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

سیستم‌های حفاظت الگوی اثرانگشت

فریده براز[۱]، بیتا امیرشاهی[۲]
[۱] دانشجوی کارشناسی ارشد دانشگاه پیام نور، farideh.baraz@gmail.com
[۲] استادیار دانشگاه پیام نور، Bita.amirshahi@gmail.com

چکیده - تشخیص اثرانگشت یک راه حل مطمئن در سیستم‌های تشخیص هویت است. با این وجود، امنیت و محرمانگی داده‌های کاربران یک نگرانی در سیستم‌های بیومتریک محسوب می‌شود و بیشتر توجه امنیت روی حفاظت الگوی بیومتریک متمرکز است تا از سرقت هویت جلوگیری شود. در این مقاله چند سیستم حفاظت الگوی اثرانگشت جدید مورد مطالعه قرار گرفته‌اند. در این سیستم‌ها معیار بررسی عملکرد، نرخ خطای برابر *(EER)* است که روی پایگاه داده عمومی *FVC* مورد آزمایش قرار گرفته‌اند. این روش‌ها از نظر صحت عملکرد در دو سناریو اصلی و سناریو کلید سرقت شده مقایسه و بررسی شده‌اند.

کلید واژه- اثرانگشت ، حفاظت الگو، قابلیت لغو، بیورمزنویسی، تبدیل ویژگی

۱- مقدمه

یک بیومتریک تعیین کننده هویت، یک ویژگی فیزیولوژیکی یا رفتاری یک شخص است مثل ویژگی صورت، عنبیه، کف دست، شبکیه چشم، صدا، امضا دست‌نویس و اثر انگشت و غیره ، که همه منحصربفرد، غیرقابل جایگزینی، عمومی و قابل اندازه‌گیری هستند. به خاطر این ویژگی‌ها، بیومتریک‌ها در تشخیص و تایید کاربران در یک سیستم بیومتریک به کار می‌روند، که بیشتر از روش‌های سنتی تشخیص مثل کارت شناسایی (ID)، گذرواژه و شماره شناسایی (PIN) رایج شده‌اند. بیومتریک می‌تواند به صورت یک تصویر یا به صورت داده‌هایی که از نمونه استخراج شده‌اند، باشند. این داده‌ها تشکیل یک الگوی بیومتریک را می‌دهند[1]. یکی از رایج‌ترین بیومتریک‌ها اثرانگشت است که در زمینه های قانونی، قضایی و جرم شناسی کاربرد فراوان دارد.

یک اثرانگشت برمبنای بیومتریک برای تایید هویت کاربران حقیقی عموما به سه دلیل استفاده می‌شود: عمومیت، برجستگی و دائمی بودن. یک اثرانگشت عبارت است از لبه‌ها و شیارها که اطلاعات زیادی از ویژگی‌های برجسته برای گروه وسیعی از کاربران حمل می‌کنند. دو ویژگی از لبه‌های محلی با هم به عنوان minutia شناخته می‌شوند ،این ویژگی‌ها، لبه پایانی و لبه شاخه‌ای هستند [2].

سیستم‌های تشخیص اثر انگشت در زمینه امنیت مورد استفاده قرار می‌گیرند، اما خود از مسئله تامین امنیت رنج می‌برند. طوری که، امنیت و محرمانگی داده‌های کاربران در سیستم-های بیومتریک یک نگرانی است. در کل چهار نوع حمله در سیستم‌های نوع بیومتریک وجود دارد: (۱) حمله سنسور، (۲) حمله بین پیمانه‌ای، (۳) حمله نرم افزار، (۴) حمله علیه الگوهای ذخیره شده در پایگاه داده. آخرین نوع حمله در سیستم‌های بیومتریک خطرناک‌ترین آنها است، زیرا الگوهای بیومتریک می-توانند با یک بدل جایگزین شوند تا امنیت سیستم به خطر بیافتد. به علاوه کاربر خصیصه بیومتریک خود را برای همیشه گم خواهد کرد (سرقت هویت) و دوباره نمی‌تواند برای شناسایی از آن استفاده کند، یعنی کاربر مجاز نمی‌تواند دو ویژگی بیومتریک از همان خصیصه انگشت تولید کند. بنابراین در یک سسیستم بیومتریک، حفاظت از الگوی بیومتریک برای امنیت در سیستم بیومتریک و حفاظت بیومتریک شخصی، یک نیاز است [1].

به خاطر این چالش‌های امنیت، علاقه به طراحی، ساخت و پیاده‌سازی محافظت الگوی بیومتریک امن افزایش پیدا کرده است. چهار نیازمندی هنگام طراحی الگوریتم حفاظت الگو نیاز است [1,3,4,5]:

ابطال پذیری. توانایی الگوریتم برای لغو الگوی کشف شده و تولید یک الگوی جدید از همان ویژگی بیومتریک است.

- تنوع. الگوی بیومتریک امن نباید اجازه بدهد تطبیق دوطرفه در سراسر پایگاه داده صورت بگیرد؛ به عبارت دیگر اگر الگوی باطل شده با مدل جدیدی جایگزین شد نبایستی با قبلی مشابه باشد، بدینوسیله کاربر پنهان می‌ماند.
- امنیت. استخراج الگوی اصلی از الگوی محافظت شده باید از نظر محاسباتی بسیار سخت باشد. این محرمانگی الگوی بیومتریک کاربر را تضمین می‌کند.
- کارایی. الگوریتم حفاظت نباید در عملکرد تشخیص سیستم بیومتریک تاثیر بگذارد یعنی نیاز است که FRR و FAR قابل قبول باشند.

به این دلیل که جایگزینی یا لغو داده‌های بیومتریک بسیار سخت است، داده‌های بیومتریک کاربران، هنگامی که برای تایید هویت بکار می‌روند باید به روش امنی محافظت شوند. بنابراین به جای ذخیره داده خام بیومتریک در پایگاه داده ارجحیت دارد که نسخه تبدیل شده مرتبط با آن ذخیره شود به این صورت که (۱) هنوز بتواند با کارایی معقول برای تطبیق استفاده شود، (۲) جعل "اصل" داده بیومتریک که با یک الگوی داده شده تطبیق دارد، بسیار سخت باشد [2].

بیومتریک قابل لغو یک کاندید مطمئن در میان روش‌های محافظت الگوی بیومتریک است. این روش برای محافظت اطلاعات بیومتریک اصلی، یک تبدیل اصولی ویژگی‌های مشتق شده بیومتریک بکار می‌برد. اگر یک الگوی بیومتریک قابل لغو کشف رمز شود، مشخصات تبدیل می‌تواند تغییر کند و بیومتریک کاربر به یک الگوی جدید نگاشت شود، که جایگزین الگوی کشف رمز شده می‌شود [6].

در [3] روشهای حفاظت الگو در کل به دو دسته تقسیم می‌شوند (۱) تبدیل ویژگی، (۲) سیستم سری بیومتریک. روش های تبدیل ویژگی یک الگوی محافظت نشده را از طریق یک تابع تبدیل به الگوی محافظت شده تبدیل می‌کند. در فاز تایید، همان تبدیل روی الگوی درخواستی اعمال می شود و کار تطبیق در فضای تبدیل شده ای انجام می شود. بسته به خصوصیات تابع تبدیل این روش به دو روش تبدیل‌های وارون ناپذیر و salting تقسیم می‌شود. تبدیل‌های وارون‌ناپذیر از توابع یک طرفه بهره می‌برند که از نظر محاسباتی به سختی وارون می‌شوند. تبدیل‌های salting یا biohashing برای حفاظت از الگوی اصلی، تابع تبدیل را با کلید مخفی ترکیب می‌کنند. بنابراین روش‌های salting روش‌های تایید هویت دوفاکتوری هستند که امنیت آنها تا حدودی به کلید مخفی بستگی دارد [4].

سیستم‌های رمزنویسی بیومتریک از خصیصه بیومتریک برای تولید یا محافظت یک کلید رمزنگاری استفاده می‌کنند. اطاعات عمومی راجع به الگوی محافظت نشده که داده‌های کمکی خوانده می‌شوند، ذخیره هستند. انتظار نمی‌رود داده‌های کمکی هیچ اطلاعات مهمی درباره الگوی محافظت نشده فاش کنند، بنابراین نیاز نیست که مخفی بمانند. در فاز تطبیق، به کمک داده‌های کمکی، از الگوی درخواستی، یک کلید رمزنگاری استخراج می شود، سپس به صورت غیرمستقیم تایید اعتبار کلید استخراج شده انجام می‌شود. سیستم رمزنویسی بیومتریک به نوبه خود، بسته به چگونگی تولید داده‌های کمکی، به دو دسته تولید کلید و انقیاد کلید تقسیم می‌شود. برای نمونه، داده کمکی از الگوی محافظت نشده تولید می‌شود، و یا با مقید کردن یک کلید خارجی مستقل به الگوی محافظت نشده بدست می‌آید [4].

تا کنون مطالعات متعددی در زمینه حفاظت الگوی اثر انگشت انجام شده است، برای نمونه M.A. Murillo-Escobar و همکاران [1] طرح محافظت الگوی اثر انگشت جدیدی براساس پنهان سازی بی نظم با استفاده از نقشه منطقی الگوریتم Murillo-Escobar [7] ارائه کرده‌اند. حفاظت الگوی بیومتریک این سیستم با استفاده از یک الگوی رمزگذاری برمبنای بی نظمی است. محافظت طرح بیومتریک ارائه شده بر مبنای تبدیل ویژگی است، اما فرایند تطبیق در یک دامنه ساده (الگوی آشکارسازی نیاز است) اجرا می‌شود. پیاده سازی آن بر مبنای یک سیستم خبره با صحت بالا، ثبت نام امن و فرایند تعیین هویت با حفاظت الگوی اثر انگشت است. امنیت طرح ارائه شده با تحلیل های امنیتی کاملا آماری تایید شده است.

Farid Benhammadi و Kadda Beghdad Bey [8] تلاش کرده‌اند یک سیستم بیورمزنویسی بسازند که ویژگی جفت minutiaهای تبدیل شده را با جهش فازی گذرواژه تولید شده توسط کاربر، ترکیب کند. جهش فازی اثر انگشت بر مبنای ساختار جفت minutia جدید است، زمانی که کد جهش دودویی

سری طبق نتایج جهش فازی اثر انگشت تولید می‌شود، بر پخش ویژگی اثر انگشت غلبه می‌کند. فرایند تعیین هویت این سیستم شامل دو مرحله است: تطبیق جهش فازی و تصدیق کد جهش سری. تبدیل جفت minutia، تطبیق الگوهای متفاوتی تولید می‌کند بنابراین مسئله حمله‌های تطبیق دوطرفه در جهش فازی اثر انگشت را رفع می‌کند. طوری که الگوی اثرانگشت اصلی نمی‌تواند دوباره ایجاد شود زیرا با تولید کلید توسط کاربر محافظت شده است. به علاوه، سیستم بیورمزنویسی ارائه شده سطح امنیت قابل قبولی را برای تایید هویت کاربران فراهم می‌کند.

Yang و همکاران [9] یک سیستم مخفی بیومتریک اثر انگشت غیر همتراز ارائه کرده‌اند که 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.

معیارهای ارزیابی متفاوت و پایگاه داده‌های متنوع در این مطالعات بکار رفته است، بنابراین مواردی جهت بررسی انتخاب شده‌اند که دارای اشتراک معیار بررسی باشند و از همه مهم‌تر یک پایگاه داده عمومی مثل FVC را برای آزمایش روش خود انتخاب کرده باشند.

در ادامه پایگاه داده FVC در بخش ۲ معرفی می‌شود و در بخش ۳ سیستم‌های حفاظت االگوی 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 FVC2004, FVC2002, FVC2000 و FVC2006 است.

FVC2000 شامل چهار پایگاه داده DB1, DB2, DB3 و DB4 است که توسط روش‌ها و یا سنسورهای متفاوت جمع آوری شده‌اند [10] که در جدول(۱) به طور خلاصه بیان شده است.

جدول (۱) : پایگاه داده FVC2000 [10]

	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

FVC2002 شامل چهار پایگاه داده DB1, DB2, DB3 و DB4 است که توسط روش‌ها و یا سنسورهای مختلف جمع‌آوری شده‌اند [11] که در جدول(۲) خلاصه آن بیان شده است.

جدول (۲) : پایگاه داده FVC2002 [11]

	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

FVC2004 شامل چهار پایگاه داده DB1, DB2, DB3 و DB4 است که توسط روش‌ها و یا سنسورهای متنوع جمع‌آوری شده‌اند [12]. جدول(۳) خلاصه آن است. 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 [12].

جدول (۳) : پایگاه داده FVC2004 [12]

	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

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 [10]. این در مورد مجموعه‌های پایگاه داده های FVC2000، FVC2002 و FVC2004 صادق است.

FVC2006 روی ارزیابی نرم افزارهای تایید اثر انگشت متمرکز شده است. این پایگاه داده، چهار پایگاه داده DB1, DB2, DB3 و DB4 دارد که توسط روش‌ها و یا سنسورهای مختلف جمع‌آوری شده‌اند [13]، که در جدول (۴) بیان شده است. 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 [13].

جدول (۴) : پایگاه داده FVC2006 [13]

	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

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 [14].

۳- معرفی سیستم‌های حفاظت الگوی اثرانگشت

سیستم‌های حفاظت الگوی 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 (EER) به صورت درصد بیان کرده‌اند.

حفاظت الگوی اثر انگشت با کد چندخطی [6] یک تکنیک الگوی اثر انگشت قابل لغو است که بر مبنای کار قبلی نویسندگان به نام کد چندخطی (MLC) می‌باشد. تغییرات و اصلاحات روی تغییر مقادیر MLC و تولید یک MLC دودویی تمرکز می‌کند. این روش که در اینجا آن را MLC می‌نامیم، روی پایگاه داده‌های FVC2002DB1، FVC2002DB2، FVC2004DB1 و FVC2004DB2 ارزیابی شده است.

نمایش سیلندر-کد minutia برگشت ناپذیر [4] یک تکنیک محافظت جدید برای سیلندر-کد minutia (MCC) ارائه کرده که یک نمایش شناخته شده خوب برای minutia محلی است. یک الگوریتم پیشرفته برای MCC وارون (یعنی بازیافت موقعیت و زاویه اصلی minutia) طراحی شده است. در این روش که اینجا آن را MCC می‌نامیم، آزمایشات اصولی نشان داده که از نظر صحت با روش‌های شاهکار قابل مقایسه است درحالی که همزمان محافظت خوبی از minutiaها انجام می‌دهد و توانمندی مقابله با متقلبان را دارد. این روش روی پایگاه داده‌های FVC2002DB1، FVC2002DB2، FVC2002DB3، FVC2002DB4 و FVC2006DB2 ارزیابی شده است.

در نمایش امن الگوی اثرانگشت [5]، که در مقاله آن را fingerprint shell نامیده‌اند، یک روش جدید محافظت اثر انگشت ارائه شده است. هدف آن تبدیل برگشت ناپذیری است که نیازمندی های قابلیت ابطال، تنوع، امنیت و کارایی را برآورده می‌کند. در این روش اطلاعات با استخراج minutiaها فراهم می‌شوند تا نمایش جدیدی بر مبنای انحنای حلزونی خاص ایجاد کند تا به جای نمایش سنتی برپایه minutia برای کار تشخیص استفاده شود. آزمایشات نشان داده که این نمایش عملکرد سیستم محافظت شده را حفظ کرده است.

۴- بررسی سیستم‌های حفاظت اثرانگشت

در جدول (۵) خلاصه عملکرد سیستم‌های حفاظت الگوی اثر انگشت با معیار EER به صورت درصد و در سناریو اصلی بیان شده است. در این سناریو عملکرد اصلی سیستم بدون استفاده از محافظت و بدون در نظر گرفتن نفوذ حمله‌گر ارزیابی

شده است. همانطور که ملاحظه می‌کنید روش MLC به نرخ خطای برابر (EER)، ۰٪ رسیده است درحالی که روش MCC در مقام بعدی قرار دارد. البته قابل ذکر است که این روش‌ها از نظر پایگاه داده تنها در دو پایگاه داده FVC2002DB1 و FVC2002DB2 مشترک هستند.

جدول (۵) : مقایسه نرخ خطای برابر(EER) روش‌های حفاظت الگوی اثر انگشت برای سناریو اصلی (برحسب درصد)

MCC	MLC	Fingerprint shell	
۱	۰	۲/۰۳	FVC2002DB1
۰/۴۹	۰	۱/۰۱	FVC2002DB2
۳/۱۴			FVC2002DB3
۳			FVC2002DB4
	۰		FVC2004DB1
	۰		FVC2004DB2
۰/۱۲			FVC2006DB2

در جدول (۶) خلاصه عملکرد این روش‌ها را در سناریو کلید سرقت شده ملاحظه می‌کنید. این سناریو حالتی از سیستم را نشان می‌دهد که الگوریتم حفاظت بکارگیری شده و سیستم مورد حمله قرار گرفته است. در این جدول روش MCC عملکرد بهتری از خود نشان داده است. پس از آن روش MLC قرار دارد.

جدول (۶) : مقایسه نرخ خطای برابر (EER)روش‌های حفاظت الگوی اثر انگشت برای سناریو کلید سرقت رفته (برحسب درصد)

MCC	MLC	Fingerprint shell	
۱/۸۸	۱/۹۷	۴/۲۸	FVC2002DB1
۰/۹۹	۲/۵۴	۱/۴۵	FVC2002DB2
۵/۲۴			FVC2002DB3
۴/۸۴			FVC2002DB4
	۶/۵۳		FVC2004DB1
	۹/۲		FVC2004DB2
۰/۱۷			FVC2006DB2

۵- نتیجه

آنچه از مطالب حاضر برآورد می‌شود نشان می‌دهد عملکرد عادی سیستم MLC از سایر سیستم‌ها بهتر بوده است. و از نظر حفاظت الگوی بیومتریک عملکرد روش MCC بهتر است.

قابل ذکر است که سیستم‌های بررسی شده پایگاه داده‌های محدودی را مورد آزمایش قرار داده‌اند، بنابراین نمی‌توان در مورد عملکرد آنها با قطعیت نظر داد.

مراجع

[1] 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 System with Application, Vol. 42, pp. 8198-8211, 2015.

[2] 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.

[3] Jain A.K., Nandakumar K., Negar A., "Biometric template security", EURASIP journal on advances in Signal Processing, pp. 11, 2008.

[4] Matteo Ferrara, Davide Maltoni, "Noninvertible Minutia Cylinder-Code Representation", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, Vol. 7, pp. 1727-1737, 2012.

[5] Chouaib Moujahdi, George Bebis, Sanaa Ghouzali, Mohammed Rziza, "Fingerprint shell: Secure representation of fingerprint template", Pattern Recognition Letters, Vol. 45, pp. 189-196, 2014.

[6] Wei Jing Wong, Andrew B.J. Teoh, M.L. Dennis Wong, Yau Hee Kho, "Enhanced multi-line code for minutiae-based fingerprint template protection", Pattern Recognition Letters, Vol. 34, pp. 1221-1229, 2013.

[7] Murillo M.A. Murillo-Escobar, F. Abundiz-Pérez, C. Cruz-Hernández, R.M. López-Gutiérrez, "A novel symmetric text encryption algorithm based on logistic map", In Proceedings of the international conference on communication, Signal Processing and computers, pp. 49-53, 2014.

[8] Farid Benhammadi, Kadda Beghdad Bey, "Password hardened fuzzy vault for fingerprint authentication system", Image and Vision Computing, Vol. 32, pp. 487-496, 2014.

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

[10] 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/

[11] 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/

[12] 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/

[13] 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/

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

- biometric
- Identification Card
- Passwod
- Personal Identification Number
- template
- ridge
- valley
- ending
- bifurcation
- security
- secrecy
- revocability
- Cross-matching
- cancellable
- transformation
- Biometric cryptosystem
- Transformed space
- Noninvertible
- Helper data
- Key-generation
- Key-binding
- Chaos
- plain
- expert
- publication
- Voronoi Neighbor Structure
- Synthetic Fingerprint Generator
- Equal Error Rate
- Multi-line code
- Noninvertible Minutia Cylinder-Code
- Genuine scenario
- Stolen key Scenario