چهارمین کنفرانس ملی ایده های نو در مهندسی برق
۲۰و۲۱ آبان ماه ۱۳۹۴ - دانشگاه آزاد اسلامی واحد اصفهان (خوراسگان)

سیستم‌های تشخیص اثرانگشت

فریده براز[۱]، احمد فراهی[۲]
[۱]دانشجوی کارشناسی ارشد دانشگاه پیام نور، farideh.baraz@gmail.com
[۲]استادیار دانشگاه پیام نور، afaraahi@pnu.ac.ir

چکیده-اثر انگشت یکی از بیومتریک‌های رایج در شناسایی و تایید هویت فردی محسوب می‌شود. سیستم‌ها و روش‌های تشخیص اثر انگشت متعددی در این زمینه پیشنهاد شده‌اند که در این مقاله چند سیستم طراحی شده جدید مرور و بررسی می‌شوند. این سیستم‌ها معیار بررسی عملکرد روش خود را نرخ خطای برابر *(EER)* در نظر گرفته‌اند و آن را روی پایگاه داده عمومی *FVC* آزمایش کرده‌اند. نتایج مقایسه این روش‌ها از نظر پایگاه داده و نوع سنسور بیان شده‌است.

کلید واژه- بیومتریک، اثر انگشت، ثبت نام، تصدیق، نرخ خطای برابر

۱- مقدمه

توسعه جامعه باعث افزایش تقاضا جهت امنیت اطلاعات می‌شود . برای رسیدن به چنین امنیتی، پیشرفت تکنولوژی ایجاب می‌کند گرایش اصلی به سمت تایید و تصدیق شخصی باشد که بر مبنای ویژگی‌های رفتاری یا فیزیولوژیکی انسان است. چنین روش‌هایی شامل تشخیص صورت، اثر انگشت، بند انگشت، گوش و قدم زدن است [1]. اثر انگشت به صورت گسترده‌ای در تشخیص فرد استفاده می‌شود ، بیشتر به این سبب که از خصوصیات ثابت بیولوژیکی انسان است، همچنین جزئیات بیشتری برای تشخیص افراد متفاوت فراهم می‌کند[2].

تشخیص بیومتریک شامل دو مرحله است (الف) ثبت نام : استخراج ویژگی‌ها از داده‌های پویش شده از بیومتریک کاربر، ایجاد الگو و ذخیره در پایگاه داده و (ب) تصدیق : استخراج همان ویژگی‌ها از داده بیومتریک درخواستی کاربر و مقایسه نتایج با الگوی ذخیره شده [3]. یکبار که شخص فرایند ثبت نام را انجام داد می‌تواند توسط نمونه موجود در سیستم تایید (تشخیص یک فرد از میان یک مجموعه بزرگ از رکوردهای بیومتریک، یعنی تطبیق یک به چند) شود یا تصدیق (یک نمونه بیومتریک زنده که توسط یک شخص ارائه شده با یک نمونه ذخیره شده مقایسه شود یعنی تطبیق یک به یک) شود. نمونه ارائه شده با نمونه ذخیره شده مقایسه می‌شود اگر فرایند تطبیق موفق باشد فرد تشخیص داده می‌شود و سیستم او را می‌پذیرد در غیر اینصورت شخص رد می‌شود. نمونه ارائه شده (واقعی) ممکن است با نمونه ذخیره شده مغایرت‌هایی داشته باشد که می‌تواند مقایسه، تطبیق و تایید را به یک فرایند نادقیق تبدیل کند، یعنی سیستم بیومتریک دارای صحت ۱۰۰٪ نیست[4] .

یکی از رایج‌ترین بیومتریک‌ها اثر انگشت است کع در زمینه-های قانونی، قضایی و جرم شناسی کاربرد فراوان دارد. یک اثرانگشت عبارت است از لبه‌ها و شیارها که اطلاعات زیادی از ویژگی‌های برجسته برای گروه وسیعی از کاربران حمل می کنند. دو ویژگی از لبه‌های محلی،یعنی لبه پایانی و لبه شاخه‌ای باهم به عنوان minutia شناخته می‌شوند.

سه شاخص برای ارزیابی عملکرد وجود دارد اول نرخ رد نادرست یعنی FRR، که به صورت نسبت تلاش‌های درست ناموفق به کل تلاشهای درست تعریف می شود ، دوم نرخ پذیرش نادرست یعنی FAR، که به صورت نسبت تلاش‌های غاصبانه موفق به کل تلاش‌های غاصبانه تعریف می‌شود و سوم نرخ خطای برابر یعنی EER، نرخ خطا وقتی که FRR و FAR برابر هستند [5].

تا کنون مطالعات متعددی در زمینه شناسایی اثر انگشت انجام شده است، برای نمونه Wenxiong Kang و همکاران [1]

یک سیستم بیومتریک چند کیفیتی نوین بر مبنای طیف غیرمماس اثر انگشت ارایه داده‌اند که ادعا شده با استخراج سه ویژگی اثر انگشت، بند انگشت و رگه‌های انگشت به جای استخراج تنها یک ویژگی بر محدودیت‌های بیومتریک تک کیفیتی فایق آمده است. پایگاه داده مورد آزمایش در این روش توسط نویسندگان گرفته شده است. Daniel Peralta و همکاران [6] یک روش استخراج minutiae استفاده کرده‌اند که اثر و بازدهی الگوریتم تطبیق اثر انگشت را بهبود می‌بخشد. در این روش نتایج آزمایش را روی پایگاه داده‌های FVC و یک پایگاه داده که توسط نویسندگان گرفته‌شده مقایسه کرده‌اند که ادعا شده به صحت تشخیص بالایی رسیده‌اند.

مطالعات دیگری در این زمینه انجام شده که روش خود را روی پایگاه داده عمومی مثل FVC آزمایش کرده‌اند. Jing-Ming Guo و همکاران [2] یک روش دسته‌بندی بر مبنای اثر انگشت ارائه و نتایج آزمایش روش خود را روی پایگاه داده FVC2000 (شامل DB1،DB2 وDB4)، FVC2002 (شامل DB1، DB2وDB4) و FVC2004 (شامل DB1، DB2وDB4) مشخص نموده‌اند. در این روش معیار ارزیابی نرخ دسته‌بندی درست (CER) و نرخ استخراج درست (CCR) است. Priyanka Das و همکاران [3] یک الگوریتم درهم اثر انگشت بدون تنظیم بر اساس گراف فاصله حداقل ارایه داده‌اند که روش خود را روی پایگاه داده FVC2002-DB1 و FVC2002DB2 آزمایش کرده و نتایج آزمایش را با معیار نرخ خطای برابر و میزان امنیت، با روش‌های مشابه مقایسه کرده‌اند.

معیارهای ارزیابی متفاوت و پایگاه داده‌های متنوع در این مطالعات بررسی و مقایسه آنها را مشکل کرده‌است، بنابراین مواردی جهت بررسی انتخاب شده‌اند که دارای اشتراک معیار بررسی باشند و از همه مهم‌تر پایگاه داده عمومی، استاندارد و شناخته شده‌ای را برای آزمایش روش خود انتخاب کرده باشند.

در ادامه پایگاه داده FVC در بخش ۲ معرفی می‌شود و در بخش ۳ سیستم‌های تشخیص اثر انگشت به طور خلاصه شرح داده می‌شوند. بررسی و مقایسه این روش‌ها در بخش ۴ بیان می‌شود. نتیجه گیری در بخش ۵ آمده است.

۲- معرفی پایگاه داده FVC

این پایگاه داده شامل چهار مجموعه پایگاه داده به نام‌های FVC2000, FVC2002, FVC2004 و FVC2006 است که در ادامه به طور خلاصه معرفی می‌شوند.

۲-۱- پایگاه داده FVC2000

FVC2000 اولین رقابت بین‌المللی برای الگوریتم‌های تایید اثر انگشت است. اولین جلسه ارزیابی اوت ۲۰۰۰ بود و نتایج یازده شرکت‌کننده در پانزدهمین کنفرانس بین‌المللی تشخیص الگو (ICPR) ارایه شد. این پایگاه داده شامل چهار پایگاه داده DB1, DB2, DB3 و DB4 است که توسط روش‌ها و یا سنسورهای متفاوت جمع آوری شده‌اند [8] که در جدول (۱) به طور خلاصه آمده است.

جدول (۱) : پایگاه داده FVC2000 [8]

	نوع سنسور	اندازه تصویر	تفکیک‌پذیری
DB1	سنسور نوری کم هزینه	۳۰۰×۳۰۰	۵۰۰ Dpi
DB2	سنسور خازنی کم هزینه	۲۵۶×۳۶۴	۵۰۰ Dpi
DB3	سنسور نوری	۴۴۸×۴۷۸	۵۰۰ Dpi
DB4	مولد مصنوعی	۲۴۰×۳۲۰	حدود ۵۰۰ Dpi

هر کدام از چهار پایگاه داده دارای دو زیرمجموعه A و B است. مجموعه A شامل ۱۰۰ اثر انگشت است که از هر اثر انگشت ۸ اثر موجود است، یعنی در کل ۸۰۰ اثر انگشت در این مجموعه وجود دارد. مجموعه B شامل ۱۰ اثر انگشت است که از هر کدام ۸ اثر موجود است، بنابراین در مجموع ۸۰ اثر انگشت وجود دارد . مجموعه B در اختیار شرکت‌کنندگان قرار می‌گیرد تا قبل از واگذاری الگوریتم، پارامترها را میزان‌سازی کنند و مجموعه A معیار است [8]. این در مورد مجموعه‌های پایگاه داده FVC2002 و FVC2004 نیز صادق است.

۲-۲- پایگاه داده FVC2002

FVC2002 دومین رقابت بین‌المللی برای الگوریتم‌های تایید اثر انگشت است. ارزیابی آن در آوریل ۲۰۰۲ بود و نتایج ۳۱ شرکت کننده در شانزدهمین کنفرانس بین‌المللی تشخیص الگو (ICPR)

ارایه شد. این پایگاه داده شامل چهار پایگاه داده DB3, DB2, DB1 و DB4 است که توسط روش‌ها و یا سنسورهای مختلف جمع‌آوری شده‌اند [9]. در جدول(۲) خلاصه آن بیان شده است.

جدول (۲) : پایگاه داده FVC2002 [9]

	نوع سنسور	اندازه تصویر	تفکیک‌پذیری
DB1	سنسور نوری	۳۸۸×۳۷۴	۵۰۰ Dpi
DB2	سنسور نوری	۲۹۶×۵۶۰	۵۶۹ Dpi
DB3	سنسور خازنی	۳۰۰×۳۰۰	۵۰۰ Dpi
DB4	تولید توسط SFinGe v2.51	۲۸۸×۳۸۴	حدود ۵۰۰ Dpi

۲-۳- پایگاه داده FVC2004

FVC2004 سومین رقابت بین‌المللی تایید اثر انگشت است. این پایگاه داده شامل چهار پایگاه داده DB3, DB2, DB1 و DB4 است که توسط روش‌ها و یا سنسورهای متنوع جمع‌آوری شده‌اند [10] که جدول(۳) خلاصه آن است.

جدول (۳) : پایگاه داده FVC2004 [10]

	نوع سنسور	اندازه تصویر	تفکیک‌پذیری
DB1	سنسور نوری	۶۴۰×۴۸۰	۵۰۰ Dpi
DB2	سنسور نوری	۳۲۸×۳۶۴	۵۰۰ Dpi
DB3	سنسور جاروبی حرارتی	۳۰۰×۴۸۰	۵۱۲ Dpi
DB4	تولید توسط SFinGe v3.0	۲۸۸×۳۸۴	حدود ۵۰۰ Dpi

پایگاه داده FVC2004 به صورت کاملا مشخصی سخت‌تر از FVC2000 و FVC2002 است که علت آن اختلال عمدی مطرح شده است. بنابراین نبایستی کسی بین FVCها مقایسه انجام دهد و یا نتیجه بگیرد که شاهکارهای تطبیق اثر انگشت پیشرفت نمی‌کنند و قابل بهبود نیستند[10].

۲-۴- پایگاه داده FVC2006

چهارمین رقابت بین‌المللی تایید اثر انگشت است. این رقابت روی ارزیابی نرم افزارهای تایید اثر انگشت متمرکز شده است. پایگاه داده FVC2006 چهار پایگاه داده DB3, DB2, DB1 و DB4 دارد که توسط روش‌ها و یا سنسورهای مختلف جمع‌آوری شده‌اند [11] که در جدول (۴) بیان شده است.

جدول (۴) : پایگاه داده FVC2006 [11]

	نوع سنسور	اندازه تصویر	تفکیک‌پذیری
DB1	سنسور میدان الکتریکی	۹۶×۹۶	۵۰۰ Dpi
DB2	سنسور نوری	۴۰۰×۵۶۰	۵۰۰ Dpi
DB3	سنسور جاروبی حرارتی	۴۰۰×۵۰۰	۵۰۰ Dpi
DB4	تولید توسط SFinGe v3.0	۲۸۸×۳۸۴	حدود ۵۰۰ Dpi

هر کدام از چهار پایگاه داده FVC2006 دارای دو زیرمجموعه A و B است. مجموعه A شامل ۱۴۰ اثر انگشت است که از هر اثر انگشت ۱۲ اثر موجود است، یعنی ۱۶۸۰ اثر انگشت در کل وجود دارد. مجموعه B شامل ۱۰ اثر انگشت است که از هر کدام ۱۲ اثر وجود دارد یعنی در مجموع شامل ۱۲۰ اثر انگشت است. مجموعه B در اختیار شرکت‌کنندگان قرار می‌گیرد تا قبل از واگذاری الگوریتم، پارامترها را میزان‌سازی کنند و مجموعه A معیار است [11].

SFinGe یک روش جدید برای تولید تصویر اثر انگشت مصنوعی است. در آزمایش یک الگوریتم تشخیص اثر انگشت، به این دلیل که خطاهای کوچک باید تخمین زده شوند به پایگاه داده بزرگی از نمونه‌ها نیاز است، اما جمع‌آوری پایگاه داده بزرگی از اثر انگشت کار پرهزینه، خسته‌کننده و حساسی است. SFinGe می تواند برای ایجاد پایگاه داده اثر انگشت با هزینه صفر، استفاده شود [12].

۳- معرفی سیستم‌های تشخیص اثر انگشت

سیستم‌های تشخیص اثر انگشت که در ادامه شرح داده می‌شوند روش خود را روی پایگاه داده FVC آزمایش و صحت عملکرد را با معیار نرخ خطای برابر بیان کرده‌اند.

در سیستم فیلترگذاری طیفی [7] که به طور خلاصه در مقاله آن را ABSF نامیده‌اند، یک فیلتر منطبق با گوس روی تصویر اثر انگشت اعمال می‌کند. از مناطق با کیفیت بالا شروع کرده و پی در پی طیف خوبی از لبه‌های بالا به سمت مناطق کیفیت پایین منتشر می‌کند. این الگوریتم منطقه تک‌نقطه ای را بالا می‌برد و در کل مناطق با کیفیت خیلی پایین را بهبود می‌بخشد. روش فیلترگذاری minutia [6] از یک استخراج‌گر minutia به نام MINDTCT استفاده کرده است که فیلترهای

قشر کوژ[ ] و قطعه‌بندی[ ] را به کار برده است. فیلتر قطعه‌بندی روی پایگاه داده FVC در تمام حالات نتایج بهتری نسبت قشر کوژ ارائه کرده است.

سیستم مخفی بیومتریک اثر انگشت غیر همتراز [5] از ساختار همسایگی Voronoi[ ] (VNS) استفاده می‌کند. در این روش سعی شده‌است با استفاده از VNS با وجود احتمال اعوجاج و چرخش طی فرایند گرفتن اثر انگشت امنیت قوی فراهم کرده و به نرخ خوبی در تشخیص برسد. الگوریتم درهم اثر انگشت غیر همتراز بر مبنای گراف فاصله حداقل [3] دو الگوریتم MDG_CSA2A و MDG_CSA2B را معرفی کرده که عملکرد MDG_CSA2B بهتر است. چالش اصلی در انتخاب درست ویژگی‌ها این است که در تحریف‌هایی مثل چرخش، تبدیل و درج و حذف minutia ثابت بماند. در این روش بردارهای فاصله حداقل میان minutiaها از نقطه هسته، به عنوان مجموعه ویژگی‌ها استفاده می‌شود که گراف فاصله حداقل نامیده می‌شود. این روش امنیت و نرخ خطای برابر خوبی بدست آورده است درحالی که هزینه محاسبات و فرایندهای تطبیق پایین است.

۴- بررسی سیستم‌های تشخیص اثر انگشت

در جدول (۵) خلاصه عملکرد سیستم‌های تشخیص هویت با معیار EER بیان شده است. همانطور که مشاهده می‌شود، روش ABSF تمام پایگاه داده‌های FVC غیر از FVC2006DB1 را مورد آزمایش قرار داده‌است، نویسندگان علت آن را تفکیک-پذیری خیلی پایین (۲۵۰dpi) و اندازه بسیار کوچک (۹۶×۹۶ پیکسل) [7] تصاویر این پایگاه داده اعلام کرده‌اند. این روش با دیگر روش‌ها در پایگاه داده مورد آزمایش، اشتراک دارد. نرخ خطای برابر آزمایش روش MINDTCT روی پایگاه داده FVC2002DB1 کمتر از سایر روش‌ها است و این نشان می‌دهد عملکرد بهتری نسبت به سایر روش‌ها روی این پایگاه داده دارد. نرخ خطای برابر روش ABSF روی پایگاه داده FVC2002DB2 کمتر از سایر روش‌ها است. عملکرد ABSF روی پایگاه داده‌های FVC2000DB1 و FVC2004DB2 از دو روش MINDTCT و VNS بهتر بوده است.

جدول (۵) : مقایسه نرخ خطای برابر(EER) روش‌های تشخیص اثر انگشت (برحسب درصد)

	ABSF	MINDTCT	VNS	MDG	نوع سنسور و اندازه تصویر
FVC2000DB1	۳/۰۹	۳/۲۹۲۲	۱۴/۳۰	–	سنسور نوری کم هزینه ۳۰۰×۳۰۰ Secure Desktop Scanner
FVC2000DB2	۱/۲۳	۲/۵۷۶۵	–	–	سنسور خازنی کم هزینه ۲۵۶×۳۶۴ Touch Chip
FVC2000DB3	۴/۲۷	–	–	–	سنسور نوری ۴۷۸×۴۴۸ DF-90
FVC2000DB4	۴/۰۴	–	–	–	تولیدکننده مصنوعی ۳۲۰×۲۴۰
FVC2002DB1	۲/۰۷	۰/۸۱۱۰	۱۱/۸۴	۲/۲۷	سنسور نوری ۳۷۴×۳۸۸ Touch View II
FVC2002DB2	۰/۸۸	۶/۶۱۱۱	۱۰/۳۸	۳/۷۹	سنسور نوری ۵۶۰×۲۹۶ FX2000
FVC2002DB3	۶/۳۲	–	۱۶/۵۲	–	سنسور خازنی ۳۰۰×۳۰۰ 100SC
FVC2002DB4	۱/۵۳	–	۱۵/۶۳	–	تولید مصنوعی ۳۸۴×۲۸۸ توسط SFinGE v2.51
FVC2004DB1	۵/۶۵	۷/۰۳۹	–	–	سنسور نوری ۴۸۰×۶۴۰ V300
FVC2004DB2	۵/۴۶	۸/۳۶۲۹	۲۰/۶۱	–	سنسور نوری ۳۶۴×۳۲۸ U.are.U400
FVC2004DB3	۲/۵۴	–	–	–	سنسور جاروبی حرارتی ۴۸۰×۳۰۰ Fingerchip FCD4B14CB
FVC2004DB4	۲/۵۹	–	–	–	تولید مصنوعی ۳۸۴×۲۸۸ توسط SFinGe v3.0
FVC2006DB1	–	–	–	–	سنسور میدان الکتریکی ۹۶×۹۶
FVC2006DB2	۰/۲۵	–	–	–	سنسور نوری ۵۶۰×۴۰۰
FVC2006DB3	۳/۷۵	–	–	–	سنسور جاروبی حرارتی ۵۰۰×۴۰۰
FVC2006DB4	۱/۹۴	–	–	–	تولید مصنوعی ۳۸۴×۲۸۸ توسط SFinGe v3.0

همانطور که بالاتر گفته شد پایگاه داده‌های مختلف توسط روش‌ها و سنسورهای متفاوتی جمع‌آوری شده‌اند. خلاصه بررسی عملکرد سیستم‌های تشخیص الگو از نظر سنسور مورد استفاده در جمع آوری پایگاه داده، در جدول (۶) تنظیم شده است. در این جدول سیستم‌های مورد بررسی به ترتیب کمترین نرخ

خطای برابر یعنی بهترین عملکرد تا بیشترین نرخ خطای برابر در ستون مربوط به هر سنسور قرار داده شده‌اند. روش ABSF در بیشتر موارد بهترین عملکرد را داشته است. MINDTCT بهترین عملکرد را با سنسور Touch View II داشته و پس از آن ABSF بهترین عملکرد بعدی را نشان داده است.

جدول (۶) : روش‌های تشخیص الگو از نظر سنسور به ترتیب کمترین نرخ خطای برابر (برحسب درصد)

سنسور کم هزینه	سنسور خازنی کم هزینه	سنسور نوری Touch View II	سنسور نوری FX2000	سنسور نوری V300	سنسور نوری U.are.U4000	تولید مصنوعی
ABSF	ABSF	MINDTCT	ABSF	ABSF	ABSF	ABSF
MINDTCT	MINDTCT	ABSF	MDG	MINDTCT	MINDTCT	VNS
VNS		MDG	MINDTCT		VNS	
		VNS	VNS			

۵- نتیجه

آنچه از مطالب حاضر برآورد می‌شود نشان می‌دهد سیستم ABSF از نظر نرخ خطای برابر بهتر عمل کرده است. این سیستم روی ۱۵ پایگاه داده FVC روش خود را آزمایش کرده و درنتیجه بهتر می توان درباره آن نظر داد. سیستم‌های MINDTCT و MDG روی تعداد محدودی پایگاه داده آزمایش شده‌اند و عملکرد آنها تنها در همان پایگاه داده‌ها مورد بررسی قرار گرفته است، بنابراین نمی توان به طور قطعی عملکرد آنها را ارزیابی کرد.

درمورد سیستم VNS، باید گفت، این سیستم از اساس برای تشخیص اثر انگشت با امنیت و قدرت در برابر اختلال تصویر اثر انگشت طراحی شده است؛ به گفته نویسندگان از نظر تشخیص عملکرد خوبی داشته اما از نظر امنیت عملکرد بهتری نشان داده است.

امنیت و محرمانه بودن داده‌های کاربران، دغدغه سیستم-های بیومتریک امروزی است. بیشتر توجه روی حفاظت الگوی بیومتریک است تا از سرقت آن طی ارتباط و اتصال جلوگیری شود. بیورمزنویسی یک شیوه امنیت جدید است که رمز نویسی را با بیومتریک ترکیب می کند. بیورمزنویسی اثر انگشت می تواند زمینه خوبی برای پژوهش‌های جدید باشد.

مراجع

[1] Wenxiong Kang, Xiaopeng Chen, Qiuxia Wu, “The biometric recognition on contactless multi-spectrum finger images”, Infrared Physics & Technology, Vol. 68, pp. 19-27, 2015.

[2] Jing-Ming Guo, Yun-Fu Liu, Jla Chang, Jiann-Der Lee, "Fingerprint classification based on decision tree from singular points and orientation", Expert System with Application, Vol. 41, pp. 752-764, 2014.

[3] Priyanka Das, Kannan Karthik, Boul Chandra Garai, "A robust alignment-free fingerprint hashing algorithm based on minimum distance graphs", Pattern Recognition, Vol. 45, pp. 3373-3388, 2012.

[4] M.A. Murillo-Escobar, C. Cruz-Hernández, F. Abundiz-Pérez, R.M. López-Gutiérrez, "A robust embedded biometric authentication system based on fingerprint and chaotic encryption", Expert Systems with Application, Vol. 42, pp. 8198-8211, 2015.

[5] Wencheng Yang, Jiankun Hu, Song Wang, Milos Stojmenovic, "An alignment-free bio-cryptosystem based on modified Voroni neighbor structures", Pattern Recognition, Vol. 47, pp. 1309-1320, 2014.

[6] Daniel Peralta, Mikel Galar, Isaac Triguero, Oscar Miguel-Hurtado, Jose M.Benitez, Francisco Herrera, "Minutiae filtering to improve both efficacy and efficiency of fingerprint matching algorithms", Engineering Applications of Artificial Intelligence, Vol. 32, pp. 37-53, 2014.

[7] Prawit Sutthiwichaiporn, Vutipong Areekul, "Adaptive boosted spectral filtering for progressive fingerprint enhancement", Pattern Recognition, Vol. 46, pp. 2465-2486, 2013.

[8] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, A. K. Jain, The 1st Fingerprint Verification Competition, August 2000, http://bias.csr.unibo.it/fvc2000/

[9] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, A. K. Jain, The 2nd Fingerprint Verification Competition, April 2002, http://bias.csr.unibo.it/fvc2002/

[10] The Biometric System Laboratory, Pattern Recognition and Image Processing Laboratory, Biometric Test Center, Biometrics Research Lab - ATVS, The 3rd Fingerprint Verification Competition, http://bias.csr.unibo.it/fvc2004/

[11] The Biometric System Laboratory, Pattern Recognition and Image Processing Laboratory, Biometric Test Center, Biometrics Research Lab - ATVS, The 4th Fingerprint Verification Competition, http://bias.csr.unibo.it/fvc2006/

[12] Biometric System Laboratory, Synthetic Fingerprint Generator, http://www.biolab.csr.unibo.it

- Enrollment
- Authentication
- ridge
- valley
- ending
- bifurcation
- False Reject Rate
- False Accept Rate
- Equal Error Rate
- Fingerprint Verification Competition
- Correct Extraction Rate
- Correct Classification Rate
- International Conference on Pattern Recognition
- Synthetic Fingerprint Generator
- Convex Hull
- Segmentation
- Voronoi Neighbor Structure
- Security
- secrecy
- Bio-cryptography
- cryptography