném prostoru jako složky X, Y a Z. Kompas je u přístrojů s Windows Phone 8 volitelný a nemusí být obsažen ve všech zařízeních.

4.2.7 Senzor pohybu

Senzor pohybu (anglicky Motion sensor) je jakousi agregací akcelerometru, kompasu a gyroskopu a obsahuje velké množství informací o poloze telefonu. Pokud některý z těchto

16. V originále Location services.

senzorů není k dispozici (typicky kompas či gyroskop), pak jsou data z něj vynechána. V případě telefonu HTC 8X nejsou dostupná data z gyroskopu, senzor pohybu tedy nemá informace o rotaci telefonu (resp. má, ale velmi nepřesné, určené akcelerometrem a kompasem).

4.2.8 Baterie

U baterie jsou dostupné dvě informace, a to sice momentální stav nabití v procentech a čas do úplného vybití telefonu, kde nejmenší dostupná jednotka jsou milisekundy. Jedná se spíše o okrajový zdroj entropie, neboť udávané hodnoty nejsou příliš variabilní.

4.2.9 Displej

Zaznamenává se dotyk, tedy jeho souřadnice X a Y, které jsou vyjádřeny relativně vůči zvolenému bodu, a časová známka, lépe řečeno doba v milisekundách, která uplynula od posledního dotyku. Tato metoda je analogická k získávání entropie z klávesnice či myši.

4.2.10 Paměť

Program může získat několik informací o stavu paměti. Důležité jsou především hodnoty pro aktuální velikost paměti, která je používána, a maximum, které bylo za běhu jedné instance programu dosaženo. Dále je možno získat informace o maximální dovolené velikosti paměti pro aplikaci (314572800 B) a celkovou paměť zařízení (934641664 B). Tyto hodnoty jsou platné pro HTC 8X a u ostatních zařízení s Windows Phone 8 se mohou lišit.

4.3 Nedostupné zdroje

Bohužel, ne všechny možné zdroje jsou dostupné. Dají se rozdělit do dvou kategorií: na zdroje, které sice jsou přístupné pomocí programovacích rozhraní systému Windows Phone 8, ale které nejsou součástí fyzického zařízení, a na zdroje, pro které nejsou veřejně dostupné API. Do první kategorie patří takové zdroje entropie, jakými jsou přední kamera, gyroskop a kompas, jakožto volitelné hardwarové vybavení telefonů. Do druhé kategorie pak patří např. síla signálu mobilní sítě, dostupná Bluetooth zařízení, nebo dostupné WiFi sítě.

4.3.1 Zdroje nepodporované zařízením

Gyroskop

Tříosý gyroskop zaznamenává rotaci přístroje, v modelu HTC 8X bohužel není gyroskop obsažen, nelze tedy z tohoto zdroje získat žádná data. Funkci gyroskopu dokáže do jisté míry nahradit akcelerometr, naměřené hodnoty ovšem nejsou tak přesné a některé údaje poskytované gyroskopem u akcelerometru zcela chybí.

Motion

Ačkoliv byl senzor pohybu zmíněn již v dostupných zdrojích, pro úplnost jej uvádím i zde, neboť kvůli chybějícímu gyroskopu nelze získat z tohoto senzoru všechny informace.

4.3.2 Zdroje, pro které nejsou API

Síla signálu

Jedním ze zdrojů, pro které není u systému Windows Phone 8 zveřejněno API, na rozdíl např. od operačního systému Android , je síla signálu. Ta by mohla sloužit jako zdroj entropie, jelikož síla signálu často kolísá. Jediným údajem, který je možný získat, je jméno mobilního operátora, ke kterému je telefon připojen, což je velmi neužitečný údaj pro potřeby aplikace.

Dostupná Bluetooth zařízení

Pro programátory jsou dostupné knihovny, které poskytují základní funkčnost technologie Bluetooth. Jedná se o přenos dat z aplikace, která se nachází na jednom telefonu, do aplikace v druhém telefonu, anebo o kopírování souborů z aplikace na jiné zařízení. Pro tyto úkony je ovšem nutné mít zařízení spárované s telefonem, což se děje prostřednictvím systémového nástroje. Není tedy možné získat seznam zařízení se zapnutou technologií Bluetooth pomocí těchto knihoven.

Dostupné Wifi sítě

Obdobně, jako programátor nezíská seznam Bluetooth zařízení, není schopen ani získat seznam dostupných WiFi sítí a údaje o parametrech těchto sítí, např. nelze získat žádné informace o síle signálu WiFi sítě, ke které je telefon připojen.

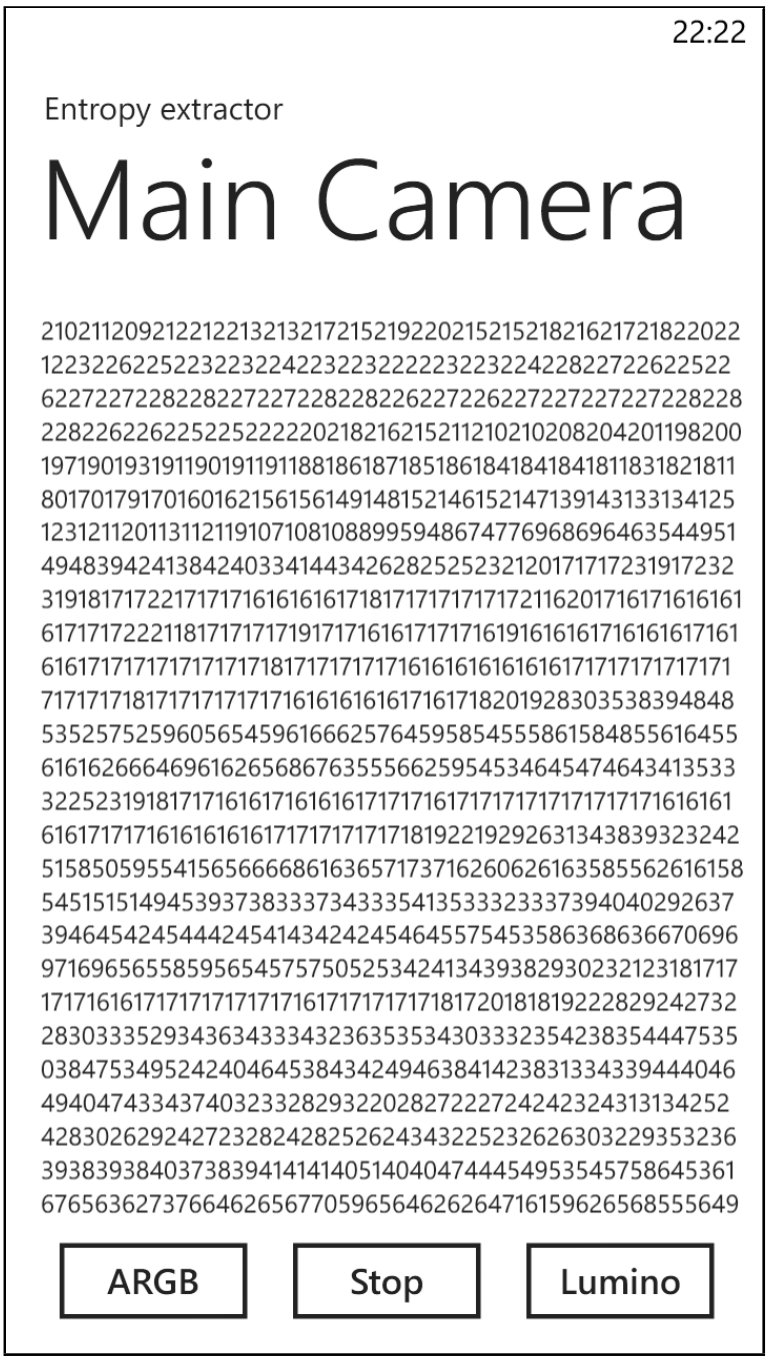
4.4 Přenos dat z mobilního telefonu do počítače

Textové soubory s daty se ukládají do Isolated Storage, což je místo v paměti telefonu, určené pro čtení a zápis dat programu. Tato složka není přístupná ostatním aplikacím a nedá se do ní dostat ani ze souborového prohlížeče systému Windows s připojeným Windows Phone zařízením. Jedním ze způsobů, jak data z úložiště dostat, je nahrát je do cloudu. Toto řešení je sice univerzální (každý uživatel, který s programem pracuje, může tato data získat), avšak implementačně náročné. Druhou variantou je použití programu Isolated Storage Explorer Tool (ISETool.exe), který je dodáván spolu s Windows Phone 8 SDK[17]. Aplikace se spouští z příkazového řádku a není příliš uživatelsky přívětivá. Alternativou je pak Windows Phone Power Tools[18], která již má i grafické uživatelské rozhraní a více funkcí.

17. Software Development Kit.
18. Dostupné z http://wptools.codeplex.com.

Oba tyto programy umožňují zkopírování souborů z Isolated Storage do uživatelsky definovaného adresáře. Tento způsob je ovšem možný pouze u lokálně přeložených programů, není tedy možné takto kopírovat data z aplikací nainstalovaných z distribučních kanálů, nicméně pro účely mého programu je toto negativum naprosto zanedbatelné.

Obrázek 4.1: Hlavní menu aplikace.



Obrázek 4.2: Ukázka spuštěné aplikace – zadní kamera.

Kapitola 5

Analýza získaných dat

Tato kapitola pojednává o analýze dat, získaných z mobilního telefonu. Nejdříve je vysvětlen termín entropie v informatice, který je v práci používán, následně jsou pak popsána a zanalyzována data z jednotlivých zdrojů. Na konci kapitoly se nachází krátké shrnutí získaných poznatků.

5.1 Entropie

Entropií se v informační teorii rozumí míra neurčitosti náhodné proměnné. Tu v roce 1948 definoval Claude E. Shannon jako [18]:

$$H(X) = -\sum_{i=1}^{n} p(x_i) \log_2 p(x_i)$$

kde x_i jsou hodnoty náhodné proměnné X a $p(x_i)$ pak pravděpodobnost výskytu každé z těchto hodnot. Báze logaritmu není pevně daná a může se lišit, v informatice se většinou používá logaritmus o dvojkovém základu. Entropie potom vyjde v bitech. Takto vypočítaná entropie se označuje jako Shannonova entropie.

5.2 Analýza jednotlivých zdrojů

Po sesbírání dat z jednotlivých zdrojů v mobilním telefonu a následným překopírováním souborů s daty do počítače bylo třeba tato data analyzovat. Pro tyto účely jsem napsal jednoduchou konzolovou aplikaci v jazyce C#, která zpracovala zadané textové soubory do seznamů hodnot, vypočítala jejich entropii a počet prvků. Pro některé zdroje platí, že rozsah jejich hodnot je pouze v rozmezí 0–255 a mohou tedy být zakódovány do 8 bitů, vždy je to ovšem v textu u příslušného zdroje uvedeno. Ostatní zdroje pak data ukládají do proměnných o alespoň 32 bitech[19]. Tato informace je důležitá zejména proto, že míra entropie nemůže překročit počet bitů, do nichž je jedno číslo ze souboru uloženo.

V následujících podkapitolách se budu podrobněji věnovat jednotlivým zdrojům, popíšu situace, za kterých byla data sesbírána, pokusím se je ohodnotit a v tabulkách uvedu jednotlivé hodnoty entropie.

19. Buď se jedná o celá čísla typu int nebo o desetinná čísla typu float.

5.2.1 Kamery

Obě kamery, jak zadní, tak přední, sbíraly data v třech různých režimech, a to ARGB, YCbCr a Y. ARGB data jsou uchovávána v 32 bitech (int). Poslední dva jmenované, YCbCr a Y, jsou režimy, které informace ukládají do proměnných typu byte, tedy na 8 bitů. Data byla sbírána po několik sekund za různých podmínek:

- při dobrých slunečních podmínkách venku na zahradě;
- za mírného šera;
- v pokoji za umělého osvětlení;
- ve vlaku za denního světla;
- pod prudkým umělým světlem;
- za úplné tmy.

Počítání entropie u kamery je poněkud obtížnější než u ostatních zdrojů. Jednak je to kvůli množství dat, která se z kamery získávají, a také kvůli tomu, že každý pixel může mít jinou entropii. Analyzoval jsem tedy malou část obrazu a to tak, že jsem pro každý pixel vypočítal jeho entropii a do tabulky jsem zavedl nejmenší, maximální a průměrnou entropii těchto pixelů jako celku. Dále jsou v tabulce údaje o počtu snímků a celkový počet prvků v souboru.

Jak je z vidět z tabulek 5.1 a 5.2, míra entropie se u kamer mnohdy podstatně liší, a to jak mezi jednotlivými podmínkami, tak i režimy. Dobrou míru entropie se podařilo získat za slunečního světla v zahradě, za šera a v pokoji. I v ostatních podmínkách jsou naměřené hodnoty entropie poměrně dobré, ovšem za naprosté tmy jsou hodnoty entropie naopak velmi nízké, kolem jednoho bitu na pixel. Dalo by se říci, že nebýt špatných výsledků za tmy, jak přední, tak zadní kamera by mohla být považována za dobrý zdroj náhodných dat. Vzhledem ke kvalitě dat získaných za naprosté tmy však toto tvrdit nelze.

Zadní kamera					
ARGB (32 b)					
Situace	**Min**	**Max**	**Průměr**	**Snímků**	**Celkem**
Zahrada	0,455021	4,754888	3,859365	27	99900
Šero	4,857575	5,129283	5,102633	35	129500
Pokoj	0,805959	4,807355	4,193200	28	103600
Vlak	1,570951	3,321928	2,900851	10	37000
Světlo	3,130125	4,640225	3,681681	30	111000
Tma	0	3,188722	0,464749	12	44400
YCbCr (8 b)					
Situace	**Min**	**Max**	**Průměr**	**Snímků**	**Celkem**
Zahrada	2,310241	5,633211	4,375380	51	188700
Šero	3,089052	4,555533	3,812231	46	170200
Pokoj	2,354075	5,201839	4,231644	42	155400
Vlak	0	3,324863	1,538213	14	51800
Světlo	2,813846	4,087462	3,910137	17	62900
Tma	0	1,407982	0,068225	21	77700
Lumino (8 b)					
Situace	**Min**	**Max**	**Průměr**	**Snímků**	**Celkem**
Zahrada	0,850243	5,843750	4,169160	64	236800
Šero	2,947989	4,544324	3,716973	44	162800
Pokoj	3,651363	5,418295	4,737850	48	177600
Vlak	0,309543	3,794654	2,694114	18	66600
Světlo	1,249460	4,392317	3,178855	21	77700
Tma	0	1,134970	0,061255	18	66600

Tabulka 5.1: Entropie zadní kamery.

Přední kamera					
ARGB (32 b)					
Situace	**Min**	**Max**	**Průměr**	**Snímků**	**Celkem**
Zahrada	3,848082	5,087465	4,922045	34	125800
Šero	4,993429	5,129283	5,124845	35	129500
Pokoj	4,607264	4,954196	4,929338	31	114700
Vlak	0	3,459432	2,728374	11	40700
Světlo	2,040224	3,906891	3,780233	15	55500
Tma	0	1,188722	0,036384	12	44400
YCbCr (8 b)					
Situace	**Min**	**Max**	**Průměr**	**Snímků**	**Celkem**
Zahrada	3,120602	5,754535	4,932745	58	214600
Šero	3,503049	5,070441	4,173674	47	173900
Pokoj	3,877781	5,403854	4,696263	50	185000
Vlak	0,391244	3,700439	3,112491	13	48100
Světlo	2,220118	3,205748	2,756347	49	181300
Tma	0	0,353359	0,001528	15	55500
Lumino (8 b)					
Situace	**Min**	**Max**	**Průměr**	**Snímků**	**Celkem**
Zahrada	3,680547	5,998045	5,147079	73	270100
Šero	3,727032	5,329097	4,460532	51	188700
Pokoj	2,300475	4,801141	3,801345	53	196100
Vlak	0,818096	4,392317	3,728073	21	77700
Světlo	3,139573	3,906891	3,751786	15	55500
Tma	0	0,353359	0,000096	15	55500

Tabulka 5.2: Entropie přední kamery.

5.2.2 Mikrofon

Podobně jako u kamer v režimech YCbCr a Y, i data z mikrofonu jsou ukládána do proměnných typu byte, tedy na 8 bitů. To ovlivňuje i entropii, které nemůže u žádného případu přesáhnout právě hodnoty 8. To ostatně dokládá i tabulka 5.3.

Data byla pořizována za normálních podmínek, a to vícekrát, pokaždé v jiném prostředí, dále byl snímán počítačově generovaný tón (2000 Hz), velmi nahlas puštěná hudba a pokusil jsem se také získat hodnoty za co největšího ticha, jakého jsem byl schopen dosáhnout. Toto ticho samozřejmě nebylo dokonalé, nicméně i přes to je znatelný pokles míry entropie vůči ostatním podmínkám. Stále se však jedná o přijatelné hodnoty (na rozdíl od kamery ve tmě). Mikrofon se tedy dá použít jako zdroj náhodných dat.

Mikrofon (8 b)		
Situace	**Entropie**	**Prvků**
Normální podmínky 1	6,048604	80000
Normální podmínky 2	6,293459	12800
Normální podmínky 3	7,077497	28800
Normální podmínky 4	6,722277	76800
Jeden tón	6,954898	44800
Hlasitá hudba	7,352649	83200
Ticho	4,777453	70400

Tabulka 5.3: Entropie mikrofonu.

5.2.3 Geopozice

Geopozice, jak je možno vidět v tabulce 5.4, poskytuje srovnatelnou míru entropie jako ostatní zdroje, podstatnou nevýhodou je ovšem nutnost pohybu, neboť při setrvávání na jednom místě se nezískávají nová data. Problémem je taktéž prodleva mezi zapnutím sběru dat a jejich získáváním, program potřebuje relativně dlouhou dobu[20], než se geolokační služby zinicializují.

Data jsem získával za jízdy v autě, na kole, při běhu a chůzi. V posledním případě jsem šel jak delší trasu, tak několik kroků[21]. Program pro sběr dat je nastaven tak, že se vždy snaží získat data z co nejpřesnějšího zdroje a aktualizuje se každých 10 metrů. Hlavně kvůli nutnosti pohybu a předvídatelnosti dat nejsou geolokační služby vhodné jako zdroj náhodnosti.

Geopozice (32 b)		
Situace	**Entropie**	**Prvků**
Auto	7,683272	2440
Běh	6,831491	654
Chůze	7,147052	1760
Kolo	7,256179	3671
Málo dat	5,023712	71

Tabulka 5.4: Entropie geopozice.

5.2.4 Akcelerometr, kompas, senzor pohybu

Data ze všech tří zdrojů, tedy z akcelerometru, kompasu a senzoru pohybu, byla sbírána za třech různých podmínek. V prvním případě bylo s telefonem pohybováno ve všech třech

20. Průměrně kolem 10 sekund.
21. V tabulce označeno jako Málo dat.

osách různou rychlostí, ve druhém zařízení nehybně leželo na desce stolu a ve třetím bylo položeno na stole v pohybujícím se vlaku.

U akcelerometru jsem jednotlivě měřil entropie všech směrových složek a časových intervalů mezi jednotlivými aktualizacemi stavů (tabulka 5.5). Především v pohybu jsou naměřené hodnoty entropie vysoké. U kompasu jsou uvedeny hodnoty pro přesnost senzoru, úhel, který zařízení svírá se severním pólem a magnetické síly pro jednotlivé souřadnice X, Y a Z (tabulka 5.6). Až na přesnost senzoru je míra entropie všech složek velmi vysoká, je ovšem nutné podotknout, že hodnoty entropie jsou téměř identické. Jednotlivé informace, které lze z kompasu získat, jsou tedy zřejmě závislé jedna na druhé. Nejvyšších hodnot entropie dosahuje senzor pohybu, neboť obsahuje nejvíce údajů[22] (tabulka 5.7). Je to ovšem dáno tím, že na rozdíl od kompasu a akcelerometru nejsou měřeny entropie jednotlivých složek, ale celkově. Výhodou je, že i při nehybném zařízení jsou tyto zdroje použitelné, nepotvrdily se tedy mé předchozí obavy, že by přístroj v nehybném stavu generoval stále stejná data.

Akcelerometr					
Situace	**X (32 b)**	**Y (32 b)**	**Z (32 b)**	**Čas (32 b)**	**Prvků**
Pohyb	6,409256	8,542671	8,018725	7,634452	1058
Nehybný	3,009930	2,813278	2,785991	7,607790	464
Vlak	5,055537	4,746693	5,529392	6,703295	254

Tabulka 5.5: Entropie akcelerometru.

Kompas						
Situace	**Přesnost**	**Směr (32 b)**	**X (32 b)**	**Y (32 b)**	**Z (32 b)**	**Prvků**
Pohyb	0,694288	9,361598	9,361598	9,361598	9,361598	662
Nehybný	0,455910	9,122766	9,105005	9,108558	9,101453	563
Vlak	0	7,300301	7,300301	7,300301	7,300301	159

Tabulka 5.6: Entropie kompasu.

5.2.5 Ostatní zdroje

Mezi zbývající zdroje patří baterie, displej a paměť. Jedná se o poměrně nedůležité zdroje, zejména v porovnání s kamerou nebo mikrofonem, uvádím je tedy zde spíše pro úplnost. Naměřené hodnoty jsou uvedeny v tabulce 5.8.

22. Soubory pro tento zdroj je ovšem nutné upravit, neboť jako jediný nemá formát, se kterým pracuje program pro analýzu dat, navíc obsahuje i neužitečné informace z chybějícího gyroskopu.

Senzor pohybu (32 b)		
Situace	**Entropie**	**Prvků**
Pohyb	12,709512	10790
Nehybný	12,847188	14508
Vlak	10,823813	2938

Tabulka 5.7: Entropie senzoru pohybu.

Stav baterie je v praxi nepoužitelný zdroj, neboť jsou data předem známa, jak momentální kapacita baterie, tak i čas do vybití lze totiž zjistit i přes aplikaci obsaženou v systému. Data se navíc aktualizují poměrně pomalu a nasbíraní rozumného množství by trvalo dlouhou dobu. V tabulce tedy tento zdroj zcela chybí.

U displeje jsem provedl dva sběry, kdy v jednom jsem se snažil o co nejpravidelnější frekvenci dotyků na to samé místo a ve druhém o co největší náhodnost, a to jak u bodu dotyku, tak i u frekvence. Za pozornost stojí zejména prvně jmenovaný příklad, kde je hodnota entropie poměrně vysoká, ač jsem se snažil dosáhnout opaku, tedy stále se opakujících stejných hodnot. Můžou za to dva faktory, jednak lidský (nejsem schopen zacílit pokaždé na to samé místo se stejnou frekvencí dotyků), ale také i technický, neboť displej není natolik citlivý a stejné fyzické místo může reprezentovat vícero hodnotami. V případě náhodných stisků je pochopitelně míra entropie lepší, ačkoliv nárůst není tak citelný. Displej se však ukázal jako relativně dobrý zdroj entropie, ovšem pro očekávané chování je potřeba relativně vysoká míra interakce s uživatelem.

Paměť, kterou aplikace momentálně používá, nepatří sama o sobě k dobrým zdrojům entropie. Paradoxně jsem lepší hodnoty naměřil po čerstvém startu aplikace, kde hodnota kolísala, než po intenzivnějším používání programu. V tom případě byla hodnota paměti poměrně stabilní. Vhodným použitím by tedy bylo měření užívané paměti programu při sběru dat z jiných zdrojů, jako samostatný zdroj není paměť příliš kvalitní, s výjimkou měření paměti po spuštění aplikace.

Displej a paměť			
Zdroj	**Situace**	**Entropie**	**Prvků**
Displej (32 b)	Jeden bod	6,729846	189
	Náhodně	7,974274	261
Paměť (32 b)	Po startu 1	5,979975	242
	Po startu 2	5,341891	163
	Po užívání 1	2,807355	7
	Po užívání 2	2,75	8

Tabulka 5.8: Entropie displeje a paměti.

5.3 Shrnutí

Analýza jednotlivých zdrojů dat ukázala, že ač se kamera mobilního telefonu může zdát jako ideální zdroj entropie, v nepříznivých světelných podmínkách je počet různých hodnot, které lze získat, velmi nízký, a nelze tedy kameru příliš doporučit, stejně jako geopozici, kde je hlavní překážkou zejména málo naměřených dat při nehybném zařízení, stejně jako u paměti, kterou aplikace využívá. Naprosto nevhodným zdrojem entropie je baterie, jejíž stav se nemění příliš často a hodnot, které jsou k dispozici, je málo. Naopak mikrofon lze považovat za vhodný zdroj entropie, neboť i v tichu je náhodnost dat dostatečná. Akcelerometr, kompas i senzor pohybu jsou taktéž vhodnými kandidáty, i při nehybném zařízení se generují různá data. Nakonec, displej lze taktéž považovat za zdroj entropie, stejně, jako je tomu u získávání entropie z myši a klávesnice stolního počítače nebo notebooku.

Kapitola 6

Závěr

Tématem této bakalářské práce byla analýza jednotlivých zdrojů entropie v mobilním telefonu s operačním systémem Windows Phone 8. Potřeba generovat náhodná čísla na mobilních zařízeních stále stoupá, neboť chytré mobilní telefony stále častěji zastupují funkci stolního či přenosného počítače a s tím se i zvyšují nároky na zabezpečení zařízení a jeho komunikace s okolím (např. e-mail nebo bankovní aplikace). Cílem práce tedy bylo prozkoumat možné zdroje entropie u přístroje s operačním systémem Windows Phone 8, získat z dostupných zdrojů data a ty využít při odhadu entropie.

Praktická část práce spočívala v napsání programu, který náhodná data sbírá a analyzuje. Ukázalo se, že některé zdroje, jako například mikrofon či akcelerometr, lze použít pro potřeby generátorů pseudonáhodných čísel. Naproti tomu kamera, která slibovala velkou míru entropie, není vzhledem k chování v nepříznivých světelných podmínkách příliš použitelná. Vhodným navázáním na tuto práci by tedy byla implementace některých generátorů s využitím zdrojů, jež jsou v této práci popsány. Druhým směrem, kterým je možné se dále vydat, je pak prozkoumání zdrojů entropie u zařízení typu Tablet PC nevyužívající operační systém Windows Phone 8, nýbrž systém Windows 8, který je určen i pro stolní počítače a má bohatší knihovnu funkcí, popřípadě analýza některé z konkurenčních platforem, jakými jsou Android či iOS.

Literatura

[1] KRHOVJÁK, Jan. *Cryptographic random and pseudorandom data generators* [online]. 2009 [cit. 2013-04-21]. Disertační práce. Masarykova univerzita, Fakulta informatiky. Vedoucí práce Václav Matyáš. Dostupné z: <http://is.muni.cz/th/39510/fi_d/>.

[2] ZÁŘECKÝ, Pavel. *Generátory pseudonáhodných čísel v prostředí mobilních telefonů* [online]. 2008 [cit. 2013-04-21]. Bakalářská práce. Masarykova univerzita, Fakulta informatiky. Vedoucí práce Jan Krhovják. Dostupné z: <http://is.muni.cz/th/173210/fi_b/>.

[3] FOLEY, Mary Jo. *Microsoft's Windows Phone 8 finally gets a „real" Windows core* [online]. 2012 [cit. 2013-04-13]. Dostupné z: <http://www.zdnet.com/blog/microsoft/microsofts-windows-phone-8-finally-gets-a-real-windows-core/12975/>.

[4] LITCHFIELD, Steve. *Nokia's new strategy and structure, Symbian to be a „franchise platform", MeeGo still in long term plans* [online]. 2011 [cit. 2013-04-13]. Dostupné z: <http://www.allaboutmeego.com/news/item/12584_Nokias_new_strategy_and_struct.php/>.

[5] ANKENY, Jason. *Samsung scraps Bada OS, folds it into Tizen* [online]. 2013 [cit. 2013-04-13]. Dostupné z: <http://www.fiercemobilecontent.com/story/samsung-scraps-bada-os-folds-it-tizen/2013-02-25/>.

[6] REED, Brad. *Android's steady march to 1 billion activations gets visualized* [online]. 2013 [cit. 2013-04-13]. Dostupné z: <http://bgr.com/2013/03/13/android-activation-growth-analysis-373572/>.

[7] DE VERE, Kathleen. *Android surges as iOS slows – comparing the growth of Android to iOS* [online]. 2012 [cit. 2013-04-13]. Dostupné z: <http://www.insidemobileapps.com/2012/09/06/android-surges-as-ios-slows-comparing-the-growth-of-android-to-ios/>.

[8] MOLEN, Brad. *Windows Phone 8 review* [online]. 2012 [cit. 2013-04-14]. Dostupné z: <http://www.engadget.com/2012/10/29/windows-phone-8-review/>.

[9] PETZOLD, Charles. *Programming Windows Phone 7*. Redmond : Microsoft Press, 1. vydání, 2010. ISBN 978-0-7356-4335-2.

[10] *System requirements for Windows Phone Emulator* [online]. 2013 [cit. 2013-04-14]. Dostupné z: <http://msdn.microsoft.com/en-us/library/windowsphone/develop/ff626524%28v=vs.105%29.aspx/>.

[11] MENEZES, Alfred J. *Handbook of applied cryptography*. Vyd. 1. Boca Raton: CRC Press, 1997, 780 s. ISBN 08-493-8523-7.

[12] KNUTH, Donald Ervin. *The art of computer programming*. 3rd ed. Upper Saddle River: Addison-Wesley, c1998, xiii, 762 s. ISBN 02-018-9684-2.

[13] Metoda Monte Carlo. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2013-03-10]. Dostupné z: <http://cs.wikipedia.org/wiki/Metoda_Monte_Carlo/>.

[14] RŮŽIČKA, Rudolf. *Využití samočinných počítačů při vzniku uměleckých děl se zvláštním zaměřením na hudbu a soudobou hudební kompozici* [online]. 1980 [cit. 2013-03-10]. Dostupné z: <http://www.fi.muni.cz/ qruzicka/Vyuziti/FI-vyuziti.HTM>.

[15] KUBĚNSKÝ, Petr. *Přínosy postupů experimentální poezie pro rozvíjení literárních kompetencí* [online]. 2010 [cit. 2013-03-10]. Bakalářská práce. Masarykova univerzita, Fakulta sociálních studií. Vedoucí práce Zbyněk Fišer. Dostupné z: <http://is.muni.cz/th/215339/fss_b/>.

[16] WALKER, John. *HotBts: Genuine random numbers, generated by radioactive decay* [online]. 1996 [cit. 2013-03-12]. Dostupné z: <http://www.fourmilab.ch/hotbits/>.

[17] MIKULKA , Zdeněk. *Generátory náhodných čísel* [online]. 2008 [cit. 2013-03-14]. Bakalářská práce. Vysoké učení technické, Fakulta elektrotechniky a komunikačních technologií. Vedoucí práce Václav Zeman. Dostupné z: <http://www.vutbr.cz/studium/zaverecne-prace?zp_id=14377>.

[18] SHANNON, Claude Elwood. A Mathematical Theory of Communication. *The Bell System Technical Journal*, July 1948, vol. 27, no. 3, s. 379–423.

Příloha A

Obsah přiloženého CD

Součástí této práce je také přiložené CD. Obsahuje

- zdrojový kód bakalářské práce ve formátu LaTeX (bc_tex) a hotovou práci ve formátu pdf;
- zdrojové kódy aplikace pro získávání entropie z telefonu pro platformu Windows Phone 8 (Entropy extractor zdrojove kody);
- zdrojové kódy aplikace pro vypočítání entropie ze souborů získaných z aplikace Entropy extractor (Entropy calculator zdrojove kody);
- zkompilovanou verzi programu Entropy calculator pro operační systém Windows spolu se soubory získanými z programu Entropy extractor (Entropy calculator spustitelna verze).