**بنام خدا**

موضوع تحقیق :

سیستم اثر انگشت هوشمند حضور و غیاب و استفاده از علم بيومتريك Intelligent Fingerprint and Attendance Systems Useing Biometrics

تکلیف تحقیق درس هوش مصنوعی

استاد مربوطه :

**جناب آقای دکتر میریان**

تهیه کننده :

**جوتد جهانبخش**

شماره دانشجویی :

**894403451726**

www.javad.jahanbakhsh@yahoo.com

زمستان 90

سنسور های اثر انگشت

از نظر دریافت تصویر به دو نوع تقسیم میشوند :  
سنسورهای خازنی   
سنسورهای نوری   
از نظر عملکرد داخلی به دو نوع تقسیم میشوند :  
سنسورهای با قابلیت دریافت,ذخیره,مقایسه ,پردازش تصویر   
سنسورهای با قابلیت فقط دریافت تصویر از اثر انگشت   
مزایا و معایب سنسورهای خازنی :  
سرعت بالا   
قابلیت روشن بودن بدون ارسال هر بار Request   
خش برداشتن در مدت زمان کوتاه   
مزایا و معایب سنسورهای نوری :  
سرعت متوسط   
برای هر بار دریافت تصویر باید عمل Request انجام شود   
مقاوم در برابر خش   
مزایا و معایب سنسورها از نظر عملکرد داخلی (نوع اول)  
دارای حافظه داخلی (مزیت)  
نگهداری اطلاعات بصورت محلی (عیب)   
سرعت بالا به دلیل پردازش تصویر بصورت داخلی(مزیت)  
مزایا و معایب سنسورها از نظر عملکرد داخلی (نوع دوم)  
گرفتن اطلاعات و ارسال آن به بیرون از سنسور(مهمترین مزیت)   
حافظه داخلی ندارند(عیب)  
سرعت به الگوریتم جستجوی نوشته شده توسط برنامه نویس بستگی دارد.(هم میتواند مزیت باشد هم از معایب)  
  
حضور و غياب  
دستگاه كارت خوان  
كارت خوان  
ساعت حضور و غياب   
ساعت حضور و غياب انگشتي   
كارتخوان دوربين دار     
سيستم  حضور و غياب   
دستگاه حضور و غياب   
كارتخوان كارتي   
 دستگاه كنترل تردد كارمندان  
 اثرانگشت  
کارتی  
 دوربين دار   
رمزی   
در بازكن  
كنترل تردد   
سيستم كنترل تردد  
اثر انگشتي   
كارتي  
كدي دوربين دار سيستم كنترل تردد اثر انگشتي  
  
**زنده بودن اثر انگشت و تشخيص هويت**

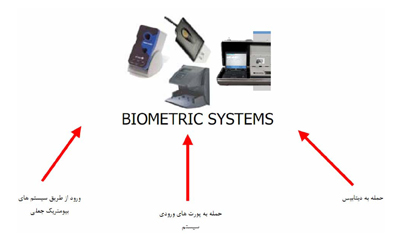
**از سال‌ها پيش از اثر انگشت افراد در جرم ‌شناسي استفاده مي شد و امروزه در علم بيومتريك نيز از آن استفاده ‌مي شود. مانند تمام ديگر اعضاي بدن DNA هاي هر شخصي الگوي ساخت اين خطوط را دارا هستند و در واقع DNA هاي هر شخص نيز كاملا منحصر به فرد است و اين موضوع تقريبا در مورد ديگر اعضاي بدن صادق اند. اثر انگشت از قديمي‌ترين روش هاي تشخيص هويت است كه با پيشرفت تكنولوژي به تنوع آن افزوده شده است. اگر چه قبلا اثر انگشت تنها در زمينه جرم قابل بحث بوده، تحقيقات در بسياري كشورها سطحي از پذيرش را نشان مي دهد كه به اين روش اجازه استفاده در برنامه هاي عمومي را مي‌دهد.خطوطي كه بر روي سر انگشتان همه انسان ها نقش بسته از ديرباز مورد توجه همه بوده است، اين خطوط نقش هاي مختلفي دارند، يكي از اين وظايف ايجاد اصطكاك بين سر انگشتان و اشياء متفاوت است مانند قلم كه با استفاده از اين اصطكاك مي توانيم اشيا را برداريم ، بنويسيم يا لمس كنيم. از سوي ديگر اين خطوط براي هر شخص منحصر به فرد است.**



روش هاي تأييد هويت موجود با سه فاكتور تقسيم بندي مي شوند:  
1- چيزهايي كه كاربران مي دانند( براي مثال رمز عبور،PIN)  
2- چـيــزهــايــي كــه كـاربـران بـه هـمـراه دارنـد (كارت‌هاي خود پرداز، كارت هاي هوشمند)  
3- چيزهايي كه مربوط به خود كاربران است (بيومتريك ها شامل:اثر انگشت، الگوي شبكيه، عنبيه) و…  
دسـتــه ســوم (بـيــومـتــريــك هــا) امــن تــريـن و ســاده‌ٍتــريــن فــاكـتــور تــأيـيــد هــويــت در دنـيــاي اطـلاعـات و ارتـبـاطـات  هـسـتـنـد. بيومتريك به روش هاي خودكار تشخيص يا تاييد هويت يك شخص زنده از طريق اندازه گيري مشخصه هاي فـيـزيـولـوژيـك يـا رفـتاري وي اطلاق مي شود.  بـديـن تـرتـيب بيومتريك يك مجموعه فناوري محسوب مي شود.

**انواع بيومتريك ها :**

**بيومتريك هاي فيزيولوژيك:** عنبيه نگاري  ، شبكيه نگاري، انگشت نگاري، چهره‌نگاري، دست نگاري، صوت نگاري

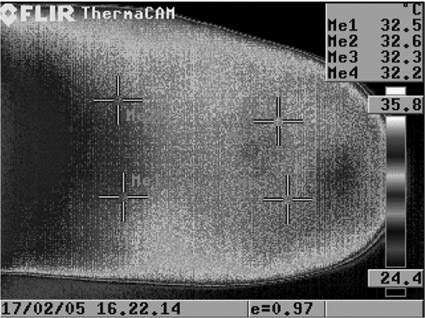


**بيومتريك هاي رفتاري:** امضا نگاري ، نحوه تايپ كردن

**ساير بيومتريك ها:** پارامترهاي ديگري هم اخيرا مورد استفاده قرار گرفته است كه به علل مختلف هنوز كاربرد وسيعي ندارند. از جمله مي توان به بيومتريك هاي نظير DNA،  نحوه راه رفتن، الگوي رگ هاي پشت دست، خطوط كف دست، شكل گوش، بوي بدن و الگوي بافت هاي زير پوستي دست اشاره كرد.  
راه حل نهايي جهت فايق آمدن بر مشكلاتي كه بعضا هر فناوري بيومتريك به همراه دارد استفـاده همـزمان از چند بيومتريك مختلف در يك سيستم است. به اين روش اصطلاحا سيستم چند لايه گفته مي شود.

**امنيت در سيستم هاي بيومتريك :**  
سيستم هاي بيومتريك همواره به روش هاي مختلف مورد هجوم قرار مي گيرند. اين نوع حملات شامل : حمله به ديتابيس ، حمله به پورت هاي ورودي سيستم و حمله به سيستم تشخيص هويت از طريق بيومتريك هاي جعلي است.    
سارقان معمولا جهت فريب سيستم هاي تشخيص هويت از روش هاي مختلفي بهره مي برند، از جمله استفاده از عكس چهره يا عنبيه فرد مقابل دوربين ، ضبط با كيفيت صداي شخص در سيستم هاي بيومتريك صوتي ، استفاده از اثر انگشت ژلاتيني و حتي استفاده از لاشه انگشت! توسط سارقان جهت ورود به سيستم.  
فرايند تشخيص هويت مي تواند هم از طريق نرم افزاري (خواندن و پـردازش اطـلاعـات بيـومتـريـك) بـاشد و هم از طريق سخت افزارهايي كه در امر تشخيص به ما كمك مي كنند .    
در روش سخت افزاري از ابزار هاي مختلفي استفاده مي شود : سنسور دما ، پالس اكسي متري انگشت ، هدايت الكتريكي بافت ،  ECG، Match كردن صداي فرد و حركت لب با تصوير برداري‌،  استفاده از اسكن سه بعدي التراسوند و ...  
در روش نرم افزاري مولفه هاي مختلفي مورد بررسي قرار مي گيرد.  در صورت: جابجابي سر‌، در عنبيه: جابجايي مردمك    
در روش تـشـخـيـص زنـده بـودن انگشـت از روش هاي مختلفي استفاده مي شود كه در ادامه به بررسي آن ها خواهيم پرداخت.

**‌الگوي دمايي نوك انگشت :**يكي از الگوهاي متفاوت در تشخيص زنده بودن اثر انگشت بررسي نقاط مختلف گرم شدن آن است ، در شكل2 قادر به مشاهده اين موضوع خواهيد بود :  
‌سارقان به روش هاي مختلفي اقدام به جعل اثر انگشت مي كنند : از جمله استفاده از مواد ژلاتيني كه كپي برداري از اثر انگشت فرد است ، استفاده از قالب اثر انگشت كه به صورت مواد سفالي و گلي در آمده اند و  همچنين استفاده از لاشه انگشت كه اثر انگشت فرد ديگري است.  
لذا بايد روشي به كار گرفته شود تا از ميان اين حالات ، اثر انگشت زنده و واقعي را تشخيص دهد. در شـكـل زير اثر انگشت يك فرد در حالات مختلف ذكر شده نشان داده شده است :

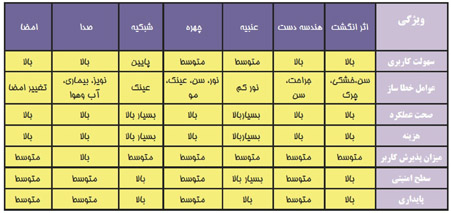


**‌**

**تشخيص از طريق تعرق بافت انگشت  :**در تكنيك تشخيص هويت توسط تعرق بافت ، فرد انگشت خود را روي حسگر قرار مــي دهــد بـعــد از مـدتـي انگشـت عـرق كـرده و ايـن تعـرق در ميـان لبـه هـاي انگشـت پخش‌‌مي‌شود كه  تصوير متفاوتي از اثر انگشت ثبت خواهد شد. اين روش تكنيكي است جهت تشخيص زنده بودن انگشت و جلوگيري از تقلب.

**‌**

**روش هاي اندازه گيري دماي بافت :**روش هاي ديگري نيز وجود دارد و آن اندازه گيري دماي بافت است . اين دما به راحتي و بدون صرف هزينه زيادي قابل اندازه گيري است. دماي بافت انگشت بين 26 تا 30 درجه سانتيگراد قرار دارد. اين  محدوده دمايي براي يك انسان سالم است و چنانچه فرد بيمار باشد موجب بالا رفتن دماي بدن و دماي انگشت شده و نمي تواند ارزيابي خوبي براي اين تشخيص باشد. در روش فوق كاربر امكان فريب سيستم را نيز خواهد داشت و مي شود با سرد يا گرم كردن بافت و نگه داشتن دما در حالت نرمال سيستم را فريب دهد.



**‌ايجاد گرما در محل قرار گيري انگشت :**  
در اين روش فرد انگشت خود را روي سنسور قرار مي دهد و دو دكمه نيز در مقابل قرار دارد چنانچه گرما در محل اثر انگشت زياد شود فرد دكمه قرمز را فشار داده و زماني كه دما كاهش مي يابد   دكمه آبي را فشار مي دهد. پوست انسان نسبت به تغييرات كوچك دما نيز حساس است و براي بدن قابل شناسايي است لذا زماني كه از انگشت هاي جعلي جهت فريب سيستم استفاده مي شود، قابليت تشخيص كم يا زياد شدن دما را نداشته و مجوز ورود به سيستم داده نخواهد شد.



**‌تشخيص زنده بودن اثر انگشت بر پايه آناليز ويولت :**يكي از روش هاي Liveness Detection استفاده از آناليز ويولت است. بر پايه اين روش مي توان اثر انگشت واقعي را از جعلي تشخيص داد.  
مواد استفاده شده در انگشت هاي جعلي معمولا سفالي يا ژلاتيني هستند، اين مواد ساختمان متراكمي دارند كه سطح نامطلوبي از اثر انگشت را ايجاد مي كنند و معمولا سطح چنين مواد سفت تر و زبر تر از بافت واقعي اثر انگشت است. اين تفاوت زبري به عنوان يك روش در تشخيص و تفكيك بافت از نوع غير بافت و جعلي است.  
Liveness Detection توسط روش Fine Movement در سطح انگشت:  
اين روش بر پايه آناليز جابجايي كوچك اثر انگشت و بررسي تغييرات حجمي خون است. در اين روش لازم است تا از يك اسكنر نوري اثر انگشت جهت آناليز تغييرات سيستول و دياستولي قلب نيز استفاده شود.

**‌آناليز  Curvelet و Curvelet Co-occurrence جهت تشخيص حمله هاي اثر انگشت جعلي به سيستم بيومتريك**  
در اين روش بر پايه يك تبديل كرولت جديد قادر خواهيم بود تا اثر انگشت هاي جعلي را تشخيص دهيم. اندازه گيري هاي بافت بر پايه مشخصه هاي انرژي  Curvelet و Curvelet Co-occurrence جهـت تشخيـص اشكـال مختلـف اثـر انگشـت اسـت. ابعـاد Feature ها توسط الگوريتم SFFS )Sequential Forward Floating Selection( كاهش داده مي شود، سپس دو دسته ويژگي مستقل روي  طبقه بندي مختلف تست مي‌شود نظير :  AddBoost.ML , SVM , K-nearest Neighbor، ... سپس همه طبقه‌ٍبند هاي ذكر شده توسط الگوريتم Majority Voting Rule به فرم يك طبقهٍ‌بندي كننده تركيبي در مي آيند. استفاده از اين روش ساده و بدون نياز به هيچ گونه سخت افزار اضافي است.



**‌استفاده از آناليز خطوط برآمدگي انگشت توسط نورهاي تابيده شده**  
اين روش بر پايه تشخيص مشخصه هاي نوري از سطح اثر انگشت (پوست) است، ايده اصلي روش فوق بر اساس جابجا شدن خطوط Papillary Line است.



**‌استفاده از آناليز Time-Series**  
در اين روش از تكنيكي جديد جهت تشخيص زنده بودن اثر انگشت استفاده شده است به اين صورت كه كاربر انگشت خود را روي سطح اسكنر فشار داده و سپس در يك ســري زمـانـي مشخـص تصـاويـري از وي ثبـت مي‌شود. 5 ويژگي از تصاوير استخراج مي‌شود كه دو ويژگي آن نشان دهنده الاستيسيته پوست اسـت. در نـهايت توسط روش SVM() انگشت سالم از ساير مواد ژلاتيني تفكيك داده مي شود.

**‌استفاده از آناليز هاي فركانسي**يكي ديگر از روش هاي Liveness Detection اسـتـفـاده از آنـالـيـز هـاي فـركـانسي است. طيف فركانسي در لبه ها وشيار هاي اثر انگشت واقعي و غير واقعي متفاوت است. اثر انگشت زنده و جعلي هر دو طيف هايي را توليد مي كنند  اما اين طـيــف هــاي فــركــانـســي در دامـنـه و بـانـد هـاي فـركـانسـي مختلـف متفـاوتنـد، در حـالت عادي انگشـت زنده طيف فوريه قوي تري نسبت به انگشت جعلي دارد. استفاده از اين روش نتايج اميدواركننده اي را در تشخيص حالات زنده و جعلي اثر انگشت داشته است.

**‌تشخيص بر پايه مدل فيلتر گبور**يكي ديگر از روش هاي تشخيص اثر انگشت واقعي از جعلي است . اين روش بر اين تكنيك تكيـه دارد كه اثر انگشت هاي واقعي و جعلي داراي Texture هــــــاي مـــتـــفــــــاوتـــــي هــســتــنـــــد. اندازه‌گيري اين Texture بر پايه انرژي گبور و مشخصه هاي co-occurrence texture  هستند، فـيـلـتر هاي استفاده شده بانك گبور چهارتايي هـــــســــتــــنــــــــد.تــــــــوســــــــط روش gray level co-occurrence matrix ) GLCM) جـــــزئـــيــــات minute اسـتـخـراج مي شوند. ابعاد اين مشخصه ها نيز تـوسط آناليز PCA كاهش داده  هستند. در اين روش از سه تكنيك : neural network, support vector ma- chine and OneR و تركيب آن ها توسط Max Rule جــهـــت طـبـقــه‌ٍبـنــدي كــردن داده هــا استفاده شده و به فرم طبقه‌ٍبندي كننده هيبريد درآمده اند.

**‌تشخيص توسط آناليز بويايي**در اين روش تشخيص بر مبناي آناليز بوي انگشت است ، به اين صورت كه ضمن ثبت اثر انگشت بوي آن نيز توسط سنسور هاي بويايي (electronic nose) ثبت مي شود. در اين روش به راحتي مي توان بين اثر انگشت هاي جعلي شامل ژلاتيني ، سيليكني ، لاستيكي و ... و اثر انگشت واقعي تفكيك داد.

**‌تشخيص بر پايه آناليز اعوجاج سطح پوست**  
اين روش بر اساس آناليز الاستيسيته سطح پوست  است، كاربر انگشت خود را روي سطـح سنسـور حـركـت داده و اطـلاعات از سنسورها ثبت شده و توسط آناليز هاي مختلفي اعوجاج سطح پوست سنجيده مي شود. در طول جابجايي انگشت روي سطح سنسور عمليات ثبت و پردازش نيز انجام مي شوند. اين اطلاعات انكد شده و پس از آناليز مجدد  اثر انگشت طبيعي تعيين مي شود.  
اين روش ها همچنان در حال پيشرفت و توسعه هستند و تمام تلاش ها براي افزايش امنيت سيستم هاي بيومتريك است.

**‌ويژگي هاي استاتيك چند گانه**  
در اين  روش از ويژگي هاي جديدي در تصاوير اثر انگشت استفاده شده است ، اين ويژگي تحت عنوان روزنه هاي منحصر به فرد بوده و براي هر فرد متفاوت هستند. با بـررسـي فيـزيـولـوژيـك و مشخصه هاي آماري اين روزنه ها مي توان تفاوت بين اثر انگشت‌هاي جعلي و واقعي را تشخيص داد. تصاوير ثبت شده در اين روش بايد داراي كيفيت بالايي باشند.  
لازم به ذكر است كه اين پروژه در دانشكده مهندسي پزشكي واحد علوم و تحقيقات تهران و در مقطع كارشناسي ارشد در حال بهينه سازي و بهبود روش هاي تشخيص جعلي بودن اثر انگشت است.  
با تشكر از جناب دكتر معقولي  كه در تكميل ايده اين پروژه راهنمايي و همكاري داشته اند.

دستگاه اسکنر اثر انگشت همستر با سنسور ضد خش و ضد خرابکاری و جعل با بهترین طراحی و با بهره گیری از جدیدترین تکنولوژی سیستم های Biometric ساخت شرکت NITGEN کره جنوبی است. این دستگاه دارای استحکام فوق العاده در برابر ضربه های فیزیکی و شوک الکتریکی است.

hamster1.jpg  
**قابلیتهای سیستم تشخیص اثر انگشت: (Hamster)**   
تغییر ناپذیری : روشن کردن کامپیوتر از طریق شناسایی اثر انگشت کاربر.   
ایمن کردن فایلها : ایمن کردن فایلهای محرمانه و ارتقا امنیت برنامه ها   
کنترل کردن : گزارشگیری از عملکرد کاربران سیستم   
غیر قابل نفوذ : غیر قابل رمزگشایی ، فقط با اثر انگشت کاربر اصلی .   
ارتقا عملکرد سیستم : تبدیل رمز Screen saver به سیستم شناسایی اثر انگشت  
موارد اضطراری : قابلیت تعریف کردن رمز برای استفاده در موارد ضروری  
از این سیستم میتوان برای شناسایی افراد از طریق شبکه و از راه دور در برنامه های مورد نظر استفاده کرد .   
رابط نرم افزاری رایگان  
قابلیت اتصال به تمامی سنسورهای موجود  
پشتیبانی از تمامی زبانهای برنامه نویسی  
پشتیبانی از تمامی سیستم های عامل  
دارنده تمامی استانداردهای جهانی مرتبط  
  
موارد کاربرد :   
امنیت برای کامپیوتر و شبکه  
تجارت الکترونیک  
ایجاد امنیت برای بانکها و موسسه های مالی برای شناسایی کاربر  
سیستم اطلاعات پزشکی  
کارهایی که در آن نیاز به شناسایی کاربر است  
قابلیت برنامه نویسی جهت استفاده از این دستگاه با سیستم های سخت افزاری و نر م افزاری مختلف  
  
مزایای سیستم تشخیص اثر انگشت (Hamster) :   
تغییر ناپذیری : نقشهای اثر انگشت تغییر ناپذیر است .   
منحصر به فردی: نقش اثر انگشت هر شخص منحصر به فرد است .   
راحت بودن : نیازی به داشتن آگاهی خاص برای استفاده کردن ندارد .   
قابل اعتماد :اعتبار امنیت سیستم را ارتقا میدهد .   
عمومیت : عمومیترین تکنولوژی بیومتریک است که پذیرفته شده است .   
قابل دسترس : در دسترس ترین سیستم بیومتریک .   
  
سیستم همستر از تکنولوژی اسکن نوری و سه بعدی بهره میگیرد ، این نوع اسکن بهترین شیوه تشخیص اثر انگشت میباشد و میزان دقت آن بسیار بیشتر از سیستم خازنی شناسایی اثر انگشت است .

**منابع**

[1] A. Maltoni, D. Maio, A.K. Jain, S. Prabhakar, Handbook of  Fingerprint  Recognition, Springer, New York, 2003, ISBN 0-387-95431-7.  
[2] T. Putte, J. Keuning, "Biometrical Fingerprint Recognition: Don't Get Your Finger Burned", Proceedings of 4th Working Conference on Smart Card Research and Advanced Applications, ACM, Bristol, UK, 2002, pp. 289-303, ISBN 0-7923-7953-5.  
[3] S. Shuckers, L. Hornak, T. Norman, R. Derakhshani, S. Parthnasardi, "Issues for Liveness Detection in Biometrics", CEMR LDCSEE, West Virginia University, USA, 2006, p. 25.  
[4] M. Kluz, "Liveness Testing in Biometric Systems", Master thesis, Brno, Masaryk University, Faculty of Informatics, Brno, CZ, 2005, p. 57.  
[5] A. Franco and D. Maltoni, "Fingerprint Synthesis and Spoof Detection", in N.K. Ratha, V. Govindaraju, Advances in Biometrics: Sensors, Algorithms and Systems, Springer, 2008  
 [6] A. Antonelli, R. Cappelli, D. Maio and D. Maltoni, "Fake Finger Detection by Skin Distortion Analysis", IEEE Transactions on Information Forensics and Security, vol.1, no.3, pp.360-373, September 2006  
 [7] J. Galbally, R. Cappelli, A. Lumini, G Gonzalez-de-Rivera, D. Maltoni, J. Fierrez-Aguilar, J. Ortega-Garcia and D. Maio, "An Evaluation of Direct Attacks Using Fake Fingers Generated from ISO Templates", to appear on Pattern Recognition Letters Special issue on ICPR08  
[8] Shankar Bhausaheb Nikam and Suneeta Agarwal , " Gabor Filter-Based Fingerprint Anti-spoofing " , J. Blanc-Talon et al. (Eds.): ACIVS 2008, LNCS 5259, pp. 1103-1114, 2008. © Springer-Verlag Berlin Heidelberg 2008  
[9]  K.-H. Nam and G. Rhee ," A Novel Region Based Liveness Detection Approach for Fingerprint Scanners "(Eds.): ICISC 2007, LNCS 4817, pp. 168-179, 2007. © Springer-Verlag Berlin Heidelberg 2007  
[10]  Brian DeCann, Bozhao Tan, and Stephanie Schuckers , " A Novel Region Based Liveness Detection Approach for Fingerprint Scanners ", M. Tistarelli and M.S. Nixon (Eds.): ICB 2009, LNCS 5558, pp. 627-636, 2009.c Springer-Verlag Berlin Heidelberg 2009  
[11]  Y.S. Moon, J.S. Chen, K.C. Chan, K. So and K.C. Woo , "Wavelet based ?ngerprint liveness detection" ELECTRONICS LETTERS 29th September 2005 Vol. 41 No. 20  
[12]  Denis Baldisserra, Annalisa Franco, Dario Maio, and Davide Maltoni و Fake Fingerprint Detection by Odor Analysis , D. Zhang and A.K. Jain (Eds.): ICB 2006, LNCS 3832, pp. 265 - 272, 2005. © Springer-Verlag Berlin Heidelberg 2005  
[13] Heeseung Choi, Raechoong Kang, Kyungtaek Choi, and Jaihie Kim , " Aliveness Detection of Fingerprints using