Biometrisk igenkänning med fingeravtryck och stereoskopisk ansiktsigenkänning

Christoffer Cronström Ulf Hörndahl

25 augusti 2014

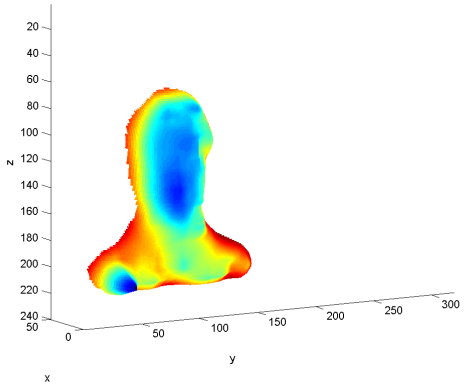
Under det senaste decenniet har maskinell identifiering av människor blivit ett område som företag, myndigheter, och flygplatser blivit intresserade av. Vi har utvärderat hur bra existerande fingeravtrycksidentifieringsmjukvara med öppen källkod är, då öppen källkod ofta bedöms som säkrare. Vi har också försökt lösa ansiktslivstecknesproblemet inom ansiktsigenkänning med hjälp av flera samtidiga kameror och metoder från datorseende.

Våra undersökningar av fingeravtrycksidentifieringsmjukvara begränsades till bara mjukvara med öppen källkod. Öppen källkod är bättre ur säkerhetssynpunkt eftersom det finns många oberoende instanser som kontrollerar säkerheten i systemet, och att man därför inte behöver lita på ett företags egna försäkran att deras mjukvara håller måttet. Dessutom var den av praktiska skäl lättare att jobba med.

I vår undersökning av fingeravtryckstekniken så fann vi att man kan uppnå tillfredsställande resultat med det upphovsrättsbefriade paketet NBIS, utgivet av den amerikanska myndigheten NIST. Paketet bygger på Bozorth-algoritmen som är framtagen av FBI.

Om systemet ställdes in på en falsk acceptans på 1/10 000, dvs. samma som en PIN-kod, blev 20 % av personerna som ägde tillträde nekade, och hade behövt scanna sitt finger flera gånger. Detta är jämförbart med vad proprietära algoritmer presterade i den nyaste undersökningen vi hittade.

Vi kunde även konstatera att de olika fingeravtryckläsarna vi använde gav ungefär likvärdiga resultat, och kan inte dra några slutsatser om vilken läsartyp som är bäst. De två olika standardiserade formaten för att lagra fingeravtrycksinformation, NIST-formatet och ANSI M1-formatet, gav även de ungefär likvärdiga resultat.

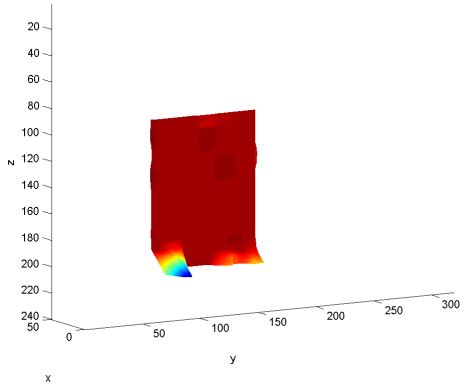


Djupkarta för ett riktigt ansikte. Skalorna och färgerna är godtyckliga.

När det gäller ansiktigenkänning, så finns ett mycket viktigt problem som kallas *face liveness detection*, eller ansiktslivstecken. Det handlar om att märka folks försök att forcera systemet genom att hålla upp ett fejkat ansikte, exempelvis ett fotografi av en betrodd person. För att ges tillgång skyddsobjektet räcker det inte med att ansiktet är betrott, utan systemet måste även övertygas om att ansiktet som visas upp är ett äkta ansikte.

Vi försökte lösa detta problem genom att ta in bilder från två kameror som fotograferat samma subjekt ur två olika, närbelägna vinklar och sedan använda så kallad *structure from motion*, struktur från rörelse, för att beräkna ansiktets utsträckning i tre dimensioner.

Vi fann att vi kunde bygga en djupkarta baserat på våra bilder, som ni kan se i bilderna. Om vi istället



Djupkarta för ett fejkat ansikte, en bit kartong med ett fastklistrat fotografi.

försöker visa upp ett foto av en person, så blir resultatet att en platt yta syns tydligt i djupkartan, vilket är lätt att identifiera maskinellt.

För att summera så kom vi fram till att det är möjligt att detektera vissa sorters försök att förbipassera ett passersystem med stereokameror, samt att den testade mjukvaran går att anpassa för att använda i en faktisk applikation.