



Universitatea Politehnica Bucureşti  
Facultatea de Automatică și Calculatoare  
Departamentul de Automatică și Ingineria Sistemelor

## LUCRARE DE DIPLOMĂ

# Utilizarea tehnologiei SDR pentru interceptarea comunicațiilor pe liniile de date

Absolvent  
Micu Sergiu-George

Coordonator  
Conf. dr. ing. Nicolae Maximilian-Eugen

Bucureşti, 2024



# Cuprins

<b>1 Introducere</b>	<b>5</b>
1.1 Context . . . . .	5
1.2 Soluții similare . . . . .	5
1.3 Obiective . . . . .	5
<b>2 Considerente teoretice</b>	<b>6</b>
2.1 Unde electromagnetice emise . . . . .	6
2.2 Domeniul frecvență . . . . .	6
2.3 Eșantionare . . . . .	6
<b>3 Formalizarea problemei</b>	<b>8</b>
3.1 Forma ideală a semnalului emis . . . . .	8
3.2 Considerente reale . . . . .	8
3.3 Semnale $q$ uzuale . . . . .	8
<b>4 Descrierea platformei SDR</b>	<b>11</b>
4.1 Tehnologia <i>Software Defined Radio</i> . . . . .	11
4.2 Caracteristicile unui SDR . . . . .	12
4.3 RTL-SDR . . . . .	12
<b>5 Studiu de caz: reproducerea unui semnal transmis prin HDMI</b>	<b>13</b>
5.1 Standarul HDMI . . . . .	13
5.2 Identificarea emisiilor . . . . .	14
5.2.1 „Brute-force“ . . . . .	14
5.2.2 Verificarea unor frecvențe uzuale . . . . .	14
5.2.3 Cunoașterea anterioară a caracteristicilor semnalului video . . . . .	14
5.3 Limitări fundamentale ale problemei . . . . .	15
5.4 Obținerea unor informații necesare reproducерii cadrelor . . . . .	16
5.4.1 Determinarea <i>refresh rate</i> -ului . . . . .	16
5.4.2 Determinarea lățimii și înălțimii cadrului . . . . .	17
5.5 Reconstituirea imaginii . . . . .	18
5.5.1 Reesantionarea . . . . .	18
5.5.2 Stabilizarea imaginii . . . . .	19
<b>6 Validarea rezultatelor pe standardul HDMI</b>	<b>21</b>
6.1 Descrierea programului dezvoltat . . . . .	21
6.2 Aspecte legate de calcul . . . . .	23
6.3 Testarea programului în diferite condiții . . . . .	23
6.3.1 Distanță mică, fără obstacole . . . . .	25
6.3.2 Distanță medie, cu obstacole . . . . .	25
6.3.3 Distanță mare, cu obstacole . . . . .	26
<b>7 Limitări și concluzii</b>	<b>27</b>
7.1 Limitări . . . . .	27
7.1.1 Limitări teoretice . . . . .	27
7.1.2 Limitări practice . . . . .	27
7.2 Concluzii . . . . .	28
<b>8 Anexe</b>	<b>29</b>
8.1 Apel al programului necesar achiziției de date . . . . .	29
8.2 Secvențe de cod pentru determinarea $W, H, \text{refresh rate}$ . . . . .	29
8.3 Citirea eșantioanelor în <code>main.py</code> . . . . .	30
8.4 Schița locului testării . . . . .	30

## Listă de figuri

1	Spectrul și faza semnalului dreptunghiular . . . . .	9
2	Spectrul și faza semnalului rampă . . . . .	10
3	Diagrama bloc a unui SDR . . . . .	11
4	Un RTL-SDR; sursă imagine: <a href="http://rtl-sdr.com">rtl-sdr.com</a> . . . . .	12
5	Pinii unui cablu ce respectă standardul HDMI; sursă imagine: <a href="http://wikipedia.org">wikipedia.org</a> . .	13
6	Spectrul (în jurul frecvenței de 148.5 MHz) unui semnal generat de transmiterea unui semnal video $1920 \times 1080 @ 60\text{Hz}$ . . . . .	14
7	Imaginea originală și o simulare a reproducерii ei, pentru o imagine complexă din punct de vedere vizual (contrast scăzut, număr mare de culori diferite, forme complexe)	15
8	Imaginea originală și o simulare a reproducерii ei, pentru o imagine simplă din punct de vedere vizual (contrast ridicat, doar două nivele de culoare, forme simple, ușor de recunoscut) . . . . .	16
9	Secvența de autocorelație circulară a datelor captate într-o secundă cu deplasare maximă de $f_e$ eșantioane . . . . .	17
10	Secvența de autocorelație circulară a datelor captate într-o secundă cu deplasare între $\frac{f_e}{rf_{\max}}$ și $\frac{f_e}{rf_{\min}}$ eșantioane . . . . .	17
11	Secvența de autocorelație circulară a datelor captate într-o secundă cu deplasare între 0 și 500 eșantioane . . . . .	18
12	Imaginea originală și o simulare a reproducерii ei folosind completarea cu zerouri .	18
13	Imaginea originală și o simulare a reproducерii ei folosind interpolarea și reeșantionarea	19
14	Compensarea deplasării folosind un cadru de referință . . . . .	20
15	Interfața programului dezvoltat . . . . .	21
16	Efectul vizual al ajustării înălțimii, $H$ corect este 1080 . . . . .	22
17	Cadrele folosite pentru testare . . . . .	23
18	Reproducerea cadrului din Figura 17a în jurul mai multor frecvențe centrale . . . .	24
19	Reprezentare schematică a unei antene de tip dipol . . . . .	25
20	Reproducerea cadrelor din Figura 17 la distanță mică . . . . .	25
21	Reproducerea cadrelor din Figura 17 la distanță medie, cu obstacole . . . . .	25
22	Reproducerea cadrelor din Figura 17 la distanță mare, cu mai multe obstacole (ziduri, mobilier, lifturi) . . . . .	26
23	Schița aproximativă a locului în care s-au realizat teste; E este punctul de emisie (unde se află cablul HDMI), punctele 1, 2, 3 reprezintă locul de unde s-au realizat teste din capitolele 6.3.1, 6.3.2, respectiv 6.3.3 . . . . .	30

## Listă de tabele

1	Performanțele unor SDR-uri și costul acestora . . . . .	28
2	Lista contribuțiilor personale . . . . .	32

# 1 Introducere

## 1.1 Context

Creșterea permanentă a cantității de informație achiziționată, stocată și prelucrată aduce cu sine o mărire a vitezelor de transmisie a datelor. Atunci când datele sunt transmise printr-o interfață fizică, de tip fir conductor, este produs un câmp electromagnetic. Pentru viteze suficiente de mari de transmisie a datelor, aceste emisii pot pătrunde în spectrul radio, făcând posibilă captarea de la distanță și studiul lor, în scopul reproducării semnalului ce le-a generat.

Marea majoritate a comunicațiilor prin fire conductoare între două echipamente sau dispozitive nu sunt criptate, mai ales când acestea se află în apropiere. Captarea și reproducerea fidelă a semnalelor folosite poate însemna accesul nemijlocit la informația pe care cele două aparate o interschimbă. În plus, întrucât captarea emisiilor electomagnetic este un procedeu pasiv, această breșă de securitate poate fi exploatață într-o manieră nedetectabilă.

Dispozitivele de tip *Software Defined Radio* (SDR) fac aplicarea acestor tehnici mai facilă, oferind posibilitatea captării emisiilor radio fără a fi necesar proiectarea de hardware. Toate funcțiile specifice radioelectronicii, e.g. modulații, demodulații, sincronizare se realizează prin software.

## 1.2 Soluții similare

Ideea reproducării semnalelor electrice din emisiile electomagnetic pe care acestea le emit există încă din Al Doilea Război Mondial, însă cu limitări profunde. Utilizarea echipamentelor radio de precizie construite în mod clasic presupune fie un sacrificiu în ceea ce privește versatilitatea, fie o creștere semnificativă a costului, pe lângă necesitatea familiarizării cu proiectarea circuitelor radio.

Deși dispozitive precum cel prezentat în *Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?* [2] funcționează cu rezultate foarte bune, acestea sunt limitate la aplicația pentru care au fost proiectate. Utilizarea tehnologiei SDR facilitează modificarea rapidă și fără cost a aplicației, i.e. același hardware poate fi folosit pentru reproducerea unui semnal video sau o comunicație serială, doar modificând componenta software.

## 1.3 Obiective

Lucrarea propune studiul teoretic al emisiilor electomagnetic ce pot conduce la reproducerea semnalului, în ce condiții se poate realiza aceasta și ce tipuri de transmisii sunt vulnerabile. Este prezentată tehnologia SDR și principalele specificații ale acestor dispozitive și legătura lor cu diferiți parametri ai semnalului ce se dorește a fi reprodus.

Rezultatele teoretice sunt verificate într-un studiu de caz ce vizează reconstrucția unui semnal video transmis prin standardul *High-Definition Multimedia Interface* (HDMI), incluzând elemente teoretice specifice semnalelor video. Sunt prezentate simultan instrumente și tehnici utile pentru extragerea unor date adiționale despre semnal în sine, ce pot facilita ulterior reconstrucția sa.

În final sunt detaliate limitările, atât teoretice, cât și practice pe care le are procedeul dezvoltat, împreună cu metode posibile pentru securizarea transmisiilor împotriva acestui tip de interceptare.

## 2 Considerente teoretice

### 2.1 Unde electromagnetice emise

Orice fir conductor parcurs de curent electric variabil în timp emite unde electromagnetice și poate fi considerat o antenă [1, pag. 495]. Pentru analiza teoretică am presupus că semnalul electric ce generează unde electromagnetice și semnalul electric rezultat din captarea acestora sunt identice; detalii legate de antenele utilizate se regăsesc în capitolul 5.1.

### 2.2 Domeniul frecvență

Semnalele pot fi reprezentate atât în domeniul timp, cât și în frecvență, iar, pentru semnale ce provin din natură, trecerea între cele două se poate realiza oricând, utilizând analiza Fourier. În funcție de context, am folosit în lucrare termenii de **pulsărie** ( $\omega$ ) și **frecvență** ( $f$ ). Între valorile celor doi există următoare relație  $\omega = 2\pi f$ .

Obiectele utilizate în această lucrare sunt

- transformata Fourier în timp continuu, aplicată semnalelor analogice  $f(t)$ , cu următoarea definiție

$$F(j\omega) = \int_{-\infty}^{\infty} f(t)e^{-j\omega t} dt \quad (1)$$

- transformata Fourier în timp discret, aplicată semnalelor digitale  $x[k]$ , cu următoarea definiție

$$X(e^{j\omega}) = \sum_{k=-\infty}^{\infty} x[k]e^{-j\omega k} \quad (2)$$

- transformata Fourier discretă, aplicată semnalelor digitale  $x[k]$  de lungime  $N$ , cu următoarea definiție

$$\text{DFT}(x) = X[k] = \sum_{n=0}^{N-1} x[n]e^{-2j\pi \frac{nk}{N}} \quad (3)$$

și inversă sa, definită

$$\text{IDFT}(X) = x[k] = \frac{1}{N} \sum_{k=0}^{N-1} X[k]e^{2j\pi \frac{nk}{N}} \quad (4)$$

Toate acestea sunt, în general, funcții complexe cu un argument real, ce pot fi reprezentate grafic prin **spectru** și **fază**. Spectrul reprezintă amplitudinile numerelor complexe ce rezultă din evaluare transformate Fourier la fiecare pulsărie (continuă sau discretă). Similar, diagrama de fază reprezintă fază numerelor complexe menționate anterior.

### 2.3 Eșantionare

Semnalele analogice, indiferent de natura lor, trebuie să fie eșantionate pentru a permite prelucrarea lor digitală. În cele mai multe cazuri, eșantionarea se face la momente egal depărtate de timp. Distanța dintre aceste momente de timp se numește **temp de eșantionare**, notat  $T_e$  ( $[T_e]_{\text{SI}} = \text{s}$ ). Aceeași informație poate fi reprezentată și în funcție de **frecvență de eșantionare**, notată  $f_e$ , ce cuantifică cât de des se realizează eșantionarea ( $[f_e]_{\text{SI}} = \text{Hz}$ ). O mărime echivalentă, definită ca numărul de eșanțioane realizate într-o secundă se numește **rată de eșantionare** (*sampling/sample rate* în engleză).

Trecerea din domeniul analog în cel discret poate aduce cu sine pierderea unor informații dacă eșantionarea nu s-a realizat corect. Teorema de eșantionare Shannon-Nyquist oferă o condiție suficientă pentru ca informația să nu fie pierdută, anume dacă transformata Fourier în timp continuu este nenulă pentru frecvențe în intervalul  $[-B, B]$  atunci eșantionarea se poate realiza fără pierdere de informație la o frecvență minimă  $f_n = 2B$ , numită frecvență Nyquist.

Teorema este folosită de cele mai multe ori în contextul semnalelor continue reale, ce au transformate Fourier în timp continuu simetrice, însă aceasta se extinde și în cazul semnalelor continue complexe. Concret, dacă transformata Fourier în timp continuu este nenulă în intervalul de frecvențe  $[f_-, f_+]$ , atunci eșantionarea se poate realiza la o frecvență minimă  $f_n = f_+ - f_-$ , însă eșantioanele vor fi complexe.

### 3 Formalizarea problemei

#### 3.1 Forma ideală a semnalului emis

În momentul de față, multe standarde de comunicare transmit informația fie binar, fie printr-o secvență de eșantioane analogice. Mai departe, am tratat cazul acestor semnale; acestea ce pot fi reprezentate sub forma

$$f(t) = \sum_{k=0}^N x[k] \cdot q(t - T_q k) \quad (5)$$

unde  $x[n]$  este un semnal discret de lungime  $N$ , ce conține informația utilă, iar  $q(t)$  este o funcție ce descrie cum evoluează în timp un anumit eșantion, cu suport de lungime  $T_q$ ; aceasta respectă proprietățile

$$* \quad q(t) = 0, \quad \forall t \notin [0, T_q)$$

$$** \quad q(t) \in \mathbb{R}, \quad \forall t \in \mathbb{R}$$

Pentru a analiza comportamentul în frecvență al acestui semnal, am folosit transformata Fourier în timp continuu

$$\begin{aligned} F(j\omega) &= \int_{-\infty}^{\infty} f(t) e^{-j\omega t} dt = \int_{-\infty}^{\infty} \sum_{k=0}^N x[k] q(t - T_q k) e^{-j\omega t} dt \\ &\stackrel{*}{=} \int_0^{NT_q} \sum_{k=0}^N x[k] q(t - T_q k) e^{-j\omega t} dt \stackrel{**}{=} \sum_{k=0}^N x[k] \int_0^{NT_q} q(t - T_q k) e^{-j\omega t} dt \\ &= \sum_{k=0}^N x[k] Q(j\omega) e^{-jT_q k \omega} = Q(j\omega) \sum_{k=0}^N x[k] e^{-jT_q k \omega} \end{aligned}$$

adică

$$F(j\omega) = Q(j\omega) X(e^{j\omega T_q}) \quad (6)$$

unde  $F(j\omega)$ ,  $Q(j\omega)$  sunt transformatele Fourier în timp continuu ale semnalelor  $f$ , respectiv  $q$ , iar  $X(e^{j\omega})$  este transformata Fourier în timp discret a semnalului  $x$ . Aceasta din urmă este periodică cu o perioadă  $2\pi$ , respectiv  $X(e^{j\omega T_q})$  cu o perioadă de  $\frac{2\pi}{T_q}$ .

#### 3.2 Considerante reale

Întrucât transformata Fourier în timp discret este întotdeauna periodică cu o perioadă de  $2\pi$ , forma descrisă anterior denotă faptul că spectrul semnalului discret ce conține datele transmise va avea o componentă periodică, vizibilă la pulsații multiple de  $\frac{2\pi}{T_q}$ . Aceasta nu apare totuși izolată, ci este ponderată de spectrul unui semnal ce codifică, în esență, forma unui eșantion. De obicei aceasta ( $q$ ) este o funcție al cărei conținut frecvențial se concentrează la frecvențe joase, având o amplitudine joasă la frecvențe mari. Pentru a recupera semnalul discret  $q$ , am considerat că, în jurul pulsațiilor de interes, spectrul lui  $q$  este o constantă.

Utilizând această presupunere, este posibilă reconstrucția (parțială) a semnalului discret  $x$  având acces la o bandă limitată de pulsații. Totodată, orice informație despre semnalul  $q$  va fi pierdută, însă acesta nu conține informație utilă, ci modelează doar o codificare a secvenței  $x$  transmise.

În realitate, funcția  $q$  va avea un efect asupra semnalului  $x$  recuperat, iar în anumite cazuri poate denatura datele recuperate. În continuare, am analizat efectul a două semnale uzuale utilizate în electronică pentru a observa cât de mult afectează acestea datele ce pot fi recuperate.

#### 3.3 Semnale $q$ uzuale

Pentru ca semnalul recuperat să fie în continuare util, este necesar ca acesta să fie distorsionat cât mai puțin de funcția  $q$  în jurul pulsațiilor de interes. Dacă acesta este totuși modificat, este preferată o distorsiune cât mai „simplă”, e.g. înmulțirea cu o constantă.

Consider funcțiile ce definesc semnale de tip dreptunghi, respectiv rampă

$$q_d(t) = \begin{cases} 1, & t \in [0, T_q) \\ 0, & \text{altfel} \end{cases} \quad \xleftrightarrow{\mathcal{F}} \quad Q_d(j\omega) = \frac{1 - e^{-j\omega T_q}}{\omega}$$

$$q_r(t) = \begin{cases} \frac{t}{T_q}, & t \in [0, T_q) \\ 0, & \text{altfel} \end{cases} \quad \xleftrightarrow{\mathcal{F}} \quad Q_r(j\omega) = \frac{e^{-j\omega T_q}(1 + j\omega T_q) - 1}{\omega^2 T_q}$$

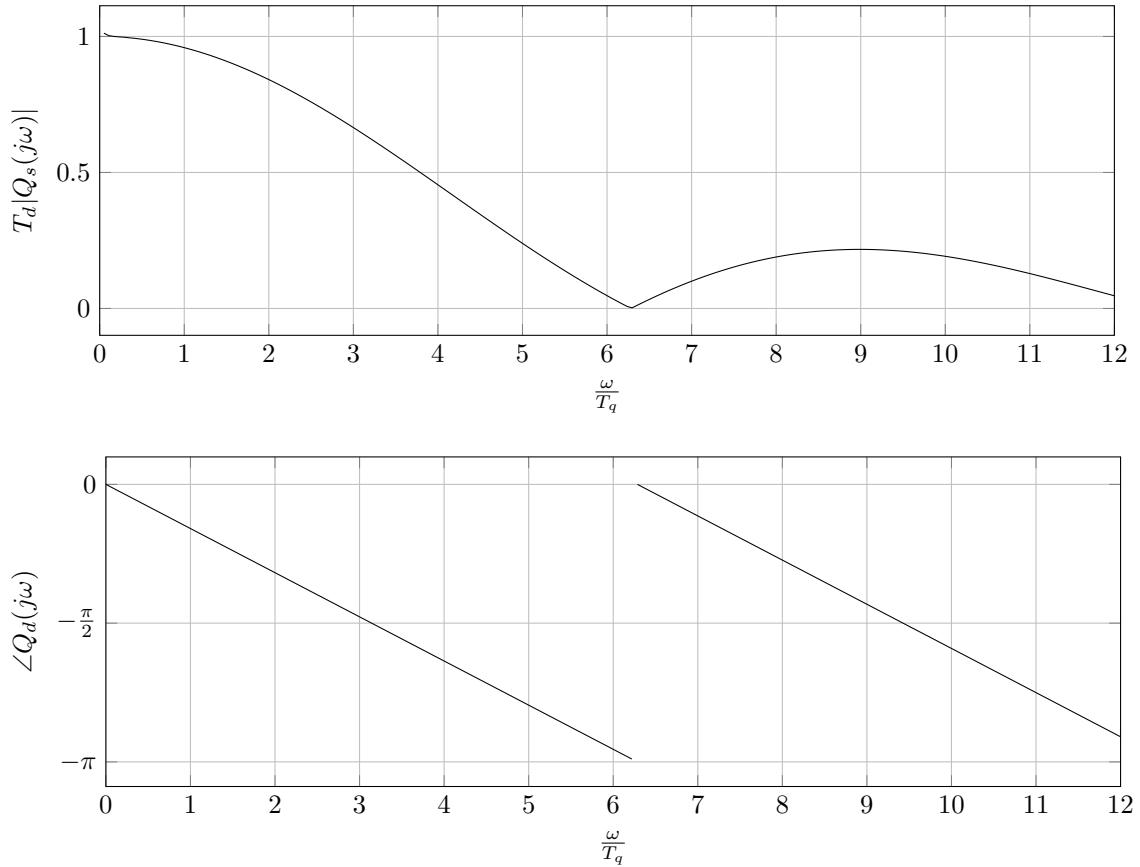


Figura 1: Spectrul și faza semnalului dreptunghiular

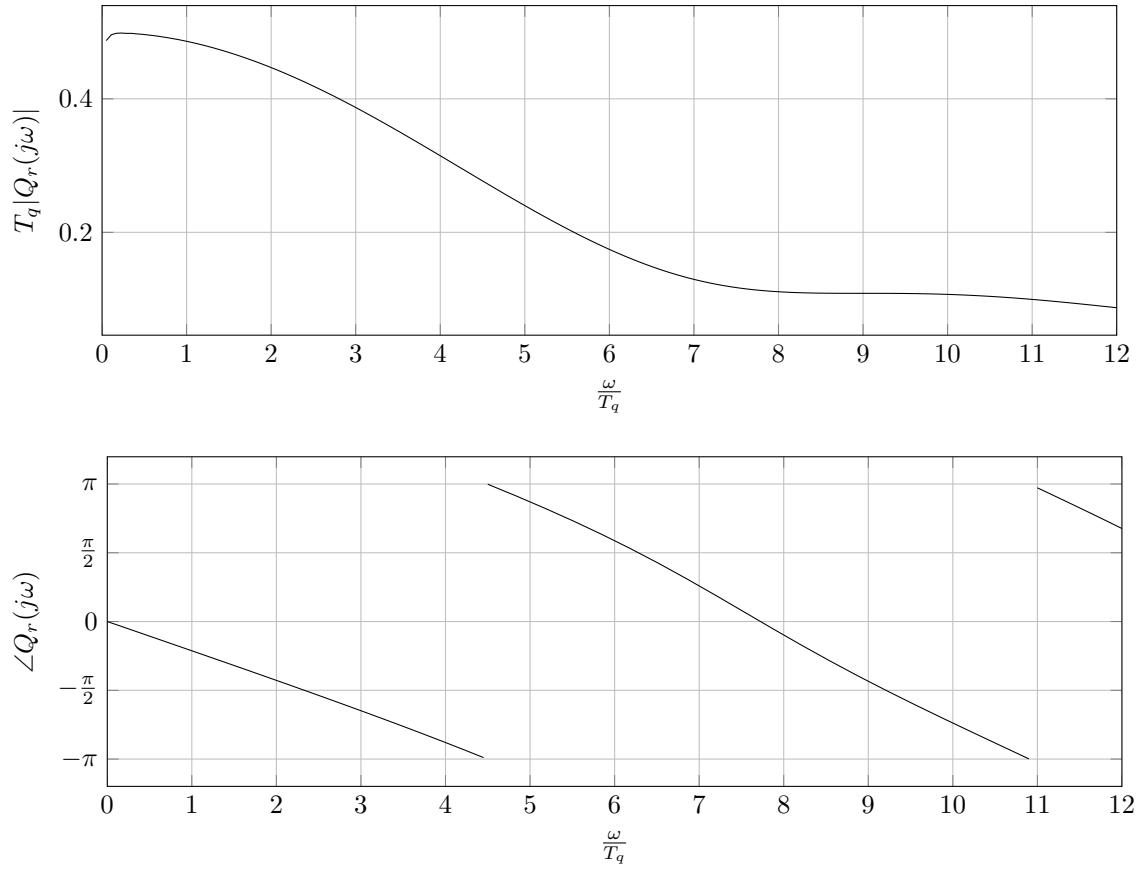


Figura 2: Spectrul și faza semnalului rampă

Spectrele și fazele celor două semnale uzuale considerate (Figura 1 și Figura 2) sunt aproximativ liniare în jurul armonicelor, într-un interval de lățime  $\frac{1}{T_q}$ . Pentru anumite armonice, transformatele Fourier în timp continuu pot fi aproximate chiar printr-o constantă, e.g. în jurul celei de-a nouă armonice.

## 4 Descrierea platformei SDR

### 4.1 Tehnologia *Software Defined Radio*

Creșterea rapidă a vitezei de calcul disponibilă pe circuite integrate și microcontrolere permite astăzi implementarea software a unor funcționalități implementate în mod convențional (sau cel puțin istoric) prin hardware. În cazul tehnologiei de radioemisie și radiorecepție, dispozitivele ce permit acest lucru poartă numele *Software Defined Radio* (SDR).

SDR-urile sunt dispozitive ce permit recepția pe o plajă largă de frecvențe, însă acestea pot capta într-un anumit moment numai un anumit interval din spectrul electromagnetic. Lățimea acestui interval este dat de teorema de eșantionare Shannon-Nyquist și poartă numele de lățime de bandă. Mijlocul acestui interval se numește frecvență centrală. În esență, un SDR translatează spectrul astfel încât frecvența centrală să fie adusă în zero, și transmite aceste date mai departe pentru a fi procesate. Această translatare se realizează conform teoremei de deplasare în frecvență a transformatei Fourier în timp continuu.

$$F(j(\omega - \omega_c)) = \mathcal{F}\{e^{-j\omega_c t} f(t)\} \quad (7)$$

O consecință a teoremei (7) este că, deși semnalul captat de antenă este unul real, după translatarea sa acesta va deveni un semnal complex, întrucât este înmulțit cu un semnal oscilator complex. Astfel, semnalul definit de relația (5) poate fi scris ca  $f(t) = I(t) + jQ(t)$ . Notația aceasta este standard în radioelectronică, iar cele două componente se numesc *în fază* (I) și *în quadratură* (Q). Diagrama bloc de funcționare a unui dispozitiv de tip SDR este prezentată în Figura 3.

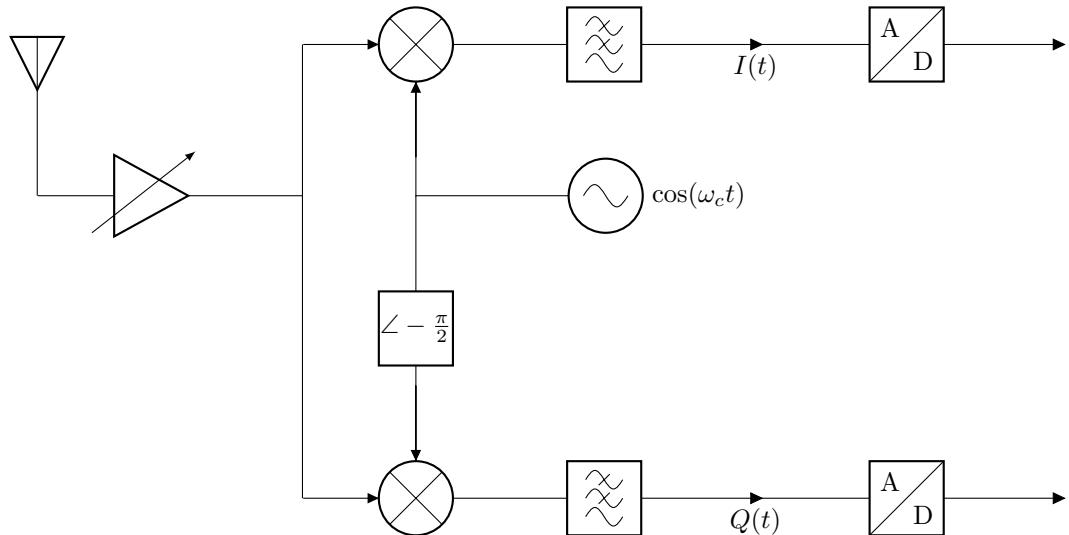


Figura 3: Diagrama bloc a unui SDR

## 4.2 Caracteristicile unui SDR

În funcție de componentele folosite și modul în care a fost proiectat, un SDR poate avea specificații diferite. Cunoașterea specificațiilor este importantă deoarece acestea impun limite asupra modului în care se poate realiza recepția emisiilor produse de cabluri și ce proprietăți trebuie să aibă semnalele ca informația să poată fi reconstruită.

Specificațiile principale ce caracterizează funcționarea unui SDR sunt

- Plaja de frecvențe de operare: reprezintă intervalul din spectrul electromagnetic în care SDR-ul poate recepta
- Lățimea maximă de bandă: caracterizează dimensiunea intervalului maxim în jurul frecvenței centrale care poate fi captat
- Frecvență maximă de eșantionare: cuantifică numărul maxim de eșantioane pe care dispozitivul le poate capta într-o secundă, notată în continuare  $f_e$
- Rezoluția convertorului analog-numeric: reprezintă numărul de biți pe care este reprezentată un eșantion unidimensional (I sau Q)
- Stabilitatea oscilatorului local: caracterizează cât de mari pot fi diferențele între frecvența centrală dorită și cea reală

## 4.3 RTL-SDR

RTL-SDR (Figura 4) este un SDR ce se bazează pe utilizarea unei componente folosită în receptoare destinate inițial pentru televiziune, produsă în masă, ceea ce îi permite să aibă un cost redus (în jur de \$30). Aceasta are o plajă de frecvențe între 500 kHz și 1766 MHz, cu o lățime de bandă de până la 2.4 MHz, corespunzătoare unei frecvențe de eșantionare de 2.4 MHz, cu eșantioane cu o rezoluție de câte 8 bit pentru componenta reală, respectiv cea imaginată [8].



Figura 4: Un RTL-SDR; sursă imagine: [rtl-sdr.com](http://rtl-sdr.com)

Practic, cu acest dispozitiv pot fi reproducute semnale ce au un  $T_q$  (definit ca în (5)) de maxim  $\frac{1}{2400\,000\text{s}} \approx 0.417\,\mu\text{s}$ . Dacă emisiile sunt rezultatul unei transmisiuni binare, RTL-SDR permite reproducerea semnalelor cu o viteză de transmitere a datelor de până la  $2.4\frac{\text{Mbit}}{\text{s}}$ . În realitate, dispozitivul suportă frecvențe și mai mari de eșantionare, de până la 3.2 MHz, însă nu mai garantează eșantionarea corectă, iar unele eșantioane pot fi pierdute.

## 5 Studiu de caz: reproducerea unui semnal transmis prin HDMI

### 5.1 Standarul HDMI

Standardul HDMI (*High-Definition Multimedia Interface*) este unul printre cele mai utilizate standarde de transmitere a cadrelor dintre o unitate centrală și un afișaj extern. Acesta transmite, pe lângă cadre și alte informații adiționale, e.g. dimensiunea cadrelor, numărul de cadre pe secundă, semnal audio. În continuare, acestea vor fi ignorate și voi descrie tehniciile necesare pentru reproducerea cadrelor transmise prin cablu, precum și cum pot fi deduse unele informații adiționale.

Înainte de a putea reproduce orice informație transmisă prin cablu, trebuie cunoscut modul în care acestea sunt codificate în acest standard. În Figura (5) sunt prezentate pinii specifici standardului HDMI și amplasarea lor.

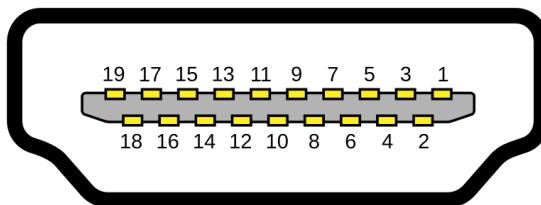


Figura 5: Pinii unui cablu ce respectă standardul HDMI; sursă imagine: [wikipedia.org](https://en.wikipedia.org)

De interes sunt doar pinii 1-9, prin care sunt transmise semnalele de la unitatea centrală la afișajul extern. Cadrele sunt transmise pixel cu pixel, linie cu linie, iar pe lângă acestea sunt transmise și informațiile adiționale, care nu fac obiectul reproducării. Acestea sunt plasate înaintea cadrelor și liniilor, deci fiecare cadru va avea un număr de pixeli mai mare (atât pe verticală, cât și pe orizontală). Toată informația adițională se va regăsi în zonele din prelungirea cadrului, conform diagramei din [4, cap. 5.1.2].

În majoritatea cazurilor, fiecare pixel din cadru este reprezentat în format RGB (*Red Green Blue*), ce presupune reprezentarea culorilor prin trei componente, fiecare corespunzătoare nivelului de roșu, verde, respectiv albastru. Conform standardului HDMI [4, cap. 6.5.1], cele trei componente sunt transmise în paralel, determinând emisii electromagnetice ale firelor ce transmit canalele de culoare să se însumeze. Din această cauză, informația legată de nuanță este pierdută, putând fi în continuare reproduse intensitatea și luminozitatea. Cum cele trei componente vor fi însumate, fără a se face distincție între ele, în continuare voi considera că emisiile radio sunt produse de un singur semnal electric, transmis pe un canal.

Fiecare pixel din cadru este reprezentat printr-un număr format din 8 biți, ce reprezintă intensitate luminoasă a pixelului respectiv. Valoarea aceasta nu este transmisă direct prin cablu, ci i se adaugă 2 biți pentru corecția erorilor [4, cap. 5.1.1, 5.1.2], astfel încât, fiecare pixel va fi reprezentat în momentul transmiterii de un număr pe 10 biți.

Parametrii cei mai relevanți în contextul unei transmisii video cadru cu cadru (precum HDMI) sunt rezoluția imaginii, compusă din lățime (notată ușual  $W$ ) și înălțime (notată ușual  $H$ ) și cât de des este transmis un cadru nou (mărime numită *refresh rate*, cu unitatea de măsură Hz). Pentru a descrie mărimile care caracterizează un cadru voi utiliza în continuare notația

$$W \times H @ rfr \text{ Hz}$$

pentru a descrie un semnal video compus din cadre cu  $W$  pixeli pe orizontală,  $H$  pixeli pe verticală și  $rfr$  cadre pe secundă.

## 5.2 Identificarea emisiilor

Înainte de a putea fi captat, trebuie identificată banda de frecvențe a semnalului radio ce conține informație utilă, în special frecvența centrală, conform definiției din capitolul 4.1. Voi descrie trei metode prin care emisiile pot fi „găsite“, iar toate presupun că se cunoaște anterior faptul că semnalul există și este produs de o transmisie prin un cablu HDMI. Nicio metodă descrisă nu poate diferenția direct între acest tip de emisie și una produsă de oricare altă comunicație digitală. Prin intermediul acestor metode urmăresc identificare în spectrul electromagnetic a unui interval în care spectrul semnalului captat are un aspect similar cu cel din Figura 6.

### 5.2.1 „Brute-force“

Această metodă presupune simpla parcurgere a spectrului electromagnetic până când este identificat un interval în care aspectul său este cel căutat. Cum dispozitivul SDR poate oferi datele reprezentării spectrului într-un interval de lățime egală cu lățimea de bandă, căutarea se poate realiza examinând intervale consecutive (ce nu se intersectează), de dimensiunea lățimii de bandă. Această metodă nu necesită nicio presupunere adițională, însă este cea mai lentă, întrucât necesită verificarea manuală a întregii plaje de frecvențe a SDR-ului.

Pentru RTL-SDR, cu o lățime de bandă de maxim 2.4 MHz și o plajă de frecvențe între 500 kHz și 1766 MHz, această metodă necesită verificarea a aproximativ 735 de intervale, deși acest număr poate fi redus folosind diferite proprietăți ale spectrului. O metodă simplă constă în utilizarea ecuației (7) și a proprietăților descrise în capitolele 3.2 și 3.3 ce, împreună, indică prezența primelor armonice, dacă cele superioare sunt vizibile, sau, echivalent, absența armonicelor superioare dacă cele inferioare nu sunt vizibile. În practică, pot apărea totuși cazuri în care armonicele inferioare nu sunt prezente la receptie deoarece au fost absorbite de diferite obiecte (e.g. perete) din mediu.

### 5.2.2 Verificarea unor frecvențe uzuale

Această metodă presupune verificarea unor frecvențe centrale corespunzătoare unor dimensiuni uzuale ale cadrelor. Deși standardul HDMI suportă o gamă largă de dimensiuni ale imaginii, majoritatea afișajelor externe sunt produse cu specificații similare, ce urmăresc niște standarde de facto ale rezoluției și *refresh rate*-ului. Deși rezoluția și *refresh rate*-ul ale semnalului video nu trebuie să fie aceleși cu cele ale afișajului extern, în practică cele două coincid în marea majoritate a cazurilor, iar cele mai comune sisteme de operare (Windows, OSX și cele bazate pe Linux) nu oferă decât rezoluții și *refresh rate*-uri standard.

Asadar, prin verificarea doar a frecvențelor centrale ce ar rezulta din emisiile caracteristice pentru combinațiile de rezoluție și *refresh rate* comune, sunt reduse semnificativ numărul de intervale ce trebuie verificate. Dezavantajul acestei metode este faptul că presupune ca semnalul HDMI căutat este caracterizat de rezoluție și *refresh rate* standard.

### 5.2.3 Cunoașterea anterioară a caracteristicilor semnalului video

Dacă rezoluția și *refresh rate*-ul sunt cunoscute anterior, este necesară verificare doar a frecvenței caracteristice pentru acel semnal video, de exemplu pentru  $1920 \times 1080 @ 60\text{ Hz}$ , prima armonică este prezentă la frecvența de 148.5 MHz.

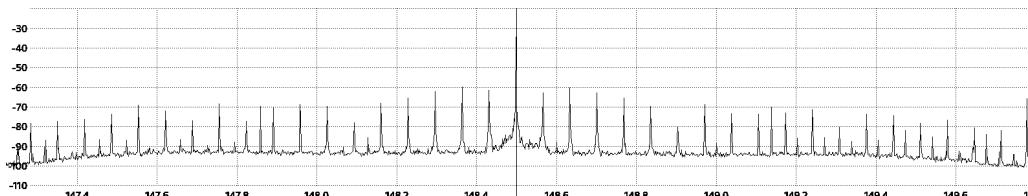


Figura 6: Spectrul (în jurul frecvenței de 148.5 MHz) unui semnal generat de transmiterea unui semnal video  $1920 \times 1080 @ 60\text{ Hz}$

### 5.3 Limitări fundamentale ale problemei

Conform Figurii 3, datele primite de la SDR sunt eșantioane ale emisiilor captate, translatable în frecvență. Notând frecvența de eșantionare a SDR-ului  $f_e$  și semnalul captat de acesta  $s_c[n]$ , avem

$$s_c[n] = e^{-j2\pi f_c \frac{n}{f_e}} \sum_{k=0}^N x[k]q \left( \frac{n}{f_e} - T_q k \right) \quad (8)$$

Presupunând că  $q(t) = q_d(t)$ , definit ca în capitolul 3.3 și aplicând modulul rezultă

$$|s[n]| = \left| \sum_{k=0}^N x[k]q_d \left( \frac{n}{f_e} - T_q k \right) \right|$$

Întrucât suma din relația anterioară este o sumă de funcții al căror suport nu se intersectează, modulul se poate distribui, ajungând la relația

$$s[n] \stackrel{not}{=} |s[n]| = \sum_{k=0}^N |x[k]|q \left( \frac{n}{f_e} - T_q k \right) \quad (9)$$

Practic, în limita presupunerilor făcute, aplicând modulul complex eșantioanelor primite de la SDR, obținem secvența  $s[n]$  ce reprezintă o reeșantionare (prin interpolare de ordin 0) a lui  $|x[n]|$ . Deși informația legată de semn este pierdută, în acest caz aceasta nu ar trebui să conteze, întrucât HDMI este un standard general, deci, ideal  $\text{Im}(x[n]) = \{0, 1\}$ .

O transmisie  $1920 \times 1080 @ 60 \text{ Hz}$  (probabil cel mai răspândit standard pentru afișaje externe) prin intermediul HDMI, va conține cel puțin  $1920 \cdot 1080 \cdot 60 = 124416000$  eșantioane într-o secundă (la care se vor adăuga și informațiile adiționale alipite cadrelor). Cum fiecare eșantion este reprezentat pe 10 biți, viteza de transmitere a datelor prin cablu este aproximativ  $1.25 \frac{\text{Gbit}}{\text{s}}$ , mult peste frecvență maximă de eșantionare a RTL-SDR, de  $2.4 \text{ MHz}$ . În ciuda acestui fapt, voi arăta că o reproducere la o rezoluție mai mică a semnalului video transmis este totuși posibilă.

Primul compromis care am ales să îl fac este renunțarea la posibilitatea de a reproduce perfect secvența de biți ce reprezintă intensitatea luminoasă a fiecărui pixel; în schimb, consider fiecare pixel ca fiind reprezentat de media biților ce îi reprezintă valoarea în realitate, astfel reducând numărul de biți transmiși într-o secundă la aproximativ 125 Mbit.

Mai departe, orice diferență dintre frecvența de eșantionare a SDR-ului și viteza de transmitere a datelor prin cablul HDMI va avea ca efect o scădere vizibilă a rezoluției cadrelor reconstruite. Rezoluția nu scade pe ambele dimensiuni, ci doar în dimensiunea orizontală,  $W$ . Acest fapt se dătorează faptului că transmiterea datelor prin HDMI este realizată linie cu linie, deci, dacă fiecare linie este eșantionată măcar odată, numărul de linii va rămâne același, însă vor varia numărul de eșantioane din fiecare linie (adică lățimea imaginii).

Am prezentat două simulări ale efectului pe care aceste limite le au asupra unui cadru în Figura 7 și Figura 8. În ambele figuri imaginile au fost scalate pe orizontală cu scopul de a conserva raportul dintre lățime și înălțime.



Figura 7: Imaginea originală și o simulare a reproducерii ei, pentru o imagine complexă din punct de vedere vizual (contrast scăzut, număr mare de culori diferite, forme complexe)

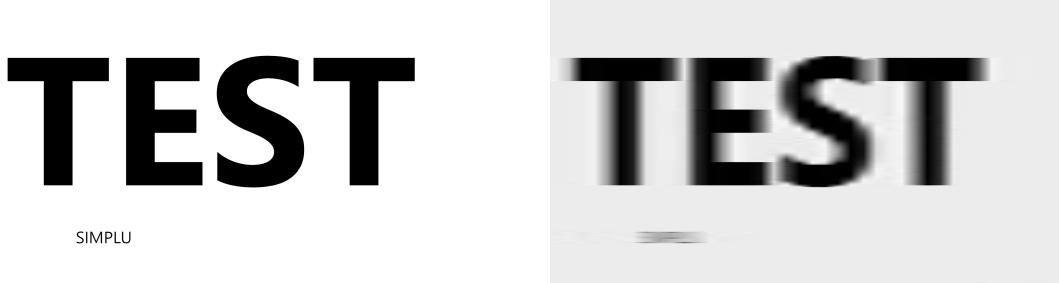


Figura 8: Imaginea originală și o simulare a reproducerii ei, pentru o imagine simplă din punct de vedere vizual (contrast ridicat, doar două nivele de culoare, forme simple, ușor de recunoscut)

În simulările din Figura 7 și Figura 8 se observă că principala problemă este rezoluția scăzută în direcția orizontală. Singurul mod în care aceasta poate fi crescută este mărirea frecvenței de eșantionare a SDR-ului (ceea ce poate însemna și utilizarea altuia, mai performant).

#### 5.4 Obținerea unor informații necesare reproducerii cadrelor

În momentul captării cu ajutorul SDR-ului, informația captată nu reprezintă decât o secvență unidimensională de eșantioane. Pentru a putea reproduce semnalul video este necesară aflarea celor trei parametri caracteristici semnalelor video, i.e. lățimea, înălțimea și *refresh rate*-ul.

##### 5.4.1 Determinarea *refresh rate*-ului

Pentru a estima *refresh rate*-ul am presupus că două cadre consecutive sunt aproape identice. Folosind datele înregistrate timp de o secundă,  $s[n] \in \mathbb{R}$ ,  $n \in [0, f_e]$ , am calculat secvența de autocorelație circulară

$$r_s[k] \stackrel{\text{not}}{=} \sum_0^{\text{sr}} s[n]s[n - k \bmod \text{sr}] \quad (10)$$

unde

$$a \bmod b = a - b \left\lfloor \frac{a}{b} \right\rfloor$$

cu notația  $|c|$  reprezentând partea întreagă a lui c, iar sr reprezentând rata de eșantionare a SDR-ului.

În ipoteza menționată mai sus, secvența de autocorelație circulară  $r_s$ , va avea vârfuri periodice, cu o perioadă egală cu lungimea unui cadru în eșantioane (ale SDR-ului). Acest fapt se datorează faptului că funcțiile periodice (în acest caz secvența de pixeli ce reprezintă cadrele captate într-o secundă) au o secvență de autocorelație periodică de aceeași perioadă [7, cap. 10.5.2.1]. Deși cadrele consecutive nu sunt identice, am constatat că, în cele mai multe cazuri, această presupunere este suficientă pentru a determina *frame rate*-ul.

Astfel, alegând limita inferioară ( $rfr_{\min}$ ) și cea superioară ( $rfr_{\max}$ ), *frame rate*-ul poate fi determinat alegând vârful cu amplitudinea maximă din intervalul  $\left[ \frac{f_e}{rfr_{\max}}, \frac{f_e}{rfr_{\min}} \right]$ . Am ilustrat un exemplu cu ajutorul unui semnal ce a generat secvența de autocorelație circulară provenită din captarea emisiilor unei transmisii  $1920 \times 1080 @ 60$  Hz la o frecvență de eșantionare  $f_e = 2.56$  MHz.

Figura 9 ilustrează capetele intervalului  $\left[ \frac{f_e}{rfr_{\max}}, \frac{f_e}{rfr_{\min}} \right]$ , cu  $rfr_{\min} = 15$  Hz și  $rfr_{\max} = 120$  Hz.

În Figura 10 vârful cu amplitudine maximă a fost marcat. Acesta apare la o deplasare  $N_c = 42630$ ; considerând că eșantionare a fost făcută la  $f_e = 2.56$  MHz, *refresh rate*-ul poate fi calculat  $rfr = \frac{f_e}{N_c} = 60.0516$  Hz, deci foarte aproape de *refresh rate*-ul real al semnalului video, 60 Hz.

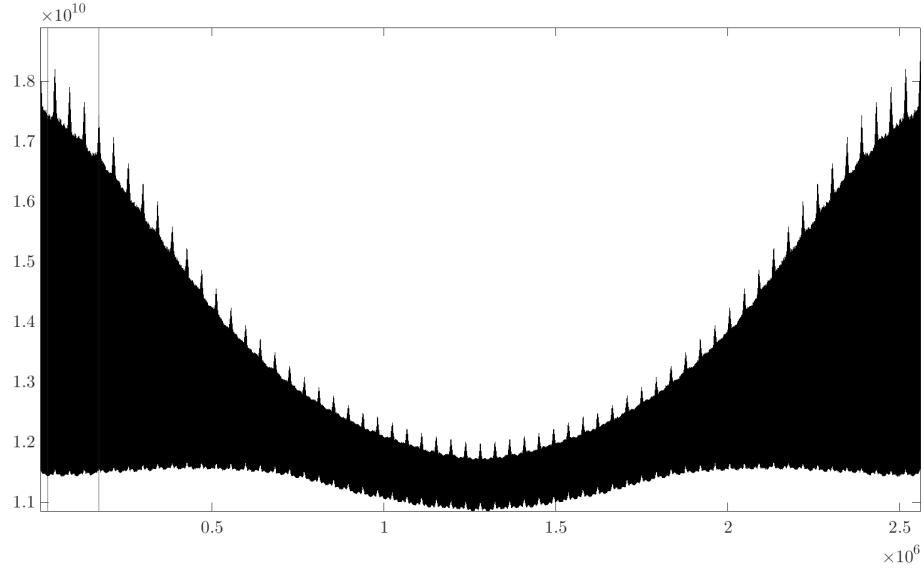


Figura 9: Secvența de autocorelație circulară a datelor captate într-o secundă cu deplasare maximă de  $f_e$  eșantioane

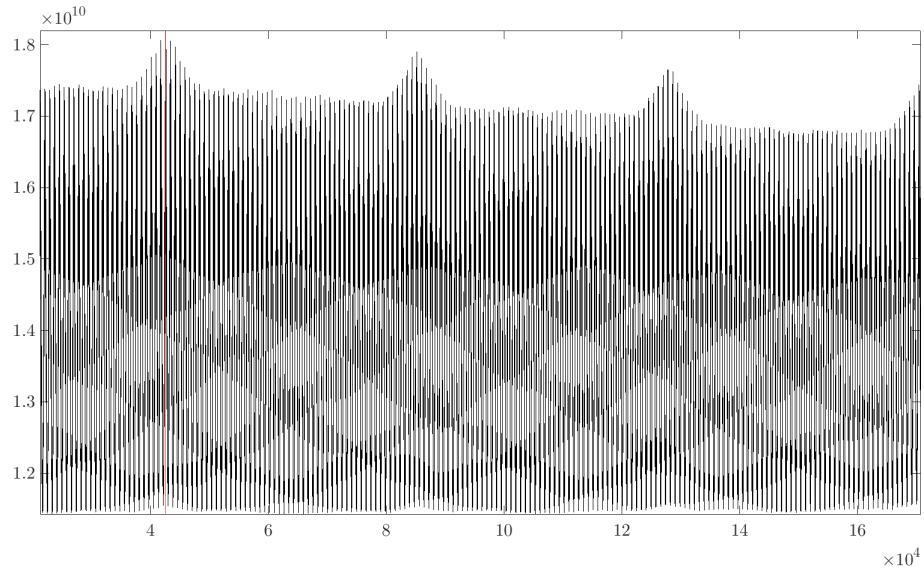


Figura 10: Secvența de autocorelație circulară a datelor captate într-o secundă cu deplasare între  $\frac{f_e}{rfr_{\max}}$  și  $\frac{f_e}{rfr_{\min}}$  eșantioane

#### 5.4.2 Determinarea lățimii și înălțimii cadrului

Am procedat similar pentru a identifica lățimea cadrului, presupunând că două rânduri consecutive dintr-un cadru sunt aproape identice, iar apoi calculând secvența de autocorelație circulară a unui singur cadru, adică  $N_c = \frac{f_e}{rfr}$

$$r_c[k] = \sum_0^{N_c} s[n]s[n - k \bmod N_c]$$

Alegerea vârfului corespunzător lățimii cadrului poate fi făcută fie impunând limite superioare pentru înălțime  $h_{\min}$ , respectiv  $h_{\max}$ , iar apoi alegând vârful cu amplitudine maximă din intervalul  $\left[\frac{N_c}{h_{\max}}, \frac{N_c}{h_{\min}}\right]$ . O altă metodă este alegerea directă a vârfului cu amplitudine maximă al secvenței de autocorelație circulară, excludând câteva eșantioane în jurul lui 0.

În Figura 11 sunt ilustrate primele 500 de eșantioane din secvența  $r_c$ , generată dintr-un cadru al semnalului din capitolul 5.4.1. Am marcat capetele intervalului  $\left[ \frac{N_c}{h_{\max}}, \frac{N_c}{h_{\min}} \right]$ , pentru  $h_{\min} = 400$  și  $h_{\max} = 2160$  (rezoluția verticală specifică imaginilor 4K), iar cu roșu a fost marcat vârful cu amplitudine maximă, ce apare la  $k_{c\max} = 38$ , deci  $W = 38$  și  $H = \frac{N_c}{W} = \frac{42630}{38} \approx 1121$ .

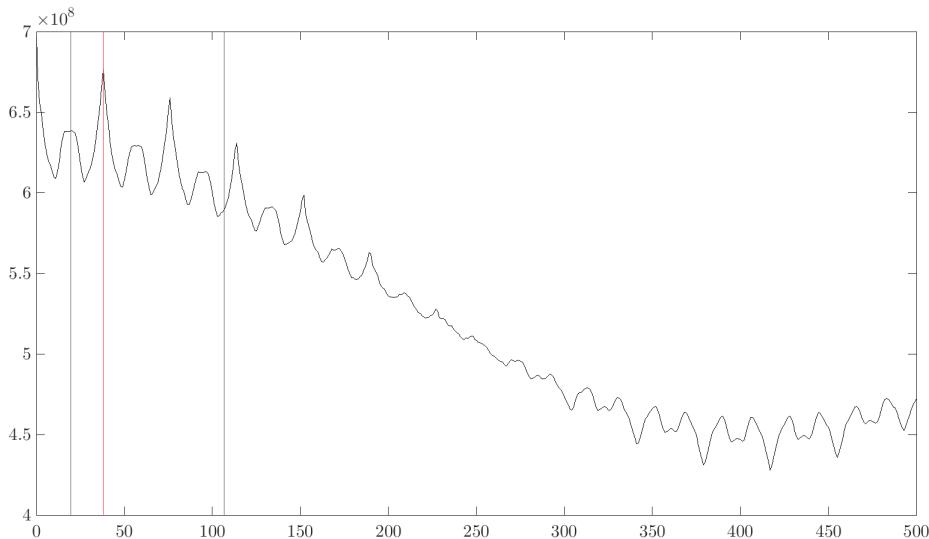


Figura 11: Secvență de autocorelație circulară a datelor captate într-o secundă cu deplasare între 0 și 500 eșantioane

Cum am menționat în 5.3, rezoluția orizontală a cadrului reproducă va scădea considerabil față de cea reală. Rezoluția verticală, este mai mare decât cea a cadrului (1121 față de 1080); acest fapt se datorează informației adiționale alipită cadrelor, conform [4, cap. 5.1.2]. În realitate, per standard, un cadr HDMI ce transmite un semnal video cu 1080 de rânduri va avea 1125 de rânduri, foarte aproape de rezoluția verticală pe care am identificat-o, 1121. Diferența apare doar din cauza erorilor de rotunjire și poate fi corectată manual.

## 5.5 Reconstrucția imaginii

### 5.5.1 Reesantionarea

Prima problemă care apare în reconstrucția imaginii este cauzată de rotunjiri, care pot face relația  $W \cdot H = N_c$  să nu fie validă. Primul mod prin care am încercat să rezolv această problemă a fost trunchierea unui cadrul, dacă  $N_c > W \cdot H$ , respectiv completarea sa cu valori de zero, dacă  $N_c < W \cdot H$ . Această metodă nu are rezultate bune, imaginea fiind prea distorsionată pentru a fi recunoscută. Figura 12 prezintă un exemplu de reconstrucție folosind această metodă.

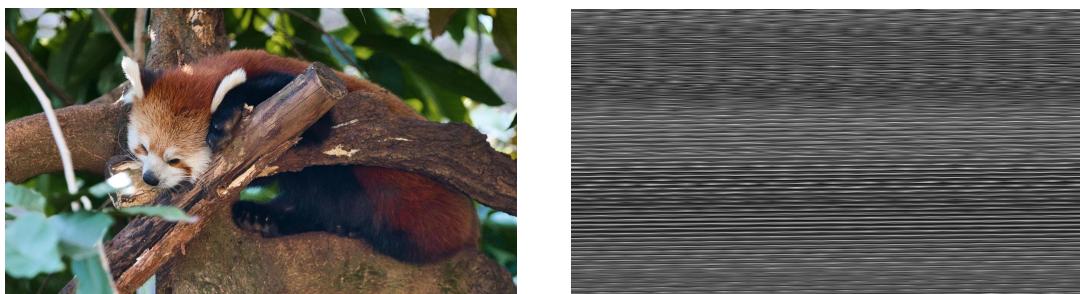


Figura 12: Imaginea originală și o simulare a reprodusorii ei folosind completarea cu zerouri

O altă abordare încercată este interpolarea semnalului ce conține eșantioanele dintr-un cadru, iar apoi eșantionarea semnalului interpolat, astfel încât noul semnal să fie format din exact  $W \cdot H$  eșantioane. Rezultatele sunt bune, formele din imagine sunt conservate, limitate totuși de rezoluția mică orizontală. Figura 13 prezintă un exemplu de reconstrucție folosind această metodă.



Figura 13: Imaginea originală și o simulare a reprodusării ei folosind interpolarea și reeșantionarea

Rezultatele metodei a două sunt satisfăcătoare doar dacă înălțimea imaginii este cea corectă. Deși este un dezavantaj, rezultatele devin din ce în ce mai bune pe măsură ce înălțimea estimată se apropie de ce reală, deci aceasta metodă oferă și un mod de ajustare vizuală, manuală și înălțimii imaginii; exemple referitoare la ajustarea se regăsesc în capitolul 6. Mai departe am folosit doar această metodă în reconstrucția cadrelor.

### 5.5.2 Stabilizarea imaginii

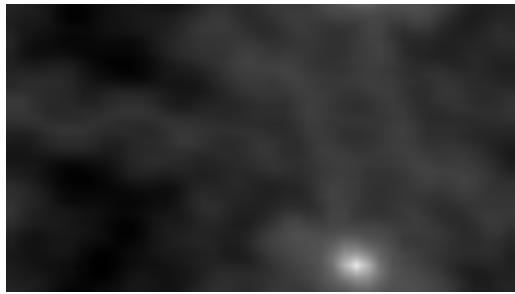
Din cauza estimărilor imperfecte și a erorilor cauzate de eșantionarea prea rară, între cadrele reproducute vor apărea deplasate atât pe verticală, cât și pe orizontală, iar această deplasare se schimbă de la cadru la cadru. Spațiile adiacente imaginii cuprind informații din cadrele adiacente. Folosind în continuare presupunerea că două cadre consecutive sunt aproape identice, am utilizat secvența de corelație circulară bidimensională între un cadru de referință și cel actual pentru a identifica vârful ce indică cu cât a fost deplasată imaginea pe verticală, respectiv orizontală. Am utilizat apoi coordonatele acestui vârf pentru a compensa această deplasare, reobținând imaginea originală.



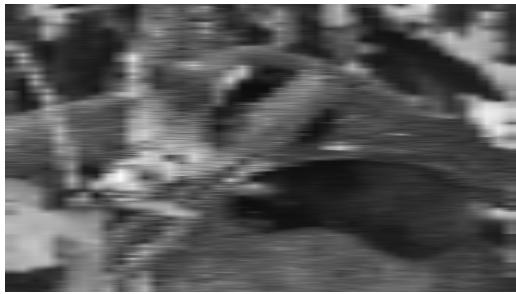
(a) Imaginea originală



(b) Simulare a reprodusului cadrului, cu deplasare



(c) Secvența de corelație circulară bidimensională între cadrul de referință și cel deplasat



(d) Cadrul cu deplasare compensată utilizând coordonatele punctului de maxim din Figura 14c

Figura 14: Compensarea deplasării folosind un cadrul de referință

Figura 14 arată performanțele bune ale acestei metode. Este de menționat că această metodă are nevoie de un cadrul de referință pentru a realiza secvența de corelație circulară bidimensională. În implementarea acestei metode, am obținut acest cadrul alegând primul cadrul captat, iar eventualele deplasări existente în cadrul de referință pot fi corectate manual.

## 6 Validarea rezultatelor pe standardul HDMI

### 6.1 Descrierea programului dezvoltat

Pentru testarea și validarea rezultatelor și metodelor obținute, respectiv dezvoltate, acestea au fost implementate într-un program dezvoltat utilizând limbajul de programare Python. Acest program funcționează pe două fire de execuție.

Primul fir este destinat exclusiv elementelor grafice și modificarea unor variabile atunci când se interacționează cu ele.

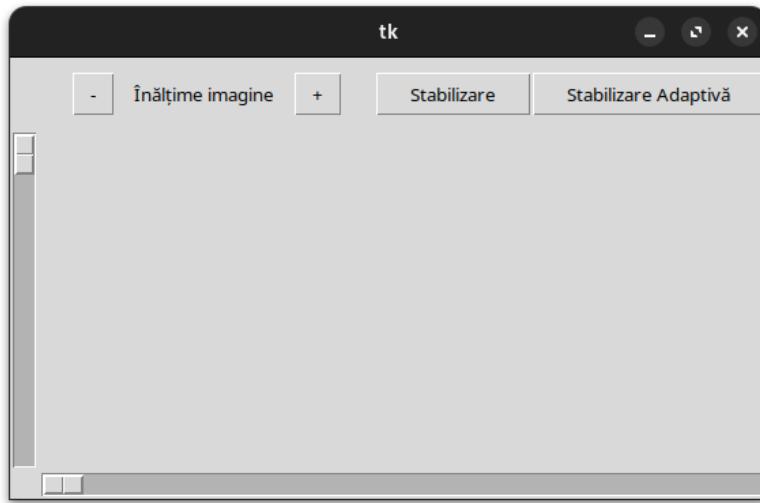


Figura 15: Interfața programului dezvoltat

În paralel, al doilea fir de execuție primește la intrare un sir de date ce reprezintă eșantioanele unui semnal recuperat, le procesează, apoi afișează cadrul reconstruit. Fiecare eșantion are 16 biți, 8 pentru componenta  $I$  și 8 pentru  $Q$ , iar componentele sunt interpretate ca numere întregi fără semn. Odată cu lansarea programului, sunt determinați automat parametrii  $W$ ,  $H$  și  $refresh rate$ -ul, iar pe baza acestuia sunt captate  $\frac{sr}{rfr}$  eșantioane pentru a fie transformate într-un cadru.

Datele sunt achiziționate cu ajutorul unui program [10] *open-source*, dezvoltat special pentru componenta principală a RTL-SDR.

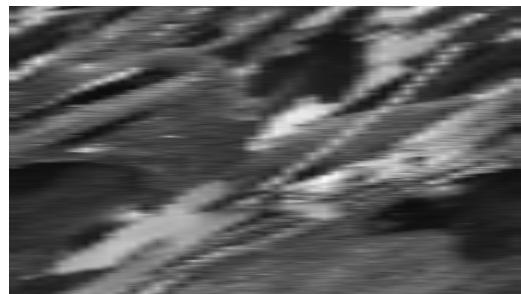
Programul permite incrementarea și decrementarea înălțimii cadrului, până când aceasta este aceeași cu cea a cadrului transmis inițial prin HDMI. Această ajustare manuală este necesară pentru ca metoda descrisă în capitolul 5.5.1 să funcționeze adevarat. În Figura 16 am inclus o simulare a relației între înălțime cadrului și imaginea reprodusă.

În plus, cele două butoane de stabilizare permit stabilizarea imaginii folosind metoda descrisă în capitolul 5.5.2. Opțiunea „Stabilizare Adaptivă“ folosește cadrul anterior drept cadrul de referință, nu primul cadru captat la rularea programului. Această opțiune are performanțe mai bune dacă apar multe modificări între primul cadru și cel actual, iar presupunerea că acestea sunt aproape identice nu mai este validă.

Ultimele elemente grafice sunt două bare de defilare, utilizate pentru deplasarea de către utilizator a imaginii de referință folosită pentru stabilizare.



(a)  $H = 1078$



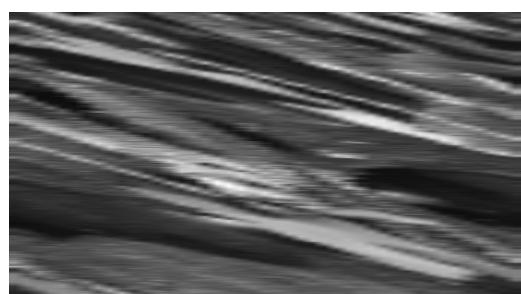
(b)  $H = 1079$



(c)  $H = 1080$



(d)  $H = 1081$



(e)  $H = 1082$

Figura 16: Efectul vizual al ajustării înălțimii,  $H$  corect este 1080

## 6.2 Aspecte legate de calcul

Am impus ca programul dezvoltat să poată prelucra un cadru într-un timp mai mic decât  $\frac{1}{r_{fr}}$ , altfel volumul de date ce trebuie procesate ar crește mai repede decât pot fi acestea procesate, deci programul nu ar mai putea lucra decât pe date înregistrate.

În această lucrare am utilizat un RTL-SDR, cu o frecvență de eşantionare setată la  $f_e = 2.56$  MHz. Calculul secvenței de autocorelație circulară cu formula de definiție din ecuația (10) este nefezabilă, deoarece aceasta are o complexitate  $O(sr^2)$ . O soluție ar fi limitarea calcului secvenței de autocorelație circulară doar în intervalul de interes, însă această optimizare nu rezolvă dependența pătratică de numărul de eşantioane ale semnalului. Dacă este utilizat un alt SDR, cu o frecvență de eşantionare mai mare, problema numărului prea mare de operații necesare apare din nou.

O altă metodă de a calcula secvența de autocorelație circulară a unui semnal  $x$  de lungime  $N$  este utilizând transformata Fourier discretă [6, cap. 3], astfel

$$r_x = \text{IDFT}(\text{DFT}(x) \cdot \overline{\text{DFT}(x)}) \quad (11)$$

Pentru calculul transformatorilor Fourier (inverse) discrete se poate utiliza algoritmul FFT, cu o complexitate  $O(sr \log sr)$ , ceea ce face identificarea  $W$ ,  $H$  și *refresh rate*-ului posibilă într-un timp semnificativ mai mic.

Întrucât fiecare cadru trebuie stabilizat înainte ca acesta să fie afișat, utilizarea unui algoritm eficient pentru calculul corelației circulare bidimensionale este necesară pentru ca programul să ruleze în timp real.

Formula din ecuația (11) se extinde și în cazul bidimensional [5, cap. 5.2.9], astfel încât secvența de corelație circulară bidimensională între două semnale  $x$  și  $y$  poate fi calculată

$$r_{xy} = \text{IDFT}_2(\text{DFT}_2(x) \cdot \overline{\text{DFT}_2(y)}) \quad (12)$$

unde  $\text{DFT}_2$  și  $\text{IDFT}_2$  sunt variantele bidimensionale ale DFT, respectiv IDFT; acestea pot fi calculate folosind algoritmul FFT în varianta bidimensională, obținând aceleași imbunătățiri ale performanței.

## 6.3 Testarea programului în diferite condiții

Pentru testare am folosit un laptop conectat printr-un cablu HDMI nemodificat la un monitor. Am inclus cadrul de test din Figura 17a pentru a analiza cât de fidelă este reproducerea unor cadre cu contrast ridicat și ce dimensiuni ale textului rămân lizibile. În Figura 17b este un cadru de test cu o varietate de culori și mai complex din punct de vedere vizual.



(a)



(b)

Figura 17: Cadrele folosite pentru testare

Am realizat teste în diferite condiții pentru a observa cum afectează distanța calitatea cadrelor, precum și influență obstacolelor (e.g. perete, ușă) aflate între cablul HDMI și punctul de recepție. Pentru toate testele, undele electromagnetice sunt produse de transmiterea unui semnal video

$1920 \times 1080 @ 60$  Hz, unul dintre cele mai răspândite standarde video.

Pentru fiecare test, am considerat toate armonicele (în limitele RTL-SDR) la care apar emisii electromagnetice și am folosit programul dezvoltat pentru reproducerea cadrelor în jurul fiecărei dintre ele, identificând-o (vizual) pe cea cu rezultatele cele mai bune. Figura 18 conține un exemplu de cum poate afecta această alegere calitatea imaginii reconstruite.

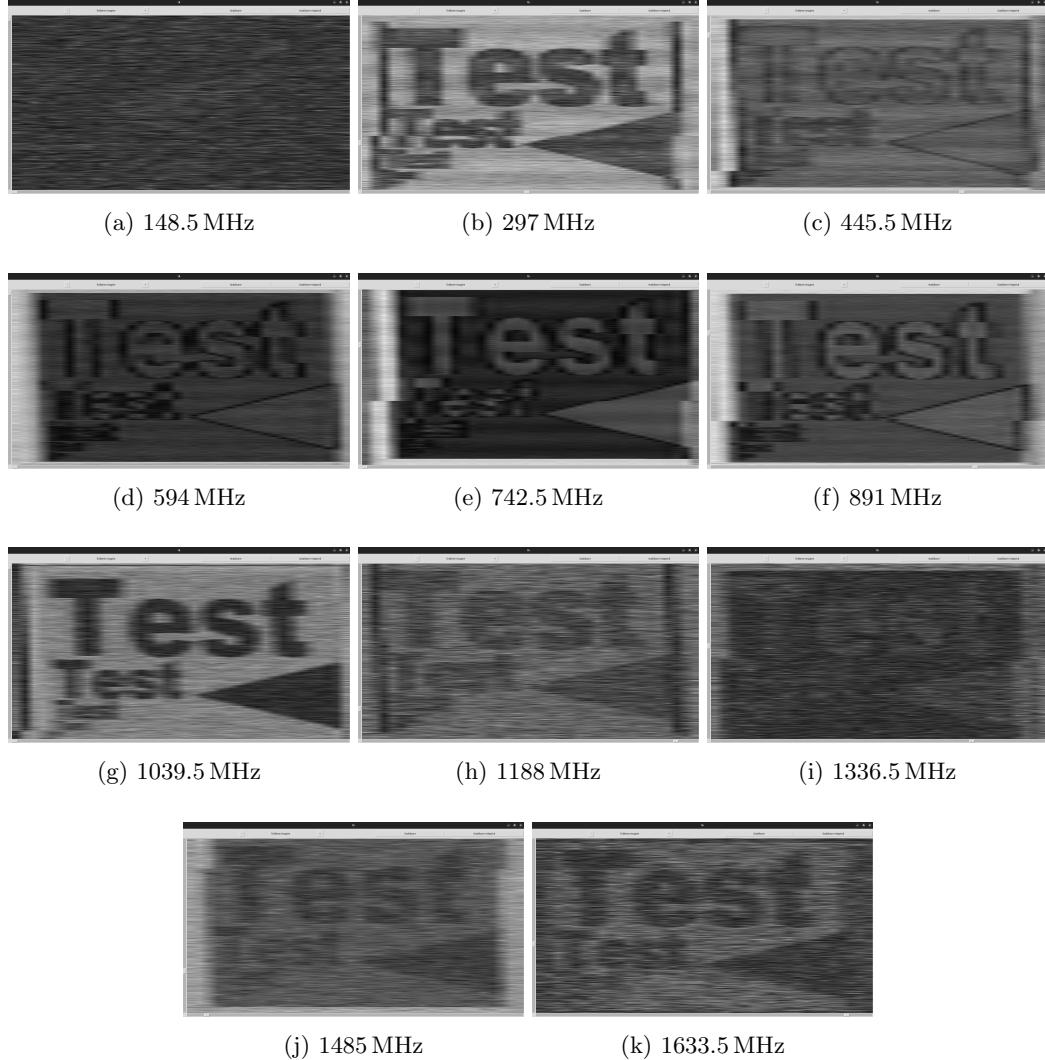


Figura 18: Reproducerea cadrului din Figura 17a în jurul mai multor frecvențe centrale

Dispozitivului SDR i-a fost atașată o antenă de tip dipol ajustabilă, reprezentată schematic în Figura 19. Pentru fiecare test lungimea  $l$  a fost ajustată astfel încât să fie egală cu o pătrime din lungimea de undă  $\lambda_c$  corespunzătoare frecvenței centrale,  $\lambda_c = \frac{c}{f_c}$ ,  $c = 299\,792\,458 \frac{\text{m}}{\text{s}}$ . [3, cap. 4.6]

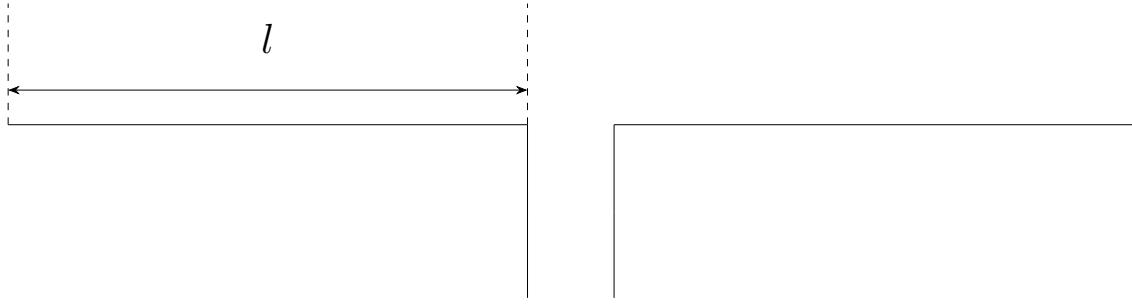


Figura 19: Reprezentare schematică a unei antene de tip dipol

### 6.3.1 Distanță mică, fără obstacole

Rezultatele din Figura 20 sunt obținute în condiții favorabile, antena fiind poziționată la o distanță mică (aproximativ 1 m față de cablul HDMI)

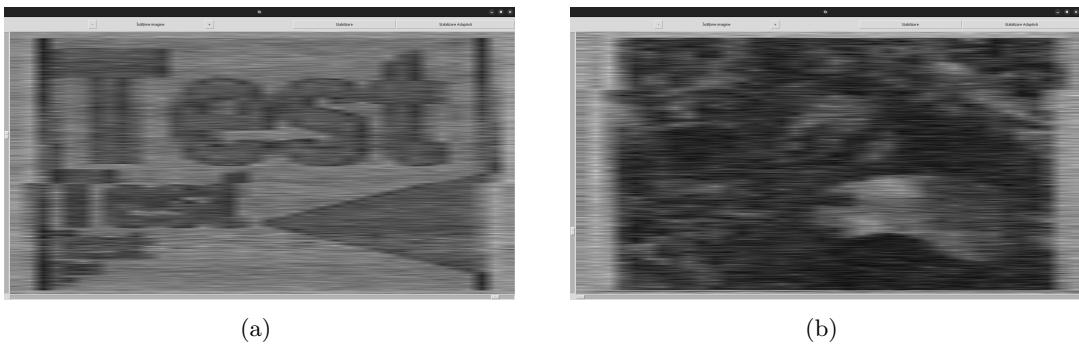


Figura 20: Reproducerea cadrelor din Figura 17 la distanță mică

Textul de dimensiuni mari este inteligibil, însă pentru dimensiuni mai mici rezoluția orizontală mică afectează lizibilitatea. De asemenea, în cadrele reproduse apare și informația adițională menționată în capitolul 5.1 în modul în care am anticipat, adică niște blocuri alipite imaginii. În cadrul din Figura 20b nu se disting decât blocuri mari de culori.

### 6.3.2 Distanță medie, cu obstacole

Am realizat acest test la o distanță mai mare, de aproximativ 8 m; punctul de emisie și cel de recepție sunt în încăperi diferite. O reprezentare schematică a locului în care au fost realizate acest teste se regăsește în Anexa 8.4.

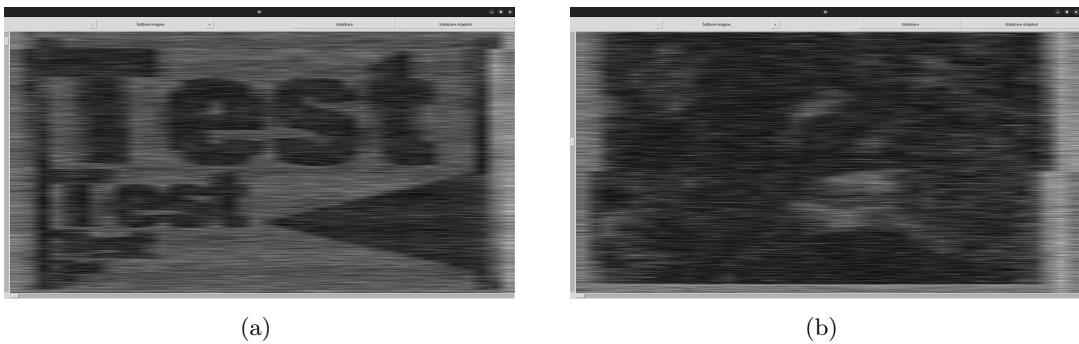


Figura 21: Reproducerea cadrelor din Figura 17 la distanță medie, cu obstacole

Rezultatele sunt similare ca cele obținute la testul anterior, însă contrastul cadrului este scăzut.

### 6.3.3 Distanță mare, cu obstacole

Acet test a fost realizat la o distanță mai mare, cu mai multe obstacole între punctul de emisie și recepție. Rezultatele sunt similare cu punctul anterior, iar, față de acesta, contrastul cadrului este și mai scăzut.

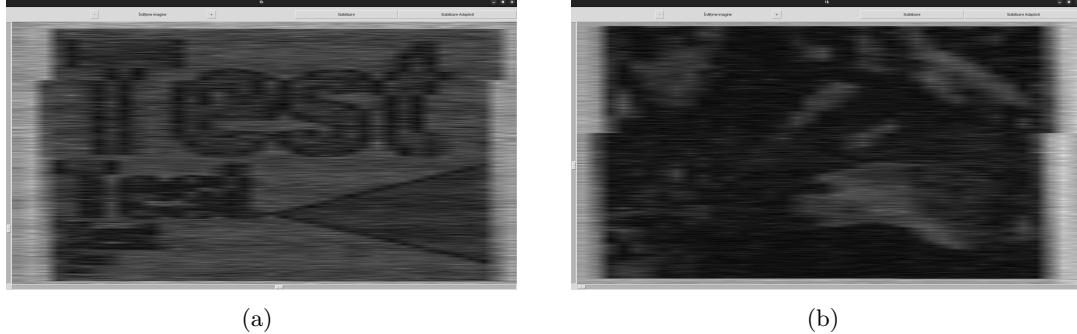


Figura 22: Reproducerea cadrelor din Figura 17 la distanță mare, cu mai multe obstacole (ziduri, mobilier, lifturi)

Programul a reușit să identifice corect parametrii cadrelor (lățime, înălțime și *refresh rate*). Înălțimea trebuie totuși modificată manual, dar aceasta se datorează erorilor de rotunjire care apar din împărțirea numărului de eșantioane dintr-un cadru la lățimea (reprodusă) pe orizontală.

Totuși, calitatea cadrului reprobus nu este foarte bună. Un factor este rezoluția scăzută pe orizontală, ce limitează detaliile ce pot fi reprodate. Alt factor ce contribuie la scăderea calității este distorsionarea informației legate de culoarea pixelilor. Efectul este mai drastic decât cel simulat în Figurile 7 și 8 și depinde de armonica în jurul căreia sunt reprodate datele, efect vizibil în Figura 18.

## 7 Limitări și concluzii

### 7.1 Limitări

#### 7.1.1 Limitări teoretice

Una dintre cele mai mari limitări teoretice ale metodei dezvoltate de mine este vizibilă în ecuația (6), ce arată că  $Q(j\omega)$  acționează ca un filtru asupra lui  $x[k]$ . Cum am menționat deja, dacă funcția  $q(t)$  este cunoscută este posibilă o aproximare a efectelor acestui filtru și, implicit, de compensare pentru el.

Dacă funcția  $q(t)$  este mai complexă, pot fi utilizate diferite tehnici de prelucrare a semnalelor direct pe semnalul recuperat. Acestea presupun, însă, cunoașterea anumitor proprietăți ale semnalului. Majoritatea protocolelor de comunicație pe linii de date au un grad de redundanță, deci prelucrarea datelor recuperate pentru a diminua efectele de filtru ale funcției  $q(t)$  este plauzibilă.

Transmiterea paralelă a mai multor semnale cu proprietăți similare, al căror emisie ocupă benzi de frecvență apropiate în spectrul electromagnetic cauzează însumarea lor, iar datele nu vor mai putea fi recuperate. În capitolul 6 această limitare este vizibilă prin absența culorii din imaginile reproducute. Specific în cazul transmisiilor prin cabluri HDMI, suma emisiilor provocate de cele trei transmisiuni paralel (una pentru fiecare canal de culoare) este în continuare utilă, de aceea poate fi reconstruită o imagine ce poate fi recunoscută.

#### 7.1.2 Limitări practice

Probabil ce mai mare limitare practică este receptia semnalului radio emis. Majoritatea dispozitivelor electronice și cablurilor de date sunt construite astfel încât emisiile electromagnetice produse de acestea să fie minime, pentru a îndeplini diferite standarde. De asemenea, multe tehnici menite să reducă interferențele externe diminuează simultan emisiile dispozitivului/cablului respectiv, e.g. ecranarea cablurilor. În practică, majoritatea semnalelor radio (emise intenționat) au o putere foarte mică, iar dispozitivele create să receptiveze unde radio (precum SDR-urile) au o sensibilitate ridicată.

Chiar dacă emisiile la sursă au o putere suficient de mare, mediul din jurul lor le poate afecta negativ puterea, fiind parțial absorbite de perete sau alte obiecte. Mai mult, majoritatea materialelor absorb unde radio preferențial, în funcție de frecvență, deci diminuarea puterii emisiilor nu este uniformă.

Un alt considerent practic este disponibilitatea spectrului radio. Diferite intervale din acesta sunt alocate pentru diferite aplicații și sunt aproape în permanență „ocupate“, făcând acel interval din spectru neutilizabil sau utilizabil dar cu interferențe. Programul dezvoltat în cadrul acestei lucrări permite reconstrucția cadrelor cu ajutorul oricărei armonice a semnalului emis de liniile de date, însă dacă o armonică se situează în intervale de frecvențe deja utilizate de alte aplicații, aceasta nu mai poate fi utilizată în program. De exemplu, în Figura 18a este vizibil efectul acestor interferențe. În România, spectrul radio în jurul frecvenței de 148.5 MHz este utilizat pentru diferite aplicații mobile, meteorologice și militare [9].

Pentru a reproduce în totalitate semnalul, este necesar ca, la recepție, fiecare valoare a lui  $x[k]$  (din ecuația 5) să fie eșantionată cel puțin o dată. Deși SDR-urile au o plajă de frecvențe largă, acestea nu sunt (de obicei) proiectate pentru lățimi de bandă (și, implicit, rate de eșantionare) ridicate, iar costul acestora crește rapid cu cât lățimea lor de bandă este mai mare. În Tabelul 1 am inclus diferite dispozitive SDR, împreună cu frecvența maximă de eșantionare și costul aproximativ al fiecaruia.

Pentru a asigura că semnalul are o amplitudine semnificativ mai mare decât zgomotul, este necesar ca la recepție să se aleagă o antenă adecvată. Deși antenele de tip dipol ajustabile sunt versatile, întrucât lungimea acestor și, implicit, frecvența la care au performanțe maxime este ajustabilă, nu este întotdeauna practică utilizarea lor. Dacă parametrii semnalului inițial sunt complet necunoscuți, este necesară utilizarea tehnicii descrise în capitolul 5.2.1 și, implicit, ajustări dese ale lungimii antenei. De exemplu, pentru a genera Figura 18, am modificat lungimea antenei pentru

Nume SDR	Frecvență maximă de eșantionare [MHz]	Pret [\$]
RTL-SDR V3	2.4	30
HackRF One	20	300
LimeSDR Mini	40	160
USRP B200	56	1300
USRP N200	100	3000
USRP X310	160	9500
USRP X440	2000	26000

Tabelul 1: Performanțele unor SDR-uri și costul acestora

fiecare armonică, iar întregul proces a durat aproximativ treizeci de minute.

O alternativă poate fi utilizarea de antene ce pot capta fidel o bandă largă din spectrul electromagnetic, e.g. antene log-periodice. Acestea sunt de obicei mai voluminoase și ar reduce semnificativ portabilitatea.

## 7.2 Concluzii

În această lucrare am arătat cum anumite transmisii prin linii de date pot fi interceptate de la distanță, chiar din alte camere, fără a fi nevoie de a modifica în prealabil liniile de date. Dispozitivele SDR, tehnica necesară aplicării procedeului dezvoltat, sunt versatile, nu au un cost ridicat și utilizarea lor nu necesită decât cunoștințe de bază din domeniul (radio)electronicii.

Totuși, rezultatele testării folosind cabluri HDMI ca suport arată limitările acestei tehnici. Am arătat cum, pentru transmisii de date pe fir, rata de eșantionare a SDR-urilor poate fi prea mică, conducând la o reproducere incompletă a datelor. Am analizat influența distanței asupra fidelității reproducării datelor și am sesizat o scădere a acesteia pe măsură ce distanța crește.

Consider că metodele descrise în această lucrare nu au precizia necesară pentru a reconstrui (aproape) perfect un semnal electric bazat emisiile electromagnetice ale acestuia, însă rezultatele arată că pentru anumite tipuri de date, unde există redundanță, reproducerea poate fi suficient de fidelă încât parte din informație să fie recuperată.

Pot exista îmbunătățiri în calitatea rezultatelor cu metoda descrisă, de exemplu prin utilizarea unui SDR mai performant sau o alegere mai atentă a antenei. Totuși, consider că o îmbunătățire sesizabilă poate fi adusă prin extinderea modelului teoretic pentru a lua în calcul aspecte ce au fost simplificate în această lucrare: materialul liniilor de date, forma acestora, influența semnalului  $q$  asupra spectrului și altele.

## 8 Anexe

### 8.1 Apel al programului necesar achiziției de date

Modul de apel în linia de comandă al programului [10], pentru  $f_c = 148.5 \text{ MHz}$ ,  $f_e = 2.56 \text{ MHz}$

```
1 rtl_sdr -g 0 -f 148500000 -s 2560000 -
```

Adăugând și programul pe care l-am dezvoltat (`main.py`) apelul arată astfel

```
1 rtl_sdr -g 0 -f 148500000 -s 2560000 - | python3 ./main.py
```

### 8.2 Secvențe de cod pentru determinarea $W$ , $H$ , *refresh rate*

```
1 corr = xcorr(fr) # fr este semnalul s din lucrare (modulul esantioanelor
                   # achiziționate de SDR)
2 corr = corr[:len(corr)//3]
3
4 fps = findfps(corr, samplerate) # variabila pentru refresh rate
5 [w, h] = findspeed(corr, samplerate, fps) # variabila pentru latimea, respectiv
                                             # inaltimea cadrului
```

```
1 def xcorr(a):
2     a = np.fft.fft(a) # algoritmul fft implementat de biblioteca numpy
3     a = a * np.conj(a)
4     a = np.fft.ifft(a)
5
6     return a
```

Secvența 1: Funcția xcorr

```
1 def findfps(corr, samplerate):
2     global fpsmin, fpsmax
3     corr = np.abs(corr)
4     spike = np.argmax(corr[int(np.round(samplerate/fpsmax)):int(np.round(samplerate/
                   fpsmin))])
5
6     return samplerate/(spike + int(np.round(samplerate/fpsmax)))
```

Secvența 2: Funcția findfps

```
1 def findspeed(corr, samplerate, fps):
2     global hmin, hmax
3     cr = corr[int(samplerate/fps/hmax):int(samplerate/fps/hmin)+1]
4     w = np.argmax(cr) + int(samplerate/fps/hmax)
5     h = int(np.round(samplerate/w/fps))
6
7     return [w, h]
```

Secvența 3: Funcția findspeed

```
1 fftcurr = np.fft.fft2(fr).conj()
2 fftlast = np.fft.fft2(lastFrame) # lastFrame este cadrul de referinta
3
4 corr2 = np.real(np.fft.ifft2(fftlast * fftcurr))
5 posmax = np.argmax(corr2)
6
7 posmax = np.unravel_index(posmax, fr.shape)
8
9 fr = np.roll(fr, posmax[0], axis=0)
10 fr = np.roll(fr, posmax[1], axis=1)
```

Secvența 4: Secvență de cod utilizată pentru stabilizarea imaginii

### 8.3 Citirea eșantioanelor în main.py

```
1 bytewbuff = bytearray()
2
3 while len(bytewbuff) < 2 * samplerate:
4     bytewbuff += os.read(0, buffer_size)
5
6 fr = bytewbuff [:2*samplerate]
7
8 fr = np.frombuffer(fr, 'u1')
9 fr = fr[0::2] + 1j*fr[1::2]
10 fr = abs(fr)
```

### 8.4 Schița locului testării

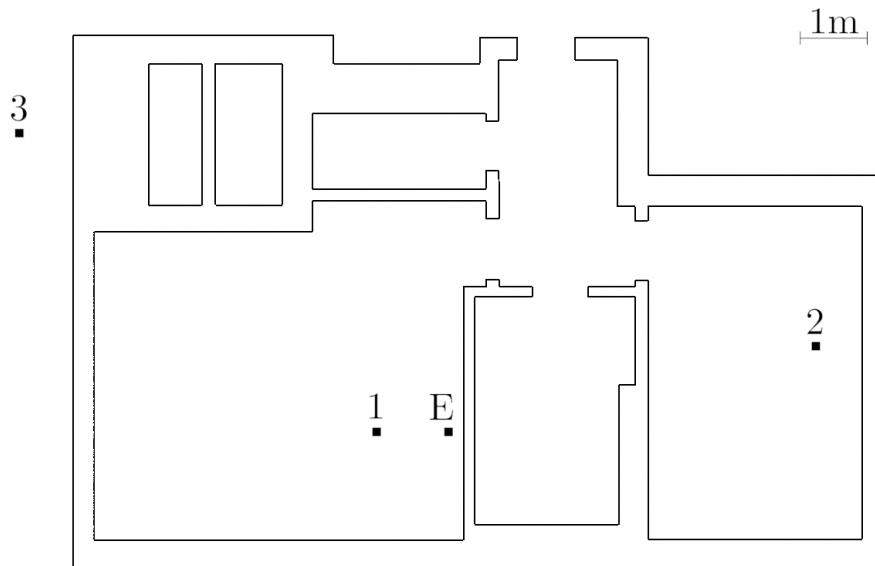


Figura 23: Schița aproximativă a locului în care s-au realizat teste; E este punctul de emisie (unde se află cablul HDMI), punctele 1, 2, 3 reprezintă locul de unde s-au realizat teste din capitolele 6.3.1, 6.3.2, respectiv 6.3.3

## Referințe

- [1] William Marcus Abraham Marcus, *Elements of Radio*, Prentice-Hall, INC., 1943.
- [2] Wim Van Eck, "Electromagnetic radiation from video display units: An eavesdropping risk?", în *Computers & Security* 4.4 (1985).
- [3] C.A. Balanis, *Antenna Theory: Analysis and Design*, Wiley-interscience, Wiley Interscience, 2005.
- [4] *High-Definition Multimedia Interface*, versiunea 1.3a, Hitachi, Ltd., Matsushita Electric Industrial Co., Ltd., Philips Consumer Electronics, International B.V., Silicon Image, Inc., Sony Corporation, Thomson Inc., Toshiba Corporation, Oct. 2006.
- [5] K.R. Rao, D Kim și Jae-Jeong Hwang, *Fast Fourier Transform - Algorithms and Applications*, Ian. 2010.
- [6] Jérôme Leclère, Cyril Botteron și Pierre-André Farine, "Improving the performance of the FFT-based parallel code-phase search acquisition of GNSS signals by decomposition of the circular correlation", în vol. 2, Sept. 2012.
- [7] Oliver C. Ibe, în *Fundamentals of Applied Probability and Random Processes (Second Edition)*, ed. de Oliver C. Ibe, a 2-a ed., Academic Press, 2014.
- [8] *RTL-SDR Blog V3 Datasheet*, RTL2832U, V3, RTL-SDR, Feb. 2018.
- [9] Autoritatea Națională pentru Administrare și Reglementare în Comunicații, *Tabelul Național de Atribuire a Benzilor de Frecvențe*, Feb. 2024.
- [10] URL: <https://github.com/osmocom/rtl-sdr>.

## **Lista contribuțiilor personale**

<b>Titlu:</b> Utilizarea tehnologiei SDR pentru interceptarea comunicărilor pe liniile de date		
<b>Autor:</b> Micu Sergiu-George		
<b>Coordonator:</b> Conf. dr. ing. Nicolae Maximilian-Eugen		
	Activitate	Durată [zile]
1	Documentare despre tehnologia SDR	5
2	Analiza teoretică a semnalelor electrice din linii de date	5
3	Identificarea emisiilor și compararea lor cu cele prezise teoretic	2
4	Familiarizarea cu diferite software-uri utile pentru SDR-uri	10
5	Implementarea unui program preliminar pentru comunicarea cu SDR-ul și interpretarea datelor achiziționate	2
6	Analiza datelor achiziționate și dezvoltarea unui mod de deducere a <i>refresh rate</i> -ului	5
7	Rezolvarea problemelor intervenite în reproducerea cadrelor (stabilizare și reesanționare)	10
8	Documentare despre transformata Fourier discretă bidimensională și utilizarea FFT pentru calculul corelației circulare bidimensionale	2
9	Realizarea unei interfețe grafice preliminare	1
10	Modificarea bibliotecii utilizată pentru afișare și refacerea interfeței grafice	2

Tabelul 2: Lista contribuțiilor personale