TDDC03-projekt, våren 2007

Verifiering av namnteckningar

David Abrahamsson Niklas Brammer

Handledare: Viiveke Fåk

Verifiering av namnteckningar

David Abrahamsson Niklas Brammer
Linköpings universitet, Sweden
Email: {davab012, nikbr998}@student.liu.se

Sammanfattning

Detta papper behandlar några olika algoritmer för analys av namnteckningar. Vi har närmare studerat en algoritm som använder Power Spectral Analysis och Principalkomponentanalys. Algoritmen har förbättrats, men vi anser att den borde omarbetas från grunden. Vi har haft för avsikt att studera fler algoritmer men har haft svårighet att finna källkod till dessa, då de flesta tillämpningarna är kommersiella.

1. Inledning

Biometrisk identifiering och verifiering kan ske på flertalet olika sätt, däribland genom ansiktsigenkänning, fingeravtryck och analys av namnteckningar.

I detta papper diskuterar vi olika sätt att analysera namnteckningar. Vi undersöker några populära sätt att verifiera på, för att se hur exakta de är. I emperidelen väljer vi ut en metod som vi implementerar och försöker förbättra.

Vi använder oss i studien av en skrivplatta, som kan registrera pennans position och tryck. Skrivplattan används i ett inledningsskede för att kontrollera implementationen. Senare byts den ut mot en databas bestående av 100 användare med vardera 20 genuina och 20 förfalskade namnteckningar.

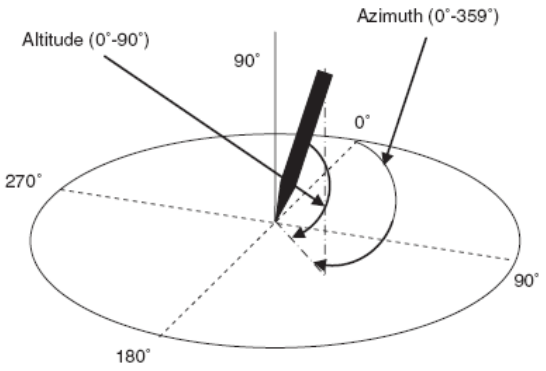
2. Bakgrund

För att mäta hur väl ett biometriskt verifieringssystem är anpassat till sin uppgift används måtten FAR (False Acceptance Rate) och FRR (False Rejection Rate). En hög FAR betyder att en användare lyckas verifiera att han är någon han inte är, medan en hög FRR indikerar att den korrekta användaren ej verifieras. Punkten där dessa felkurvor skär varandrat kallas EER (Equal Error Rate) och detta värde brukar användas för att avgöra hur bra ett verifieringssystem är.

Målet med där att minimera både FAR och FRR. Beroende på systemets säkerhetskrav är dessa olika viktiga. Ett system som ska vara extra säkert kräver ett lägre FAR på bekostnad av högre FRR. Detta innebär att den legitima användaren kan nekas åtkomst vid några av sina försök men medför att det blir extra svårt för en förfalskare vilket i många fall är det viktigaste. [2]

Vid signaturigenkänning måste användaren när denna läggs in i systemet skriva in sin namnteckning ett antal gånger. När användaren senare ska använda systemet jämförs den nu skrivna namnteckningens karakteristika med de tidigare inlagda för att avgöra om användaren är legitim. Till skillnad från andra sätt att biometriskt identifiera användare kan den legitima användarens signatur skilja sig ganska mycket från gång till annan. Exempelvis är ett fingeravtryck i kontrast till detta tämligen statiskt.

Det finns två olika sätt att läsa in signaturer, off-line /statiskt och on-line/dynamiskt. Vid off-line-inläsning används enbart statiska data, det vill säga att enbart signaturens utseende analyseras. Detta kan exempelvis ske genom inskanning av ett papper på vilket signaturen skrivits. Vid on-line-inläsning används exempelvis en elektronisk skrivplatta som utöver spatial data även kan läsa av data som hastighet, tryck och pennans lutning och vridning. Figur 1 visar detta. Denna metod blir säkrare då den utökade karakteristiken uppenbart gör namnteckningen svårare att förfalska än exempelvis en namnteckning på ett papper. Även om en förfalskare kan kopiera en signatur är det osannolikt att han kan skriva in den med samma hastighet och samma tryck på pennan som originalanvändaren. Fler karakteristika innebär inte nödvändigtvis ett säkrare system, eftersom vissa av dessa värden fluktuerar mycket från gång till annan.[2]



Figur 1. Data Som kan registreras av plattan [7]

3. Teori

I detta papper ligger fokus på hur data som fångas in från en skrivplatta ska tolkas. En enkel skrivplatta registrerar med jämna mellanrum (typiskt ca 100 -150 gånger per sekund) pennans x-position, y-position och tryck. Vissa avancerade skrivplattor kan även registrera pennans vinkel. Detta genererar stora mängder data som sedan måste behandlas på lämpligt sätt för att bli hanterbart och få bra EER. [2]

Vid on-line-inläsning talar man om två olika typer av information; lokal och global. Lokal information kan vara pennans tryck i den aktuella punkten medan ett globalt värde exempelvis är tiden det tar att skriva hela namnteckningen. Ett globalt värde kan även beskriva en del av signaturen, exempelvis tiden mellan att man sätter ner pennan och lyfter den igen. Ett verifieringssystem som helt bygger på globala värden blir mycket snabbt, men inte speciellt exakt. Många metoder kombinerar lokala och globala värden.[6]

Nedan beskriver vi ett antal algoritmer som kan användas för att hantera data som fångats in från en skrivplatta. Principalkomponentanalysen, som presenteras sist, kommer vi att studera vidare i emperin.

3.1 Artificial neural networks

Neurala nätverk kan användas för att lösa problem som inte lätt kan lösas med datalogiska metoder. Ett exempel på detta är mönsterigenkänning, som kan kopplas ganska väl till vårt problem med igenkänning av namnteckningar. Neurala nätverk kräver en viss inlärningsfas innan de kan börja tillämpas. Systemen kan tillåtas att fortsätta lära sig även när de tagits i bruk, men det vanliga är att inlärningsfasen avslutas när resultatet är tillfredsställande.

Det finns exempel där neurala nätverk med bakåtpropagering har testats extensivt för signaturigenkänning med mycket goda resultat. En FRR på 0,0 % (teoretiskt 0,0001 %) och en FAR på mindre än 0,1 % har uppnåtts i försök gjorda av Dariusz med flera [1].

3.2 Dynamic Time Warping

Dynamic time warping (DTW) är en algoritm som jämför likheter mellan två sekvenser som kan variera i tid eller hastighet. Det kan exempelvis röra sig om en och samma person som vid olika tillfällen går olika fort, eller två strängar av olika längd som ska jämföras. Dynamic time warping används främst inom området röstigenkänning, men textigenkänning är även ett område inom vilket det ökar.

En signatur kan beskrivas av ett antal kurvor (position, tryck osv). Metoden hittar för varje element i kurvan för den ena signaturen, det bäst motsvarande elementet i kurvan för den andra signaturen. För att göra det försöker man minimera det totala euklidiska avståndet mellan punkterna. [8]

Enligt Martens och Claesen har DTW länge förekommit inom textigenkänning , utan att ansträngning har gjorts för att dra nytta utav namnteckningens specifika karakteristika. Exempelvis finns för namnteckningar flertalet referensbilder, utifrån vilka man kan avgöra vilka delar som är viktiga och vilka som är mindre viktiga. I sin rapport presenterar de sin implementering som ger en hyfsat låg EER. [4]

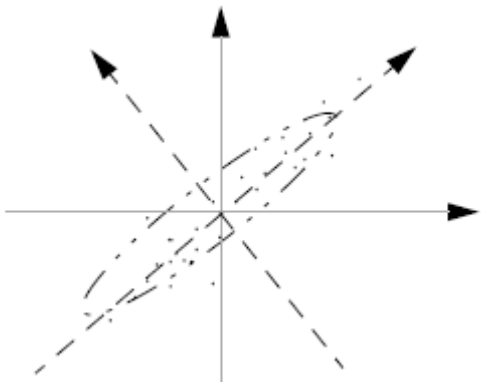
3.3 Hidden Markov Model

Den dolda Markovmodellen (HMM) är en statistisk modell i vilken det modellerade systemet ses som en Markovprocess med okända parametrar. Tricket är att plocka fram de dolda parametrarna genom att analysera de kända. När dessa erhållits kan de användas till exempelvis mönsterigenkänning. Dolda Markovmodeller är, precis som DTW, viktiga inom röstigenkänning.

Kashi med flera hävdar att man med hjälp av dolda Markovmodeller signifikant kan förbättra prestandan hos ett system för igenkänning av namnteckningar. De utgår från en algoritm som tar hänsyn till både globala och lokala egenskaper, och menar att de får FAR att minska från 13 % till 5 % när de använder sig utav dolda Markovmodeller.[6]

3.4 Principal Component Analysis

Principalkomponentanalys används för att hitta lågdimensionella samband i högdimensionella rum. Den är likt den dolda Markovmodellen en statistisk modell. Vid principalkomponentanalys sker en relativt grov komprimering utav de data man har tagit in. Från utgångsläget med många variabler arbetar man sig ner till 2-3 dimensioner, så att man lätt ska kunna göra en jämförelse. Figur 2 visar hur man vrider diagrammet så att en axel hamnar i den riktning där de finns flest punkter. Denna axel blir den första principalkomponenten. Sedan vrider man så att nästa axel hamnar där det finns många punkter och så vidare.[3][5]



Figur 2. Principalkomponentanalys [5]

4. Empirisk studie

I vår studie har vi valt att undersöka ett system som använder sig av principalkomponentanalys. Vi utgår från en implementation gjord i en tidigare laboration vid universitetet. Utifrån den lägger vi till kod för att få fram FAR- och FRR-värden och försöker förbättra dem. Metoden som används är Power Spectral Analysis på de värden som fås från skrivplattan, nämligen x, y och tryck (z).

Genom en PSA förändras inte storleken på indatan. För att komma till rätta med det delas spektrumet in i 11 delområden och i varje område räknas ett medelvärde fram. Dessa 11 värden läggs sedan ihop för x,y och z och bildar en 33-dimensionell vektor.

För att ytterligare minska storleken på datan används Principalkomponentanalys, som beskrivs ovan. Efter detta har vi fortfarande 33 dimensioner, men sorterade efter relevans. När man i vanliga fall gör PCA väljer man ut x antal dimensioner, sparar värdena för dessa och slänger resten. Vi sparar alla 33 för att kunna jämföra vad som händer beroende på hur många dimensioner som används senare när namnteckningar ska jämföras med varandra.

En signatur representeras alltså av sin koordinat i det 33-dimensionella rummet. För att avgöra hur lika en inmatad signatur är referenssignaturerna, mäter vi det euklidiska avståndet mellan signaturen och den referenssignatur som ligger närmast. Vi vill ha detta värde mellan noll och ett för enkel jämförelse. En signatur som ligger längre bort från den närmaste referenssignaturen än *template_max*, där *template_max* är det största avståndet mellan de två referenssignaler som ligger längst från varandra, räknas som en säker icke-träff och får värdet noll. Vi räknar ut likheten med följande formel:

similarity = mindist/template_max

4.1 Testdata

Den testdata som används är från den offentliga databasen från andra omgången i SVC 2004 [9], den första internationella tävlingen i signaturigenkänning. Databasen består av totalt 100 uppsättningar signaturdata. Varje uppsättning innehåller 20 genuina signaturer och 20 noggranna förfalskningar gjorda av minst fyra olika personer. Värt att notera är att de som bidrog med signaturer fick träna in en ny personlig signatur av integritetsskäl samt att signaturerna är både kinesiska och engelska. För att efterlikna vår skrivplattas funktion använde vi oss enbart av värdena för x-position, y-position och tryck.

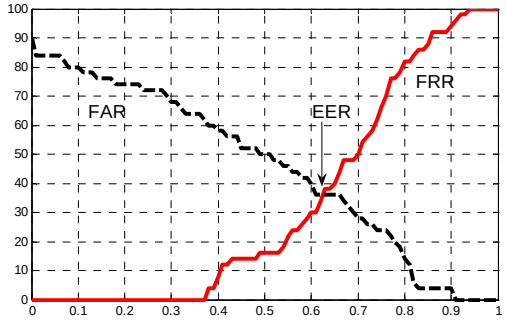
4.2 Testets förfarande

Algoritmen initieras med de 6 första genuina signaturerna för person 1 till 40, härefter kallade referenssignaturer. För att testa algoritmen använder vi först genuin signatur 10 till 20 för person 1 till 5 för att se FRR. När algoritmen matas med en signatur får vi som svar ett värde mellan 0 och 1 som visar hur lik signaturen är referenssignaturen. Vid 1 är de identiska. För att bestämma om signaturen är tillräckligt lik och alltså ska accepteras jämförs svaret vi får med ett så kallat gränsvärde. Om svaret är högre än gränsvärdet accepteras signaturen. FRR beräknas för gränsvärden mellan 0 och 1, i steg om 0,1. Antalet accepterade signaturer divideras med 50, det vill säga det totala antalet signaturer som algoritmen testas med, och multipliceras med 100 för att få FRR i procent.

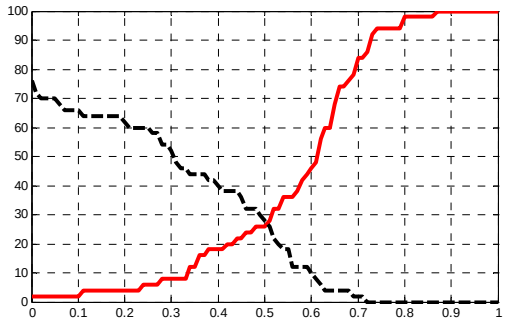
För att beräkna FAR använder vi samma förfarande, men med förfalskad signatur 1 till 10 som indata. Vi plottar sedan FAR och FRR med gränsvärdet på x-axeln och procent på y-axeln.

Ett ungefärligt värde på EER fås genom att läsa av var kurvan för FRR och FAR skär varandra.

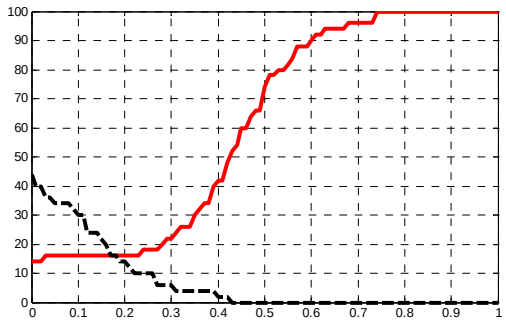
Vi får enligt figur 3 ett EER-värde på 37 % som är under all kritik. Genom att använda fler dimensioner vid jämförelsen av en signatur mot referenssignaturerna får vi bättre och bättre värden. Bäst värde får vi då alla 33 dimensioner används. Vår EER blir då 16 %, enligt figur 5.



Figur 3. Matchning i tre dimensioner



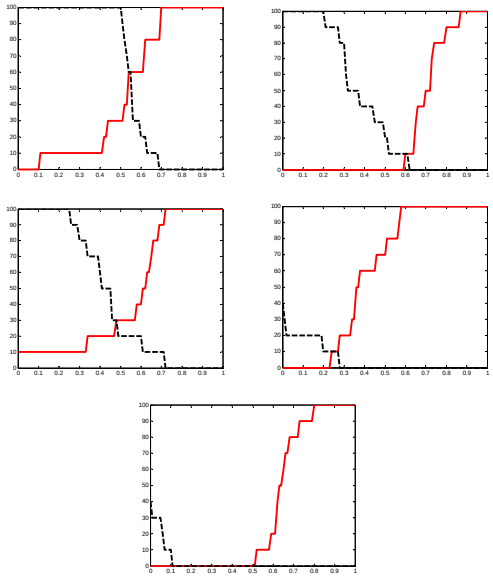
Figur 4. Matchning i 11 dimensioner



Figur 5. Matchning i 33 dimensioner

Vid skapandet av FAR- och FRR-kurvor använder vi oss av flera signaturer men med samma gränsvärde. För att undersöka hur mycket vi kan minska EER genom individuella gränsvärden för varje person tar vi

fram graferna för person 1-5 separat. Vi använder oss av 11 dimensioner för hastighetens skull.

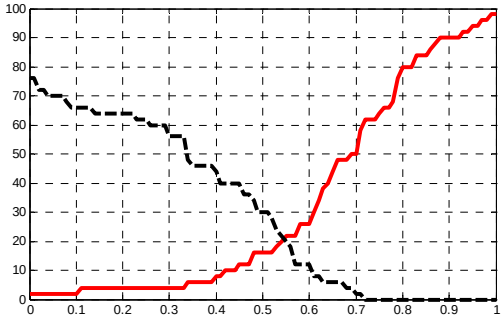


Figur 6. FAR/FRR för fem olika användare med globalt gränsvärde

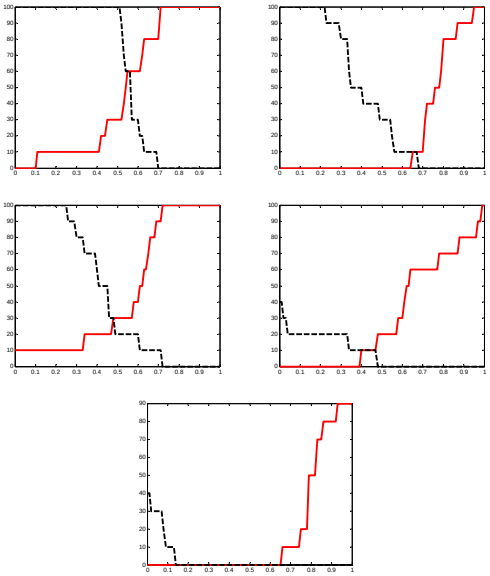
I figur 6 ser vi att några personer har sitt EER vid ett lågt värde på gränsvärdet och några vid ett högt. Optimalt är om alla figurer har skärningen mellan kurvorna vid samma gränsvärde. För att åstadkomma detta behöver vi använda lokala gränsvärden som komplement till det globala.

Vi vill att det lokala gränsvärdet ska visa hur mycket en användares signaturer skiljer sig från varandra i normala fall. Den metod vi använder går ut på att ta fram *local_th*, som är det största av de minsta avstånden mellan alla referenssignaler. Om alla referenssignaler ligger nära varandra, kommer *local_th* att ha ett lågt värde och FAR-/FRR-kurvan ha sitt EER långt till vänster. Slutligen normaliserar vi alla *local_th* för att de ska ligga mellan noll och ett.

De lokala gränsvärdena multipliceras med det globala och kurvorna får det utseende som ses i figur 7. Figur 8 är samma som Figur 4 men vi använder lokala gränsvärden.



Figur 7. Matchning i 11 dimensioner med lokalt och globalt gränsvärde



Figur 8. FAR/FRR för fem olika användare med lokalt och globalt gränsvärde

5. Lösning och analys

Här presenterar vi våra tankar om varför det blev som det blev i den empiriska studien.

5.1 Utvärdering och jämförelse

Att från litteraturen avgöra vilken av alla metoder för verifiering av namnteckningar som är bäst är svårt. Den största svårigheten för oss ligger i att alla använder sina egna databaser med testdata, vilket gör det omöjligt att avgöra om en algoritm är bättre än en annan bara genom att se FAR och FRR.

Eftersom vi inte hittar några implementeringar av modellerna har vi inte kunnat göra egna jämförelser med våra testdata.

5.2 Förbättringar av empirisk modell

I empirin undersökte vi en av modellerna men resultaten från den modellen var så pass dåliga att vi tror den behöver omarbetas helt och hållet. Vi har inte hittat någon annan som använt sig av Power Spectrum Analysis och det finns nog goda skäl till det.

Vi lyckades förbättra modellen lite genom att lägga till lokala gränsvärden. Den skulle förmodligen gå att förbättra ytterligare med någon av de många lokala och globala jämförelser som går att göra. Trots detta anser vi att den mest intressanta fortsättningen till detta arbete är att implementera någon av de övriga modellerna.

6. Relaterat arbete

Inom området bedrivs forskning i stor utsträckning. Det finns en diger lista över tekniska rapporter som behandlar biometrisk verifiering av signaturer. De algoritmer vi har studerat står enbart för en bråkdel av de olika tillgängliga studierna som gjorts.

Något som kan vara intressant är att studera textigenkänning, där det i större utsträckning finns program med öppen källkod

7. Slutsatser

Verifikation av namnteckningar är fortfarande ett hett ämne. Bland biometriska verifieringsmetoder anses den vara den mest accepterade.

Trots att det bedrivs mycket forskning sker stor del av programvaruutvecklingen kommersiellt och det är därför svårt att hitta implementeringar att analysera och testa.

Referenser

[1] Dariusz Z. Lejtman and Susan E. George “On-line handwritten signature verification using wavelets and back-propagation neural networks”, IEEE proceedings of Sixth International Conference on Document Analysis and Recognition ICDAR'01, Seattle, USA, pp 992-996, 2001.

[2] A.K. Jain, Friederike D. Griess and Scott D. Connell, "On-line Signature Verification", Pattern Recognition, vol. 35, no. 12, pp. 2963--2972, Dec 2002.

[3] Bin Li, Kuanquan Wang, David Zhang: “On-Line Signature Verification Based on PCA (Principal Component Analysis) and MCA (Minor Component Analysis)”. ICBA 2004: 540-546.

[4] Martens, R. (IMEC, Leuven, Belgium); Claesen, L. “On-line Signature Verification by Dynamic Time-Warping“, Proceedings of the 13th International Conference on Pattern Recognition, 1996, pt. 3, p 38-42 vol.3

[5] Claesson, Fredrik. ”Identity verification using signatures”. LiTH-ISY-EX-3013. 2001.

[6] Kashi, R.S. (Lucent Technologies); Hu, J.; Nelson, W.L.; Turin, W. “On-line Handwritten Signature Verification using Hidden Markov Model Features”, Proceedings of the International Conference on Document Analysis and Recognition, ICDAR”v 1, 1997, p 253-257

[7] Marcos Faundez-Zanuy. “On-line signature recognition based onVQ-DTW”. Pattern Recognition, v 40, n 3, March, 2007, p 981-992

[8] Wirotius, M.; Ramel, J.-Y.; Vincent, N. “Selection of Points for On-Line Signature Comparison” Proceedings - International Workshop on Frontiers in Handwriting Recognition, IWFHR, Proceedings - Ninth International Workshop on Frontiers in Handwriting Recognition, IWFHR-9 2004, 2004, p 503-508

[9] http://www.cs.ust.hk/svc2004/Task2.zip