Kommmunikation

EQ1270 STOKASTISKA SIGNALER OCH SYSTEM

29 februari 2016

Carl-Johan Larsson
910307-3152
Email: cjlars@kth.se

Gustaf Rydholm
900821-1238
Email: grydholm@kth.se

***Sammanfattning*—Agent 007 är i Stockholm för att lösa hans senaste uppdrag. Han har erhållit en krypterad bild på brottslingen han är ute efter, men har haft stora problem att avkryptera den eftersom krypteringsnyckeln blivit distorderad då den skickats till han $SpyPhone^{TM}$. James bond har tagit hjälp av två elektrostudenter som arbetar för den svenska underrättelsetjänsten för att hjälpa honom att avkoda bilden.**

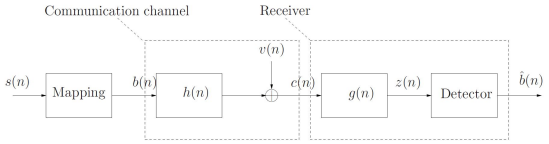
Bilden filtrerades och avkodades med hjälp av ett FIR-Wienerfilter med goda resultat. James Bond kunde samma dag gripa brottslingen. Brottslingen visade sig vara Jokern.

I. Introduktion

Målet med projektet var att desgina en metod för att avkoda en krypteringsnyckel som skickats via digital radio kommunikation. Då krypteringsnyckeln skickats har signalen blivit förvrängd och distorderad av nätbrus. Den valda designen för att avkoda och återskapa krypteringsnyckeln var ett utjämningsfilter.

II. Teori

Då en signal skickas över ett kommunikationsnätverk så uppkommer störningar i signalen. Denna process kan illustreras av figur 1 .



Figur 1: *Filtrerade signalen* $b(n)$.

Där $s(n) \in \{0, 1\}$ är de krypterade data bitarna, som sedan mappas till symboler $b(n) \in \{-1, 1\}$. När de sedan sänds med digital radiokommunikation så tillkommer även en distortion av signalen, $h(n)$ och ett pålagt brus $v(n)$. När sedan signalen som ska avkodas erhålls, $c(n)$, så är den modifierad på ett sätt som kan modelleras med hjälpa av ekvation 1. Olika kommunikationskanaler har olika störningar, i detta fall kan vi utgå ifrån att nätstörningen $v(n)$ är gaussiskt vitt brus.

$$c(n) = \sum_{l=0}^{3} h(l)b(n-l) + v(n) \tag{1}$$

Signalen som ska avkodas skickas sedan till ett utjämningsfilter,$g(n)$, som tar bort bruset som uppkommit från nätverksstörningarna. För detta används ett kausalt FIR-Weinerfilter. För en närmare perfekt återskapning av signalen krävs ett olinjärt filter, dock uppfyller ett linjärt filter målen för uppgiften. Det kausala FIR-Weinerfilter kan modelleras som i ekvation 2, där $\hat{b}(n)$ är en estimator av $b(n)$.

$$\hat{b}(n) = sign\{\sum_{l=0}^{L} g(l)c(n-l)\} \tag{2}$$

För att designa ett utjämningsfilter krävs det att man har någon sorts information om den utsända signalen. Denna information används för att hitta de rätta vikterna för filtret, $g(l)$.

För att göra detta har normalekvationerna använts, ekvationerna 3,4. Med hjälp av dessa går det att skapa de optimala vikterna till filtret, ekvation 5.

$$r_{\mathbf{bc}} = E[b\mathbf{c}] \tag{3}$$

$$\mathbf{R}_{\mathbf{c}}^{-1} = E[\mathbf{c}\mathbf{c}^T] \tag{4}$$

$$g_{FIR} = \mathbf{R}_{\mathbf{c}}^{-1} r_{\mathbf{bc}} \tag{5}$$

För att avgöra om vikterna är optimala används medelkvadratfelet som ett mått på optimalitet hos vikterna 6. När medelkvadrat felet,MSE, mellan

estimatorn och den utsända signalen närmar sig noll, närmar sig vikterna optimalt värde.

$$MSE[\hat{b}(\mathbf{c})] = E[(\hat{b}(\mathbf{c}) - b)^2] \tag{6}$$

När man erhållt vikterna så går det det sedan att använda filtret på den mottagna signalen och återskapa den utsända signalen i den utsträckning ett linjärt filter kan på olinjär information.

III. Praktik

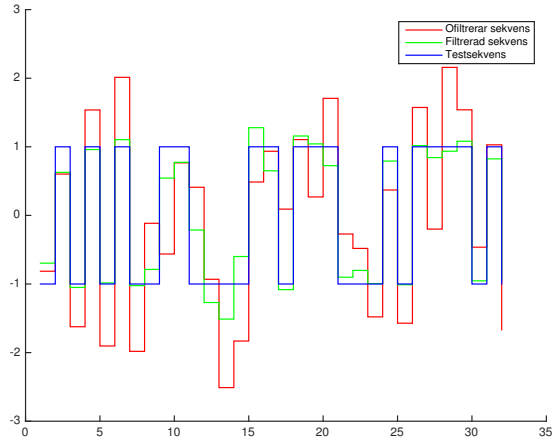
För avkoda nyckeln måste vikterna i det kausala FIR-Wienerfiltret bestämmas. Detta sker genom att använda den mottagna signalen, $\mathbf{c}(n)$, och testsekvensen, $\mathbf{b}_t(n)$, som är givna i uppgiften. Först skapas en autokorrelationsfunktion (akf) för $\mathbf{c}(n)$. Med hjälp av akf:n kan sedan effektspektrummet, $\mathbf{R_c}$, beräknas. Från datasekvenserna $\mathbf{c}(n)$ och $\mathbf{b}_t(n)$ utförs sedan en korskorrelation $\mathbf{r_{cb}}_t(n)$. Vikterna till viktfunktionen, g_{FIR}, beräknas av ekvation 5. Med dessa beräkningar nu utförda kan skattning av den ursprungliga singalen göras med ekvation 2. För att avgöra om denna skattning är bra används medelkvadratfelet, ekvation 6, där en god skattning ger värdet noll. En iteration av denna process utfördes där upp till 32 bitar av meddelandesignalen användes, detta för att träningssignalen bara hade detta antalet bitar.

Det optimala utjämningsfiltret hade en grad på 31, där den avkrypterade bilden ges av figur 2.

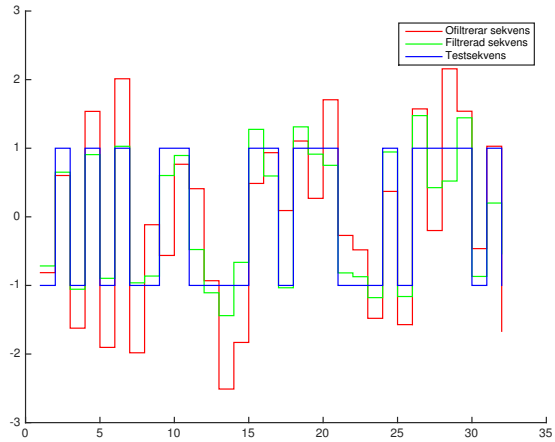
Figur 2: *Avkrypterade bilden på fienden.*

Att detta filter är optimalt kan motiveras av att jämföra med en filtrerad nyckel av ett lägre gradtal, som i detta fallet ges av grad 23 och visas i figur 4.

Genom att jämföra de skattade signalerna ser man att signalen i figur 3 är bättre anpassad till testsekvensen än vad i figur 4. Detta syns ännu tydligare



Figur 3: *Den skattade signalen med grad 31 jämförd med testsekvensen och den mottagna signalen.*

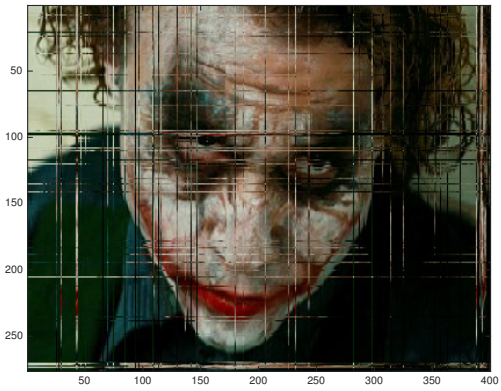


Figur 4: *Den skattade signalen med grad 23 jämförd med testsekvensen och den mottagna signalen.*

genom att använda den nyckel som är given av grad 23 för att avkryptera bilden på fienden, som man ser i figur 5 är av visuellt sämre kvalité än figur 2.

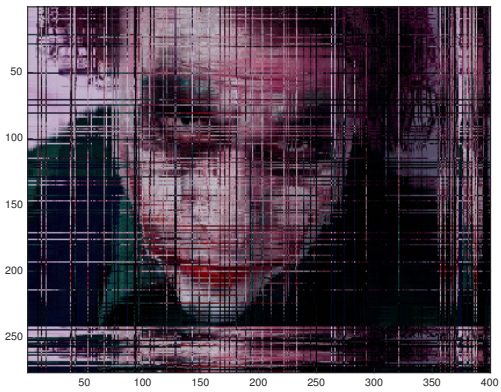
För att undersöka hur stor inverkan bitfel hade på informationen i bilden testades tillslut olika intervall av medvetna bitfel i nyckeln. Detta gjodes genom att på ett slumpmässigt sätt invertera bitar i nyckeln, så -1 blev 1 och 1 blev -1.

Beroende på vilka bitar i nyckeln som påverkades blev resultaten olika vid flera iterationer. Dock så var den gräns, där vi ansåg att det ej längre gick att urskilja bilden vid många iterationer, kring 550 bitfel. Bilden som erhölls vid 550 bitfel i krypte-



Figur 5: *Avkrypterad bild på fienden med gradtal 23.*

ringsnyckeln illustreas i figur 6.



Figur 6: *Bild på fienden med 550 bitfel.*

IV. Slutsatser

Bilden som filtrerades med ett FIR-Wienerfilter kunde avläsas med god marginal, dock var det kvar en del distortioner i bilden. Detta kan ha berott på att bitar från nyckeln försvunnit vid överföring via kommunikationsnätet, men med största sannolikhet att filtreringen av signalen ej var helt optimal då ett linjärt filter användes. För ha att uppnå bättre skattning av ursprungliga signalen hade olinjära metoder behövts användas.