INSO
11980-11
1st.Edition
Mar.2014

جمهوری اسلامی ایران
Islamic Republic of Iran
سازمان ملی استاندارد ایران
Iranian National Standardization Organization

استاندارد ملی ایران
۱۱۹۸۰-۱۱
چاپ اول
اسفند ۱۳۹۲

فناوری اطلاعات: قالب‌های تبادل داده‌های زیست سنجی: قسمت ۱۱: نشانه/امضاء پردازش شده‌ی داده پویا

Information technology-biometric data interchange formats- Part 11:signature/sign processed dynamic data

ICS: 35.040

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران به موجب بند یک مادهٔ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفه تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

نام موسسه استاندارد و تحقیقات صنعتی ایران به موجب یکصد و پنجاه و دومین جلسه شورای عالی اداری مورخ ۹۰/۶/۲۹ به سازمان ملی استاندارد ایران تغییر و طی نامه شماره ۲۰۶/۳۵۸۳۸ مورخ ۹۰/۷/۲۴ جهت اجرا ابلاغ شده است .

تدوین استاندارد در حوزه های مختلف در کمیسیون های فنی مرکب از کارشناسان سازمان ، صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می شود وکوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و وارد کنندگان، مراکز علمی و تخصصی، نهادها، سازمان های دولتی و غیر دولتی حاصل می شود . پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی نفع و اعضای کمیسیون های فنی مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می شود.

پیش نویس استانداردهایی که مؤسسات و سازمان های علاقه مند و ذی صلاح نیز با رعایت ضوابط تعیین شده تهیه می کنند درکمیتهٔ ملی طرح و بررسی و درصورت تصویب ، به عنوان استاندارد ملی ایران چاپ و منتشر می شود . بدین ترتیب ، استانداردهایی ملی تلقی می شوند که بر اساس مفاد نوشته شده در استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که سازمان ملی استاندارد ایران تشکیل می‌دهد به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین المللی استاندارد (ISO)[1] ،کمیسیون بین المللی الکتروتکنیک (IEC)[2] و سازمان بین المللی اندازه شناسی قانونی (OIML)[3] است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می کند . در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی های خاص کشور ، از آخرین پیشرفت های علمی ، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود .

سازمان ملی استاندارد ایران می تواند با رعایت موازین پیش بینی شده در قانون ، برای حمایت از مصرف کنندگان ، حفظ سلامت و ایمنی فردی و عمومی ، حصول اطمینان از کیفیت محصولات و ملاحظات زیست محیطی و اقتصادی ، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/ یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید.

سازمان می تواند به منظور حفظ بازارهای بین المللی برای محصولات کشور ، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید . همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سازمان ها و مؤسسات فعال در زمینهٔ مشاوره ، آموزش ، بازرسی ، ممیزی و صدور گواهی سیستم های مدیریت کیفیت و مدیریت زیست‌محیطی ، آزمایشگاه ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش ، سازمان ملی استاندارد ایران این گونه سازمان ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می کند و در صورت احراز شرایط لازم ، گواهینامهٔ تأیید صلاحیت به آن ها اعطا و بر عملکرد آن ها نظارت می کند . ترویج دستگاه بین المللی یکاها ، کالیبراسیون (واسنجی) وسایل سنجش ، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است .

1- International Organization for Standardization
2 - International Electrotechnical Commission
3- International Organization of Legal Metrology (Organisation Internationale de Metrologie Legale)
4 - Contact point
5 - Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

"فناوری اطلاعات: قالب های تبادل داده‌های زیست سنجی :قسمت ۱۱: نشانه/امضاء پردازش شده‌ی داده پویا "

رئیس:	**سمت و/ یا نمایندگی**
رودکی، مصطفی (فوق لیسانس مهندسی برق)	مدیر تولید صنایع قطعات الکترونیک
دبیر:	
ظل‌انوار، محمد علی (لیسانس مهندسی برق)	کارشناس اداره کل استاندارد فارس
اعضاء: (اسامی به ترتیب حروف الفبا)	
ابراهیمی، علی اکبر (فوق لیسانس مخابرات)	کارشناس صنایع قطعات الکترونیک
پروا، بهروز (لیسانس مهندسی صنایع)	کارشناس اداره کل استاندارد فارس
جاویدی، محمد جواد (لیسانس شیمی)	کارشناس سازمان صنعت معدن تجارت
حکم طلعت، هادی (فوق لیسانس الکترونیک)	کارشناس صنایع قطعات الکترونیک
صداقت، عزیز (لیسانس کامپیوتر)	کارشناس صنایع قطعات الکترونیک
عطروش، حسینعلی (لیسانس مهندسی برق الکترونیک)	کارشناس اداره کل استاندارد فارس

کاووسی، زهرا (فوق لیسانس مهندسی فناوری اطلاعات)	کارشناس سازمان صنعت معدن تجارت
کشتگری، منیژه (دکتری مهندسی کامپیوتر)	استادیار دانشگاه صنعتی شیراز
مغانی، مهدی (کارشناس ارشد ریاضی کاربردی)	کارشناس سازمان فناوری اطلاعات
یوسفی، عبدالله (لیسانس صنایع)	کارشناس سازمان صنعت، معدن و تجارت

فهرست مندرجات

	عنوان	صفحه
	آشنایی با سازمان ملی استاندارد	ب
	کمیسیون فنی تدوین استاندارد	ج
	پیش گفتار	ه
	مقدمه	و
۱	هدف و دامنه کاربرد	۱
۲	مراجع الزامی	۱
۳	اصطلاحات و تعاریف	۱
۴	انطباق	۲
۵	قراردادها	۳
۶	روابط قالب داده	۴
۷	نشانه/ امضاء ثبت شده	۴
۸	قالب رکورد نشانه/امضاء پردازش شده	۷
۹	پیوست الف (روش شناسی آزمون انطباق)	۱۷
۱۰	پیوست ب (ویژگی های ASN.1 قالب داده)	۱۸
۱۱	پیوست پ (نشانه /امضاهای مناسب برای کاربرد احراز هویت)	۲۱

پیش گفتار

استاندارد "فناوری اطلاعات:قالب‌های تبادل داده‌های زیست سنجی:قسمت ۱۱- نشانه/امضاء پردازش شده‌ی داده پویا" که پیش نویس آن در کمیسیون های مربوط توسط سازمان ملی استاندارد تهیه و تدوین شده است و در سیصدو بیست و دومین اجلاس کمیته ملی استاندارد رایانه و فرآوری داده ها مورخ۱۳۹۲/۱۱/۲۸ مورد تصویب قرار گرفته است، اینک به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات موسسه استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می شود .

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت های ملی و جهانی در زمینه صنایع، علوم و خدمات، استانداردهای ملی ایران در مواقع لزوم تجدید نظر خواهد شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود، هنگام تجدید نظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت. بنابراین، باید همواره از آخرین تجدید نظر استانداردهای ملی استفاده کرد.

منبع و ماخذی که برای تهیه این استاندارد مورد استفاده قرار گرفته به شرح زیر است:

ISO/IEC 19794-11 :2013 ,information technology –biometric data interchange formats- part11 :signature/sign processed dynamic dat

فناوری اطلاعات: قالب‌های تبادل داده‌های زیست سنجی:قسمت ۱۱- نشانه/امضاء پردازش شده‌ی داده پویا

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد تعیین قالب تبادل داده رفتاری نشانه/امضاء پردازش شده که از سری‌های زمانی اقتباس شده اند، وسایل کاربردی ضبط کننده مثل تبلت های دیجیتالی[1] وسایل محاسباتی بر مبنای قلم[2] یا سیستم های قلمی پیشرفته می باشد.

کاربرد قالب تبادل داده به صورت عمومی می باشد به گونه ای که ممکن است در طیف وسیعی از نواحی کاربردی که نشانه‌های‌دست نوشته‌یا نشانه/امضاء پیچیده باشد،مورد استفاده قرارگیرد.هیچ الزامات ویژه- کاربردی یا خصیصه‌ای در این استاندارد ملی عنوان نشده‌است.این‌استاندارد شامل تعریف اصطلاحات مربوطه، شرحی از داده‌های اقتباس شده و قالب داده برای در برگیری داده همراه با توصیه لازم درباره مناسب بودن یک مجموعه نشانه/امضاء کاربر برای اهداف احراز هویت می باشد.

بهتر است داده های زیست سنجی ذخیره وارسال شده مهر زمانی داشته باشند و تکنیک های رمزنگاری برای- حفظ سندیت، یکپارچگی ومحرمانه بودن مورد استفاده قرار گیرد هرچند این قوانین هدف این استاندارد نمی باشد.

۲ مراجع الزامی

مدارک الزامی زیر حاوی مقرراتی است که در متن این استاندارد ملی ایران به آن ها ارجاع داده شده است. بدین ترتیب آن مقررات جزئی از این استاندارد ملی ایران محسوب می شود .

در صورتی که به مدرکی با ذکر تاریخ انتشار ارجاع داده شده باشد ، اصلاحیه ها و تجدید نظرهای بعدی آن مورد نظر این استاندارد ملی ایران نیست . در مورد مدارکی که بدون ذکر تاریخ انتشار به آن ها ارجاع داده شده است ، همواره آخرین تجدید نظر و اصلاحیه های بعدی آن ها مورد نظر است.

استفاده از مراجع زیر برای این استاندارد الزامی است :

2-1 ISO/IEC 19785-2 , information technology –common biometric exchange formats framework- part2:procedures for the operation of the biometric registration authority

2-2 ISO/IEC 19794-1 , information technology –biometric data interchange formats-part 1: framework

۳ اصطلاحات و تعاریف

1- digitizing tablets

2- pen-based computing devices

در این استاندارد علاوه بر اصطلاحات و تعاریف استاندارد ISO/IEC 19794-1، تعاریف و اصطلاحات زیر به کار می رود.

۳-۱

رویداد پویا

رویداد بالا و پایین رفتن قلم و یا نقطه برگشت

۳-۲

پایین رفتن قلم

رویدادی که در آن نوک قلم صفحه نوشتن را لمس می کند.

۳-۳

داده رویداد – پویا

داده ای که موقعیت قلم، فشار و زمان را برای رویداد پویا نشانه/امضاء داده شده، ثبت می کند.

۳-۴

بالا رفتن قلم

رویدادی که در آن نوک قلم صفحه نوشتن را لمس نمی‌کند.این رویداد بعد از رویداد پایین رفتن قلم می باشد.

۳-۵

نمایش نشانه/امضاء

داده ای که از یک نشانه/امضاء ساده ثبت شده است.

یادآوری- یک نمایش نشانه/امضاء همیشه با یک رویداد پایین آمدن قلم شروع و با بالارفتن قلم خاتمه می یابد.اما می تواند تعداد بیشتری بالا و پایین رفتن قلم در نمایش نشانه/امضاء وجود داشته باشد.

۳-۶

نقطه برگشت[1]

رویدادی که درآن نشانه انحراف از نمونه های مجاور X، Yو یا تغییرات کانال F ناشی می شود.

۴ انطباق

یک رکورد داده زیست سنجی در صورت تامین تمام الزامات اصلی مرتبط با موارد زیر با این استاندارد مطابقت دارد.

الف) ساختار داده، مقادیر داده و رابطه بین عناصر داده که در بند ۸ این استاندارد تعیین شده است.

ب) رابطه بین مقادیر داده و داده زیست سنجی ورودی، با توجه به تولید رکورد داده زیست سنجی که در بند ۸ این استاندارد تعیین شده است.

1- turning point

در صورتیکه تمامی‌رکوردهای داده زیست سنجی خروجی مطابق با این استاندارد باشند آنگاه سیستمی که رکوردهای داده زیست سنجی را تولید می‌کند از این استاندارد ملی پیروی می کند.لازم نیست‌که‌یک سیستم توانایی تولید رکوردهای داده زیست سنجی مطابق با تمامی جنبه‌های این استاندارد را داشته باشد اما باید توانایی تولید موارد ادعا شده توسط سیستم را داشته باشد.

یک سیستم که از رکوردهای داده زیست سنجی استفاده می کند در صورتیکه خوانده شود و برای هدف مورد نظر سیستم استفاده گردد با این استاندارد ملی مطابقت دارد.لازم نیست که یک سیستم توانایی استفاده از رکوردهای داده زیست سنجی مطابق با تمامی جنبه های این استاندارد را داشته باشد اما باید توانایی استفاده از مواردی که توسط سیستم ادعا شده را داشته باشد.

۵ قراردادها

۵-۱

سیستم مختصات

سیستم مختصات برای بیان موقعیت قلم باید یک سیستم مختصات دو بعدی باشد.محور X بایستی محورافقی صفحه نوشتن با مختصات X با قابلیت افزایش به سمت راست و شروع از صفر باشد.محورYبایستی محور عمودی صفحه نوشتن با مختصات Y با قابلیت افزایش به سمت بالا و شروع از صفر باشد.

۵-۲

ترتیب بایت

با ارزش ترین بایت های یک ارزش چند بایتی در آدرس های پایین تر در حافظه نسبت به بایت های با ارزش کم تر ذخیره می شوند.

درون یک بایت، بیت ها از شماره ۸ تا ۱ شماره گذاری می شوند که در آن بیت شماره ۸ بیت با بیشترین ارزش وبیت شماره ۱، بیت با کمترین ارزش می باشد.

۵-۳

شناسه نوع قالب ثبت شده

رکوردهای داده تعیین شده دراین استاندارد می‌توانند در یک رکورد اطلاعات زیست سنجی[1] سازگار با چارچوب قالب تبادل زیست سنجی متعارف[2]،جاسازی[3] شوند.این بند بلوک داده زیست سنجی[4] شناسه صاحب قالب و بلوک داده زیست سنجی شناسه نوع قالبی که درصورت جاسازی در رکورد اطلاعات زیست سنجی چارچوب قالب تبادل زیست سنجی متعارف[5] بایستی مورد استفاده قرار گیرد را فهرست می کند.این شناسه‌توسط IBIA

1- biometric information record (BIR)
2- common biometric exchange formats frame work (CBEFF)
3- Embedded
4-biometric data block (BDB)
5-common biometric exchange formats frame work biometric information record (CBEFF BIR)

،مرجع قانونی ثبت چارچوب قالب تبادل زیست سنجی متعارف، ثبت شده است(به استاندارد ISO/IEC 19785-2 مراجعه شود).

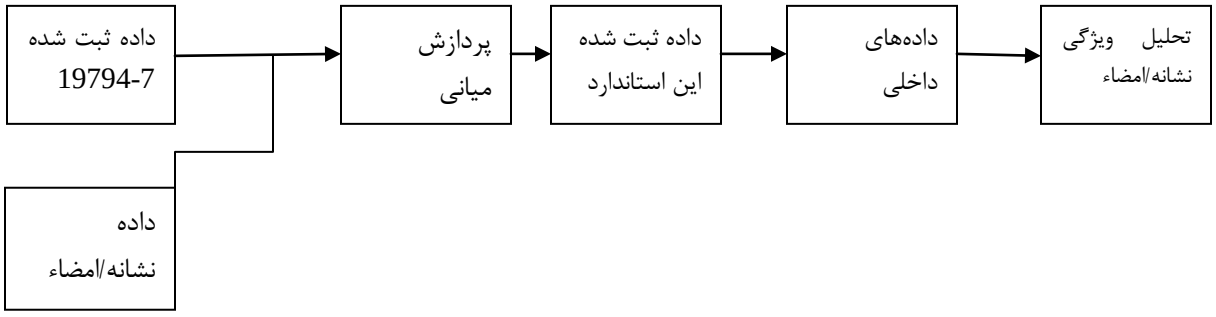
دارنده قالب‌های تعریف شده دراستاندارد ISO/IEC 19794، استاندارد ISO/IEC JTC 1/SC 37 می باشد.شناسه دارنده قالب، ۲۵۷می باشد(0101HEX).جدول۱ شناسه نوع قالب های تعریف شده در این استاندارد را فهرست می کند.

جدول ۱ – شناسه های نوع قالب

شناسه قالب	نام اختصاری	شناسه تمام موضوع
۱۶(۰۰۱۰HEX)	نشانه/امضاء پردازش شده پویا	ISO(1) - صحت ثبت نام (1) – سازمان زیست سنجی(19785) CBEFF (0) - bdbs(0) jtc1-sc37 (257) نشانه/امضاءی پردازش شده پویا (16)

۶ روابط قالب داده

قالب داده پردازش‌شده دراین‌استاندارد می‌تواند قالب نهایی‌مورد استفاده بوسیله الگوریتم های تحلیل نشانه/امضاء پویا برای تحلیل خصیصه‌های نشانه/امضاء نباشد.قالب، یک قطعه بر پایه قالب داده امضاء با اطلاعات کافی جهت استنتاج خصیصه‌های نشانه/امضاء در الگوریتم های مختلف می باشد.کاربرد آن در نمودار شکل ۱ نشان داده شده است.



شکل ۱ – نمودار قالب داده

۷ داده نشانه / امضاء ثبت شده

۷-۱ مرور

با ثبت داده رویداد پویا درروییدادهای پویای نشانه/امضاء مهم همانند: پایین آوردن قلم، بالا بردن قلم و نقطه برگشت این رویدادها می توانند در قسمت های بزرگتر ترکیب شوند یا برای هر تحلیل خصیصه با یک دنباله از نشانه قیاس شوند.

داده نشانه/امضاء به عنوان یک دنباله ای‌از داده رویداد پویا برای هررویداد پویای قابل توجه که از تمامی خصیصه های یک مجموعه داده پیروی می کند، ثبت خواهد شد.

۲-۷

داده رویداد پویا

هر زمان که رویداد امضاءی پویا به صورت زیر حادث شود، مختصات X، Y، فشار F، زمان T، و نوع رویداد باید ثبت گردد.

الف) پایین آمدن قلم؛

ب) بالا آمدن قلم؛

پ) نقطه برگشت.

۱-۲-۷

پایین آمدن قلم

پایین آمدن قلم یک رویداد است که نوک قلم صفحه نوشتن را لمس می کند.پایین آمدن قلم هنگامی که تغییرات کانال F به صورت زیر دنبال شود، نمایان می گردد.

$F_n > 0$ و $F_{n-1}=0$

۲-۲-۷

بالا آمدن قلم

بالا آمدن قلم یک رویداد است که نوک قلم صفحه نوشتن را ترک می‌کند.بالا آمدن قلم هنگامی‌که تغییرات کانال F به صورت زیر دنبال شود، نمایان می گردد.

$F_{n-1}>0$ و $F_n=0$

۳-۲-۷

نقطه برگشت

یک نقطه برگشت یک رویداد است که نشانه انحراف از نمونه های مجاور Y،X یا تغییرات کانالF ناشی می شودکه Q، Xیا Yمربوط به کانال F را مشخص می‌کند.دو نوع نقطه برگشت به صورت زیر تعریف می شود:

نوع اول : تغییر از مثبت به صفر یا منفی. در این نوع، نقطه برگشت کانال Q باید شرایط زیر را برآورده سازد.

$Sign(Q_{n-1} - Q_{n-2}) = sign(Q_n - Q_{n-1}) =$ مثبت

$Sign(Q_{n+2} - Q_{n+1}) = sign(Q_{n+1} - Q_n) =$ ۰ یا منفی

یا

$Sign(Q_{n-1} - Q_{n-2}) = sign(Q_n - Q_{n-1}) =$ ۰

$Sign(Q_{n+2} - Q_{n+1}) = sign(Q_{n+1} - Q_n) =$ منفی

که در آن Q_n نقطه برگشت کانال Q می باشد.

نوع دوم : تغییر از منفی به صفر یا مثبت. در این نوع، نقطه برگشت کانال Q باید شرایط زیر را برآورده سازد.

$Sign (Q_{n-1} - Q_{n-2}) = sign (Q_n - Q_{n-1}) =$ منفی

$Sign (Q_{n+2} - Q_{n+1}) = sign (Q_{n+1} - Q_n) =$ ۰ یا مثبت

یا

$Sign (Q_{n-1} - Q_{n-2}) = sign (Q_n - Q_{n-1}) =$ ۰

$Sign (Q_{n+2} - Q_{n+1}) = sign (Q_{n+1} - Q_n) =$ مثبت

که در آن Q_n نقطه برگشت کانال Q می باشد.

قبل از محاسبه نشانه انحراف که از نمونه های مجاور ناشی می شود بهتر است x ، y و کانال F توسط یک فیلتر میانگین جابجا شونده نقاط M که در زیر آمده، هموار شوند[1].(M بایستی حتما عدد فرد باشد)

$$Qi = \frac{1}{M} \sum_{m=-\frac{M-1}{2}}^{\frac{M-1}{2}} Q\,i + m$$

که Q_i نمونه i ام کانال Q می باشد.

واحد اندازه‌گیریX وY بر حسب میلی‌متر، واحد اندازه گیری F برحسب نیوتن و واحد اندازه گیریT بر حسب میلی‌ثانیه می‌باشد. برای بازگرداندن به مقادیر واقعی، مقادیر عدد صحیح داده شده در بدنه رکورد تبادل داده زیست سنجی[2] باید بر ارزش مقیاس‌ارائه شده در سرآیند[3] نمایش تقسیم گردد.با انتخاب مقادیر مقیاس‌مناسب، نتایج متفاوت برای کاربردهای مختلف ارائه می شود.

۳-۷ خصیصه های کلی داده

پارامترهای دیگر که باید برای تحلیل پویای نشانه/امضاء کلی ثبت گردد به شرح زیر است:

الف) زمان کل ؛

زمان کل T به صورت اختلاف زمان اولین ثبت و زمان آخرین ثبت یک نشانه/امضاء ؛

واحد اندازه گیری میلی‌ثانیه می باشد.

برای بازگرداندن به مقادیر واقعی، مقادیر عدد صحیح داده شده در فیلد زمان کل‌باید بر ارزش مقیاس T ارائه شده در سرآیند نمایش تقسیم گردد.

ب) تعداد کل نقاطی که TNP را به دست آورده اند(یک تابع از زمان و زمان نمونه برداری ظرفیت‌های رقمی کننده) ؛

تعداد کل نقاط اندازه گیری شده به صورت تعداد کل مختصات ثبت شده برای یک نشانه/امضاء با عدد صحیح تعریف می شود.

1- smoothed

2- biometric data interchange record (BDIR)

3- header

پ) مقادیر میانگین؛

X_{mean} : ارزش میانگین مقادیر X

Y_{mean} : ارزش میانگین مقادیر Y

F_{mean} : ارزش میانگین مقادیر فشار F

زمانیکه قلم با رقمی‌کننده در تماس‌است X_{mean} ،Y_{mean}، F_{mean} مقادیر میانگین حسابیX،YوF می باشند.واحد اندازه گیری X_{mean} ،Y_{mean} میلی‌متر و واحد اندازه گیری F_{mean} نیوتن است.

برای بازگرداندن به مقادیر واقعی، مقادیر عدد صحیح داده شده در فیلد مقادیر میانگین X، Y باید به ترتیب بر ارزش مقیاس X و Yارائه شده در سرآیند نمایش تقسیم گردد.

ت) مقادیر انحراف استاندارد

S_X: ارزش انحراف استاندارد X

S_Y: ارزش انحراف استاندارد Y

S_F: ارزش انحراف استاندارد F

S_X، S_Y، S_F انحراف استاندارد مقادیر X، Y، F می باشند.

$$S = \sqrt{\frac{\Sigma(v-m)^2}{n}}$$

که در آن:

V : مقادیر X ، Y یا F

m : میانگین حسابی X، Y یا F

n : تعداد مقادیر

واحد اندازه گیری S_X و S_Y میلی‌متر و واحد اندازه گیری S_F نیوتن می باشد.

برای بازگرداندن به مقادیر واقعی، مقادیر عدد صحیح داده شده در فیلد مقادیر انحراف استاندارد X، Y باید به ترتیب بر ارزش مقیاس X ، Yارائه شده در سرآیند نمایش تقسیم گردد.

ث) ضریب همبستگی

(ضریب همبستگی تمام داده (X,Y) تا سه رقم اعشار +1)× R_{XY}- 1000

این ارزش همیشه مثبت خواهد بود.ضریب همبستگی تمامی داده XY برابر با R به صورت زیر است.

$$R = \frac{n \cdot \Sigma_i(xi - yi) - \Sigma_i xi \cdot \Sigma_i yi}{\sqrt{(n \cdot \Sigma_i xi^2 - (\Sigma_i xi)^2) \cdot (n \cdot \Sigma_i yi^2 - (\Sigma_i yi)^2)}}$$

n : تعداد مقادیر

۸ قالب رکورد نشانه /امضاء پردازش شده پویا

۸-۱ مرور

این استاندارد ترکیب رکورد نشانه/امضاء پردازش شده پویا را تعریف می کند.

هررکورد باید به یک موضوع منفرد مربوط باشد وباید شامل یک رکورد نشانه/امضاء پردازش شده پویا باشد.(شامل یک یا تعداد بیشتری نمایش).سازمان قالب رکورد به شرح زیر است:

الف) یک سرآیند رکورد عمومی با طول ثابت (۱۵ بایت) شامل اطلاعات در مورد تمامی رکوردها

ب) یک بدنه نمایش شامل یک رکورد منحصراز نشانه/امضاء پردازش شده پویا برای‌هر نمایش نشانه/امضاء شامل:

- یک سرآیند با طول متغیر شامل داده مربوط به یک نمایش نشانه/امضاء منحصر؛
- داده رویداد پویا و خصیصه های کلی داده مربوط به یک نمایش نشانه/امضاء منحصر؛
- داده اختیاری‌گسترش یافته [1] (در بند ۸-۷ شرح داده شده است).

۸-۲ سرآیند رکورد عمومی

ساختار سرآیند رکورد عمومی باید مطابق تعریف ارائه شده در جدول شماره ۲ باشد.

جدول ۲- سرآیند بلوک داده نشانه/امضاء پردازش شده پویا

فیلد سرآیند رکورد عمومی	طول	توضیحات
شناسه قالب	۴ بایت	شناسه قالب بایستی در ۴ بایت ثبت شود.شناسه قالب باید شامل سه کاراکتر "SPD" که توسط یک بایت صفر به عنوان یک رشته پایان دهنده صفر دنبال می شود
شماره نسخه	۴ بایت	شماره نسخه آن قسمت از استاندارد ISO/IEC 19794 که برای ساخت رکورد تبادل داده زیست سنجی استفاده می شود باید در ۴ بایت قرار گیرد.این شماره نسخه باید شامل سه عدد ASCII که توسط یک بایت صفر به عنوان یک رشته پایان دهنده صفر دنبال می شود، باشد.اولین ودومین کاراکتر ،بزرگترین شماره نسخه و سومین کاراکتر کوچکترین شماره نسخه را بیان می کند.شماره نسخه باید به صورت "۰۱۰" – شماره ۱ بازبینی ۰ باشد.
طول رکورد	۴ بایت	طول تمام رکورد تبادل داده زیست سنجی باید در ۴ بایت ثبت شود.این شمار باید طول کل رکورد تبادل داده زیست سنجی شامل سرآیند یک رکورد عمومی و یک یا تعداد بیشتری رکوردهای نمایش باشد.
تعداد نمایش	۲ بایت	تعداد کل رکوردهای نمایش شامل رکورد تبادل داده زیست سنجی باید در ۲ بایت ثبت شود.حداقل یک نمایش الزامی است.
پرچم تایید	۱ بایت	یک پرچم تایید یک بایتی باید بلوک تصدیق مربوط به هر سرآیند رانشان دهد.ارزش آن باید ۰۰HEX باشد تا نشان دهد هیچ نمایشی شامل بلوک تصدیق نمی باشد. **یادآوری**- پرچم تایید برای سازگاری بالاتر با نسخه های بعدی قالب که در آن ممکن است سرآیند های نمایش شامل بلوک تصدیق باشد، اضافه شده است.

۸-۳ سرآیند نمایش

۸-۳-۱ مرور

فیلد سرآیند نمایش باید مطابق تعاریف جداول ۳ و ۶ باشد.

[1] - extended

جدول ۳ – عناصر معمول سرآیند نمایش

نام	طول	متن متناسب تعاریف قالب رکورد
طول نمایش	۴ بایت	طول را در بایت های سرآیند نمایش شامل فیلد های سرآیند نمایش مشخص می کند.
ضبط تاریخ وزمان	۹ بایت	ضبط فیلد زمان و تاریخ بایستی زمان شروع نمایش را در مختصات زمان جهانی نشان دهد.(utc). فیلد ضبط تاریخ و زمان باید شامل ۹ بایت باشد.ارزش آن باید به شکل ارائه شده در استاندارد ISO/IEC 19794-1 به رمز در آورده شود.
شناسه تکنولوژی وسیله ضبط	۱ بایت	شناسه تکنولوژی وسیله ضبط باید در یک بایت به رمز درآورده شود.این فیلد باید طبقه تکنولوژی وسایل ضبط مورد استفاده برای بدست آوردن نمونه زیست سنجی ضبط شده را نشان دهد.ارزش HEX ۰۰ نشان دهنده تکنولوژی ناشناخته می باشد.برای فهرست مقادیر ممکن به جدول ۴ مراجعه شود.
شناسه ارائه دهنده وسیله ضبط	۲ بایت	شناسه ارائه دهنده وسیله ضبط بایستی سازمان زیست سنجی مالکیت محصول که رکورد تبادل داده زیست سنجی راتولید می کند نشان دهد.شناسه ارائه دهنده الگوریتم وسایل ضبط بایستی در ۲ بایت‌که هویت سازمان زیست سنجی یک چهارچوب قالب تبادل زیست سنجی متعارف را حمل میکند به رمز درآورده شود.(ثبت شده بوسیله IBIA یا دیگر مراجع قانونی تایید صلاحیت شده)یک ارزش تماماً صفر باید بیانگر عدم گزارش ارائه دهنده وسایل باشد.
شناسه نوع وسیله ضبط	۲ بایت	شناسه نوع‌وسیله ضبط باید نوع محصولی که رکورد تبادل داده زیست سنجی را تولید می کند مشخص سازد. این شناسه باید به وسیله مالک محصول ثبت شده یا دیگر مراجع قانونی تاییدصلاحیت شده ، ذکر گردد.نوع های محصول ثبت شده باید شامل تمامی ترکیب های ممکن لوح های نوشتن و قلم به عنوان یک محصول منحصر در جاییکه کاربرد دارد، باشد.یک ارزش تماماً صفر باید بیانگر عدم گزارش نوع وسایل باشد. اگر شناسه ارائه دهنده وسایل ضبط به صورت 0000 HEX باشد در آن صورت شناسه نوع وسایل ضبط نیز باید به صورت 0000HEX باشد.
رکورد کیفیت	ا تا n بایت	یک رکورد کیفیت باید شامل یک فیلد طول که با صفر یا تعداد بیشتری بلوک های کیفیت‌دنبال می شود ،باشد. فیلد طول باید شامل یک بایت باشد.فیلد طول باید تعداد بلوک های کیفیت را به صورت عدد صحیحی بدون علامت بیان کند. هر بلوک کیفیت باید شامل: - یک امتیاز کیفیت - یک شناسه ارائه دهنده الگوریتم کیفیت - شناسه الگوریتم کیفیت بهتر است یک امتیاز کیفیت کارایی مقایسه پیش بینی شده یک نمایش را بیان کند.یک امتیاز کیفیت باید در یک بایت با عدد صحیح بدون علامت به رمز درآورده شود. مقادیر مجاز به صورت زیر می باشد. ۰ تا ۱۰۰ که مقادیربالاتر کیفیت بهتر را نشان می دهد. ۲۵۵، برای مثال ff hex برای نشان دادن اینکه تلاش جهت محاسبه امتیاز کیفیت مردود می باشد. شناسه ارائه دهنده الگوریتم کیفیت باید در ۲ بایت که شناسه سازمان زیست سنجی یک چارچوب قالب تبادل زیست سنجی متعارف را حمل می کند به رمز درآورده شود(ثبت شده بوسیله IBIA یا دیگر مراجع قانونی تاییدصلاحیت شده). یک ارزش تماماً صفر باید بیانگر عدم گزارش ارائه دهنده الگوریتم کیفیت باشد.

جدول ۳ – عناصر معمول سرآیند نمایش- ادامه

		شناسه الگوریتم کیفیت باید الگوریتم کیفیت ارائه دهنده که امتیاز کیفیت را تولید می‌کند، مشخص سازد. این شناسه باید توسط تامین کننده الگوریتم کیفیت یا دیگر مراجع قانونی تاییدصلاحیت شده ذکرگردد.شناسه الگوریتم کیفیت بایستی در ۲ بایت به رمز درآورده شود.یک ارزش تماماً صفر باید بیانگر عدم گزارش الگوریتم کیفیت باشد.

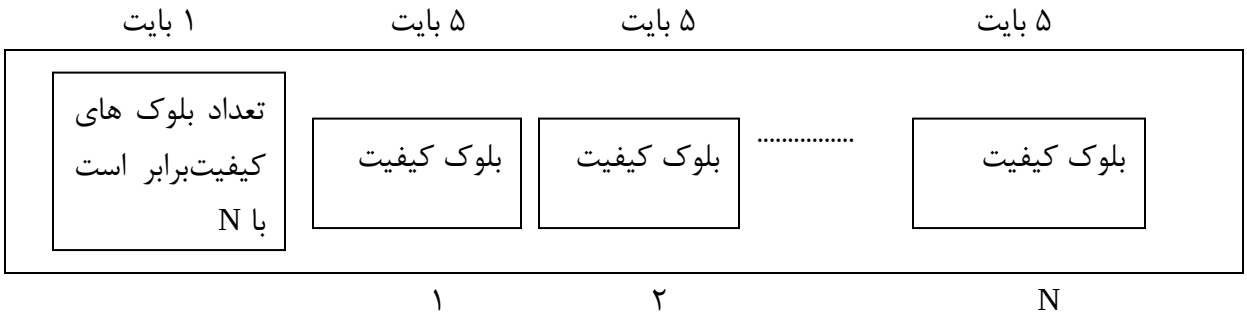
۸-۳-۲ قالب برای شناسه تکنولوژی وسایل ضبط

جدول ۴ - قالب برای شناسه تکنولوژی وسایل ضبط

نام	طول	طبقه تکنولوژی وسایل
شناسه تکنولوژی وسایل ضبط	۱ بایت	شناسه تکنولوژی وسایل ضبط بایستی در یک بایت به رمز در آورده شود که: ۰۰ HEX : ناشناخته یا مشخص نشده ۰۱ HEX : الکترومغناطیس ۰۲ HEX : نیمه رسانا ۰۴ HEX : قلم مخصوص با حس گرهای سرعت ۰۸ HEX : قلم مخصوص با حس گرهای نوری تمامی مقادیر دیگر توسط SC 37 برای کاربردهای آینده ذخیره شده است.

۸-۳-۳ قالب توصیف گر کیفیت

این استاندارد باید امتیازهای کیفیت مختلفی را در هرنمایش همانگونه که در شکل ۲ نشان داده شده پشتیبانی نماید. بهتر است هر امتیاز با استفاده از یک بلوک کیفیت ۵ بایتی که در جدول شماره ۵ نشان داده شده به رمز درآورده شود.



شکل ۲- پشتیبانی برای بلوک های کیفیت چندگانه

جدول ۵ – ساختار فیلد های کیفیت

شرح		طول	مقادیر معتبر	ملاحظات
تعداد بلوک های کیفیت		۱ بایت	۰ تا ۲۵۵	این فیلد با تعداد بلوک های کیفیت ۵ بایتی که توسط ارزش آن بازتاب داده می شود ،دنبال می‌شود.ارزش‌صفر به این معنا است‌که هیچگونه تلاشی برای اختصاص امتیاز کیفیت صورت نپذیرفته است.در این حالت هیچ بلوک کیفیتی موجود نمی باشد.
بلوک کیفیت	امتیاز کیفیت	۱ بایت	۰ تا ۱۰۰ ۲۵۵	۰ : کمترین ۱۰۰ : بیشترین ۲۵۵ : تلاش مردود برای اختصاص امتیاز کیفیت
	شناسه ارائه دهنده الگوریتم کیفیت	۲ بایت	۰ تا $FFFF_{HEX}$	شناسه ارائه دهنده الگوریتم کیفیت باید بوسیله IBIA یا دیگر مراجع قانونی تایید صلاحیت شده به عنوان یک سازمان زیست سنجی چارچوب قالب تبادل زیست سنجی متعارف در تطابق با روش های ثبت شناسه ارائه دهنده چارچوب قالب تبادل زیست سنجی متعارف در استاندارد ISO/IEC 19785-2 ثبت شود.یک ارزش تماماً صفر باید نشان دهد که ارزش این فیلد گزارش نشده است.
	شناسه الگوریتم کیفیت	۲ بایت	۰ تا $FFFF_{HEX}$	شناسه الگوریتم کیفیت باید بوسیله IBIA یا دیگر مراجع قانونی تایید صلاحیت شده به عنوان یک سازمان زیست سنجی چهارچوب قالب تبادل زیست سنجی متعارف در تطابق با روش های ثبت شناسه ارائه دهنده چهارچوب قالب تبادل زیست سنجی متعارف در استاندارد ISO/IEC 19785-2 ثبت شود.یک ارزش تماماً صفر باید نشان دهد که ارزش این فیلد گزارش نشده است.

امتیاز کیفیت- ۱ بایت- امتیاز کیفیت همان گونه که در استاندارد ISO/IEC 29794-1 تعریف شده باید بیان کننده ارزش نمایش تصدیق پیش بینی شده یک نمونه زیست سنجی باشد.مقادیر معتبر برای امتیاز کیفیت اعداد صحیح بین ۰ تا ۱۰۰ می باشند که مقادیر بالاتر نشانگر کیفیت بیشتر می باشد.ارزش ۲۵۵ برای به کار بردن یک موقعیت ویژه می باشد.یک ورودی ۲۵۵ باید تلاش مردود جهت محاسبه امتیاز کیفیت را نشان دهد.این ارزشامتیاز کیفیت با استاندارد ISO/IEC 19784-1 که درآن ۲۵۵ برابر با عدد ۱- است، متناسب و هم آهنگ می باشد.

یادآوری۱- BioAPI برخلاف استاندارد ISO/IEC19794 از عدد صحیح علامت دار استفاده می کند.

شناسه ارائه دهنده الگوریتم کیفیت -۲ بایت. برای توانمندسازی دریافت کننده امتیاز کیفیت به منظور تفاوت قائل شدن بین امتیازهای کیفیت تولید شده توسط الگوریتم های مختلف، تهیه کننده امتیازهای کیفیت باید به طور منحصر به فرد توسط یک فیلد دو بایتی شناخته شود.این امتیاز کیفیت توسط IBIA یا دیگر مراجع قانونی تاییدصلاحیت شده شده ثبت شده است.

شناسه الگوریتم کیفیت -۲ بایت. رمز محصول به صورت عدد صحیح که توسط ارائه دهنده الگوریتم کیفیت اختصاص یافته است، را مشخص می‌کند.این رمز مشخص می‌کند که کدام الگوریتم ارائه دهنده در محاسبه امتیاز کیفیت مورد استفاد قرار گرفته است و بهتر است در محدوده ۱ تا ۶۵۵۳۵ قرار گیرد.

یادآوری ۲- امتیازهای کیفیت چندگانه محاسبه شده با الگوریتم یکسان (شناسه ارائه دهنده و شناسه الگوریتم)نباید در یک نمایش منحصر، ارائه شوند.

جدول ۶- عناصر سرآیند نمایش نشانه/امضاء پردازش شده پویا

شرح	طول	مقادیر معتبر	ملاحظات
ارزش مقیاس x	۲ بایت	نما ۰×۱F تا ۰×۰ کسر ۰×۷FF تا ۰×۰	یک ارزش مقیاس X باید شامل ۲ بایت باشد.۵ بیت با بیشترین ارزش در اولین بایت باید توان (نما) فیلد E را تشکیل دهد و ۱۱ بیت باقیمانده باید کسر فیلد F را تشکیل دهد. قسمت نمایی فیلد E شامل یک عدد صحیح بدون علامت، نشان دهنده پایه ۲ نمایی ارزش مقیاس است که به ۱۶ متمایل می شود.برای توان، مقادیر صحیح علامت دار در محدوده ۱۶- تا ۱۵ مجاز می باشد.برای به رمز در آوردن ارزش توان ،باید ۱۶ را جهت بدست آوردن ارزش بدون علامت اضافه کرد.برای از رمز درآوردن ارزش توان ،۱۶ بایستی از محتوای E کاسته شود. قسمت کسری فیلد E ، شامل قسمت بیت (در نمادسازی دودویی) است که در سمت راست ممیز دودویی رقم اعشاری ارزش مقیاس قرار می گیرد.اعشار باید در محدوده ۲> مانتیس≤ ۱ مقیاس گذاری شود. $s = \left[1 + \frac{F}{2^{11}}\right] \cdot 2^{E-16}$ ارزش مقیاس گذاری دارای محدوده 2^{-16} تا 2^{15} (۱+ ۲۰۴۷/۲۰۴۸) است. برای مثال از ۰/۰۰۰۰۱۵۲۵۸۷۸۹۰۶۲۵ تا ۶۵۵۲۰ مثال : زمانیکه $E=16$ و $F=0$آنگاه $S=1$ می باشد. در صورت ناشناخته بودن ، ارزش مقیاس بر روی HEX ۰۰ تنظیم می شود.
ارزش مقیاس Y	۲ بایت	نما ۰×۱F تا ۰×۰ کسر ۰×۷FF تا ۰×۰	یک ارزش مقیاس Yباید شامل ۲ بایت باشد.۵ بیت با بیشترین ارزش در اولین بایت باید توان (نما) فیلد E را تشکیل دهد و ۱۱ بیت باقیمانده باید کسر فیلد F را تشکیل دهد. قسمت نمایی فیلد E شامل یک عدد صحیح بدون علامت ، نشان دهنده پایه ۲ نمایی ارزش مقیاس است که به ۱۶ متمایل می شود .برای توان، مقادیر صحیح علامت دار در محدوده ۱۶- تا ۱۵ مجاز می باشد.برای به رمز در آوردن ارزش توان ،باید ۱۶ را جهت بدست آوردن ارزش بدون علامت اضافه کرد.برای از رمز درآوردن ارزش توان ،۱۶ بایستی از محتوای E کاسته شود. قسمت کسری فیلد E ، شامل قسمت بیت (در نمادسازی دودویی) است که در سمت راست ممیز دودویی رقم اعشاری ارزش مقیاس قرار می گیرد .اعشار باید در محدوده ۲> اعشار≤ ۱ مقیاس گذاری شود. $s = \left[1 + \frac{F}{2^{11}}\right] \cdot 2^{E-16}$ ارزش مقیاس گذاری دارای محدوده 2^{-16} تا 2^{15} (۱+ ۲۰۴۷/۲۰۴۸) است. برای مثال از ۰/۰۰۰۰۱۵۲۵۸۷۸۹۰۶۲۵ تا ۶۵۵۲۰ مثال : زمانیکه $E=16$ و $F=0$آنگاه $S=1$ می باشد. در صورت ناشناخته بودن ، ارزش مقیاس بر روی HEX ۰۰ تنظیم می شود.

جدول ۶- عناصر سرآیند نمایش نشانه/امضاء پردازش شده پویا- ادامه

شرح	طول	مقادیر معتبر	ملاحظات
ارزش مقیاس T	۲ بایت	نما ۰×۱F تا ۰×۰ کسر ۰×۷FF تا ۰×۰	یک ارزش مقیاس T باید شامل ۲ بایت باشد.۵ بیت با بیشترین ارزش در اولین بایت باید توان (نما) فیلد E را تشکیل دهد و ۱۱ بیت باقیمانده باید کسر فیلد F را تشکیل دهد. قسمت نمایی فیلد E شامل یک عدد صحیح بدون علامت، نشان دهنده پایه ۲ نمایی ارزش مقیاس است که به ۱۶ متمایل می شود .برای توان، مقادیر صحیح علامت دار در محدوده ۱۶- تا ۱۵ مجاز می باشد.برای به رمز در آوردن ارزش توان ،باید ۱۶ را جهت بدست آوردن ارزش بدون علامت اضافه کرد.برای از رمز درآوردن ارزش توان ،۱۶ بایستی از محتوای E کاسته شود. قسمت کسری فیلد E ، شامل قسمت بیت (در نمادسازی دودویی) است که در سمت راست ممیز دودویی رقم اعشاری ارزش مقیاس قرار می گیرد اعشار باید در محدوده ۲> اعشار≤ ۱ مقیاس گذاری شود. $s = \left[1 + \frac{F}{2^{11}}\right] \cdot 2^{E-16}$ ارزش مقیاس گذاری دارای محدوده 2^{-16} تا 2^{15} (۱+ ۲۰۴۷/۲۰۴۸) است. برای مثال از ۰/۰۰۰۰۱۵۲۵۸۷۸۹۰۶۲۵ تا ۶۵۵۲۰ مثال : زمانیکه *E=16* و *F=0*آنگاه *S=1* می باشد. در صورت ناشناخته بودن ، ارزش مقیاس بر روی *HEX* ۰۰ تنظیم می شود.
ارزش مقیاس F	۲ بایت	نما ۰×۱F تا ۰×۰ کسر ۰×۷FF تا ۰×۰	یک ارزش مقیاس F باید شامل ۲ بایت باشد.۵ بیت با بیشترین ارزش در اولین بایت باید توان (نما) فیلد E را تشکیل دهد و ۱۱ بیت باقیمانده باید کسر فیلد F را تشکیل دهد. قسمت نمایی فیلد E شامل یک عدد صحیح بدون علامت ، نشان دهنده پایه ۲ نمایی ارزش مقیاس است که به ۱۶ متمایل می شود. برای توان، مقادیر صحیح علامت دار در محدوده ۱۶- تا ۱۵ مجاز می باشد.برای به رمز در آوردن ارزش توان ،باید ۱۶ را جهت بدست آوردن ارزش بدون علامت اضافه‌کرد.برای از رمز درآوردن ارزش توان ،۱۶ بایستی از محتوای E کاسته شود. قسمت کسری فیلد E، شامل قسمت بیت (در نمادسازی دودویی) است که در سمت راست ممیز دودویی رقم اعشاری ارزش مقیاس قرار می گیرد .اعشار باید در محدوده ۲> اعشار≤ ۱ مقیاس گذاری شود. $s = \left[1 + \frac{F}{2^{11}}\right] \cdot 2^{E-16}$ ارزش مقیاس گذاری دارای محدوده 2^{-16} تا 2^{15} (۱+ ۲۰۴۷/۲۰۴۸) است. برای مثال از ۰/۰۰۰۰۱۵۲۵۸۷۸۹۰۶۲۵ تا ۶۵۵۲۰ **مثال** : زمانیکه *E=16* و *F=0*آنگاه *S=1* می باشد. در صورت ناشناخته بودن ، ارزش مقیاس بر روی *HEX* ۰۰ تنظیم می شود.

جدول ۶- عناصر سرآیند نمایش نشانه/امضاء پردازش شده پویا- ادامه

شرح	طول	مقادیر معتبر	ملاحظات
تعداد رکوردهای داده رویداد پویا	۴ بایت	۰×۱ تا ۰×FFFFFFFF	تعداد رکوردهای داده رویداد- پویا بایستی تعداد کل رکوردهای داده پویا در نمایش نشانه/امضاء را نشان دهد.
تعداد نمونه ها برای جابجایی فیلتر میانگین	۱ بایت	۰×۱ تا ۰×FF	تعداد نمونه ها برای جابجایی میانگین. M باید یک عدد فرد باشد. $Qi = \frac{1}{M} \sum_{m=-\frac{M-1}{2}}^{\frac{M-1}{2}} Q\,i + m$

۸-۴ بدنه نمایش

هر رویداد نشانه/امضاء باید از داده رویداد پویا که ثبت شده و در جدول شماره ۷ تشریح شده، منتج شود.بنابراین نقاط برگشت درصفحات X، Y ثبت شده می‌باشند.(اگر داده در دسترس باشد حتی درصورت عدم تماس قلم با صفحه نوشتن)،رویداد های بالا رفتن قلم و پایین بردن قلم ثبت می‌شوند و در صورت اعمال فشار آنگاه نقاط برگشت در F به صورت اختیاری ثبت می شوند.

جدول ۷ – رکورد داده رویداد پویا

شرح	طول	مقادیر معتبر	ملاحظات
X	۲ بایت	۰×۰ تا ۰×FFFF	مختصات X باید در ۲ بایت ثبت شود.مقادیر عدد صحیح در محدوده ۳۲۷۶۸- تا ۳۲۷۶۷ مجاز می باشند.این مقادیر باید با عدد صحیح بدون علامت بعد از اضافه کردن عدد ۳۲۷۶۸ به هر ارزش به رمز درآورده شود.بنابراین برای اعداد غیرمنفی، بیت ۸ از بزرگترین بایت دارای ارزش ۱ می باشد و برای اعداد منفی، بیت ۸ از بزرگترین بایت دارای ارزش صفر است.برای خارج سازی از حالت رمز این مقادیر، عدد ۳۲۷۶۸ باید از ارزش هر رکورد کاسته شود.
Y	۲ بایت	۰×۰ تا ۰×FFFF	مختصات Y باید در ۲ بایت ثبت شود.مقادیر عدد صحیح در محدوده ۳۲۷۶۸- تا ۳۲۷۶۷ مجاز می باشند.این مقادیر باید با عدد صحیح بذون علامت بعد از اضافه کردن عدد ۳۲۷۶۸ به هر ارزش به رمز درآورده شود.بنابراین برای اعداد غیرمنفی، بیت ۸ از بزرگترین بایت دارای ارزش ۱ می باشد و برای اعداد منفی، بیت ۸ از بزرگترین بایت دارای ارزش صفر است.برای خارج سازی از حالت رمز این مقادیر، عدد ۳۲۷۶۸ باید از ارزش هر رکورد کاسته شود.

جدول ۷ – رکورد داده رویداد پویا–ادامه

F	۲ بایت	۰×۰ تا ۰×FFFF	فشار باید در ۲ بایت ثبت شود.مقادیر عدد صحیح در محدوده ۰ تا ۶۵۵۳۵ مجاز می باشند.این مقادیر باید بر مبنای عدد صحیح بدون علامت به رمز درآورده شود. اگر فشار اندازه گیری نشود، مقادیر بر روی صفر تنظیم می شوند.
T	۲ بایت	۰×۰ تا ۰×FFFF	فشار باید در ۲ بایت ثبت شود.مقادیر عدد صحیح در محدوده ۰ تا ۶۵۵۳۵ مجاز می باشند.این مقادیر باید بر مبنای عدد صحیح بدون علامت به رمز درآورده شود.
نوع رویداد	۱ بایت	۰×۰ تا ۰×۱ F	نوع رویداد باید در یک بایت ثبت شود که در آن: بیت شماره ۱: بالابردن قلم بیت شماره ۲ : پایین بردن قلم بیت شماره ۳ : نقاط برگشت X بیت شماره ۴: نقاط برگشت Y بیت شماره ۵ : نقاط برگشت F بیت شماره ۶ : نوع نقاط برگشت X بیت شماره ۷ : نوع نقاط برگشت Y بیت شماره ۸ : نوع نقاط برگشت F زمانیکه هر رویداد اتفاق می افتد باید با ارزش ۱ به رمز درآورده شود.برای نقاط برگشت ، نوع نقاط برگشت برای نوع ۱ باید با ارزش صفر و برای نوع ۲ با ارزش یک به رمز درآورده شود.

جدول ۸ - خصیصه کلی داده

شرح	طول	مقادیر معتبر	ملاحظات
زمان کل	۲ بایت	۰×۰ تا ۰×FFFF	زمان کل باید در ۲ بایت ثبت شود.مقادیر عدد صحیح در محدوده ۰ تا ۶۵۵۳۵ مجاز می باشند.این مقادیر باید بر مبنای عدد صحیح بدون علامت به رمز درآورده شود.
X_{mean}	۲ بایت	۰×۰ تا ۰×FFFF	میانگین X باید در ۲ بایت ثبت شود.مقادیر عدد صحیح در محدوده ۳۲۷۶۸- تا ۳۲۷۶۷ مجاز می باشند.این مقادیر باید با عدد صحیح بذون علامت بعد از اضافه کردن عدد ۳۲۷۶۸ به هر ارزش به رمز درآورده شود.بنابراین برای اعداد غیرمنفی، بیت ۸ از بزرگترین بایت دارای ارزش ۱ می باشد و برای اعداد منفی، بیت ۸ از بزرگترین بایت دارای ارزش صفر است.برای خارج سازی از حالت رمز این مقادیر، عدد ۳۲۷۶۸ باید از ارزش هر رکورد کاسته شود.

جدول ۸ - خصیصه کلی داده –ادامه

Y_{mean}	۲ بایت	۰×۰ تا ۰×FFFF	میانگین Y باید در ۲ بایت ثبت شود.مقادیر عدد صحیح در محدوده ۳۲۷۶۸- تا ۳۲۷۶۷ مجاز می باشند.این مقادیر باید با عدد صحیح بدون علامت بعد از اضافه کردن عدد ۳۲۷۶۸ به هر ارزش به رمز درآورده شود.بنابراین برای اعدادغیرمنفی ،بیت ۸ از بزرگترین بایت دارای ارزش ۱ می باشد و برای اعداد منفی، بیت ۸ از بزرگترین بایت دارای ارزش صفر است.برای خارج سازی از حالت رمز این مقادیر، عدد ۳۲۷۶۸ باید از ارزش هر رکورد کاسته شود.
F_{mean}	۲ بایت	۰×۰ تا ۰×FFFF	فشار میانگین باید در ۲ بایت ثبت شود.مقادیر عدد صحیح در محدوده ۰ تا ۶۵۵۳۵ مجاز می باشند.این مقادیر باید بر مبنای عدد صحیح بدون علامت به رمز درآورده شود.
انحراف استاندارد X	۲ بایت	۰×۰ تا ۰×FFFF	انحراف استاندارد X باید در ۲ بایت ثبت شود.مقادیر عدد صحیح در محدوده ۰ تا ۶۵۵۳۵ مجاز می باشند.این مقادیر باید بر مبنای عدد صحیح بدون علامت به رمز درآورده شود.
انحراف استاندارد Y	۲ بایت	۰×۰ تا ۰×FFFF	انحراف استاندارد Y باید در ۲ بایت ثبت شود.مقادیر عدد صحیح در محدوده ۰ تا ۶۵۵۳۵ مجاز می باشند.این مقادیر باید بر مبنای عدد صحیح بدون علامت به رمز درآورده شود.
انحراف استاندارد F	۲ بایت	۰×۰ تا ۰×FFFF	انحراف استاندارد F باید در ۲ بایت ثبت شود.مقادیر عدد صحیح در محدوده ۰ تا ۶۵۵۳۵ مجاز می باشند.این مقادیر باید بر مبنای عدد صحیح بدون علامت به رمز درآورده شود.
ضریب همبستگی	۲ بایت	۰×۱ تا ۰×FFFF	ضریب همبستگی باید در ۲ بایت ثبت شود.مقادیر عدد صحیح در محدوده ۰ تا ۶۵۵۳۵ مجاز می باشند.این مقادیر باید بر مبنای عدد صحیح بدون علامت به رمز درآورده شود.

۸- ۶ داده گسترش یافته

فیلد طول داده گسترش یافته باید تعداد بایت های محتوی در فیلد داده گسترش یافته اختیاری‌را نمایش دهد. فیلد طول بایستی شامل۲بایت بوده ونمایشگر تعداد بایت های محتوی بعدی با عدد صحیح بدون علامت باشد.مقادیر در محدوده ۰ تا ۶۵۵۳۵ مجاز می باشند.

فیلد داده گسترش یافته اختیاری که می‌تواند توسط الگوریتم مقایسه استفاده شود،مجاز به برخورداری از داده اضافی می باشد.ساختار فیلد داده گسترش یافته شده توسط این استاندارد تعیین نمی‌شود.اگر داده گسترش یافته موجود باشد والگوریتم مقایسه قالب آن را تشخیص ندهد آنگاه الگوریتم باید از آن صرف نظر کند.

یادآوری- الگوریتم های مقایسه مورد ادعا که برای انطباق بلوک های داده با قالب های استاندارد ISO/IEC 19794 مورد استفاده قرار می گیرد بهتر است توانایی دستیابی به کارایی زیست سنجی یکسان را در رابطه با نرخ های خطا هنگام پردازش بلوک های داده بدون وجود داده های طویل و در زمان پردازش بلوک های داده با وجود داده های طویل، داشته باشند.اگر داده طویل موجود باشد و الگوریتم مقایسه به آن نیاز نداشته باشد آنگاه الگوریتم باید از آن صرف نظر کند.

پیوست الف

(الزامی)

روش شناسی آزمون انطباق

این استاندارد قالب تبادل داده زیست سنجی برای ذخیره سازی، ثبت و انتقال یک یا تعداد بیشتری نمایش نشانه/امضاء را تعیین می‌کند.هر نمایش با یک ابرداده[1] کیفیت ویژه که دریک رکورد سرآیند قرار دارد ضمیمه می باشد.این پیوست آزمون هایی برای بررسی صحت رکورد ارائه می نماید.

اهداف این استاندارد تا زمان آزمون شدن محصولات زیست سنجی در جهت تعیین انطباق با ویژگی های آنها به صورت کامل قابل دستیابی نمی باشد.پیاده سازی انطباق یک پیش نیاز الزامی برای دستیابی به قابلیت عملکرد داخلی در میان اجرا می باشد.

بیانیه آزمون،الزامات استاندارد ISO/IEC19794 را به کاربردی ترین حالت پوشش می دهد.بنابراین نتایج انطباق بوجود آمده توسط فیلدهای‌آزمون، درجه واقعی انطباق پیاده سازی را برای رکوردهای قالب تبادل داده استاندارد ISO/IEC19794 را منعکس می سازد.این یک محرک برای توسعه روش شناسی آزمون انطباق می باشد.

هدف این پیوست الزامی تعیین عناصر روش شناسی آزمون انطباق، بیانیه های آزمون و روش های آزمون در صورت کاربرد با این استاندارد می باشد. برای ویرایش این استاندارد محتوای این پیوست تحت عنوان یک سند مجزا برای تکمیل این استاندارد در دسترس می باشد(اصلاحیه).

1 - Metadata

پیوست ب
(اطلاعاتی)
ویژگی های ASN.1 قالب داده

ب-۱) خلاصه تحلیل [1]رمزگذاری داده نشانه/امضاء پردازش شده پویا

این استاندارد تمام نمایش‌های سطح بیت قالب رکورد تبادل داده زیست سنجی نشانه/امضاء پردازش شده داده پویا که برای انتقال یا ذخیره سازی مناسب می باشد را تعیین می کند.

اگرچه این استاندارد برای تعاریف محتوای اطلاعات این قالب به صورت مستقل از نمایش های سطح بیت مفید می باشد(خلاصه تحلیل).این استاندارد موارد زیر را ممکن می سازد :

الف - از رمزگذاری های(در جاییکه مناسب باشد) متفاوت استفاده می‌نماید (مثال :رمزگذاری XML)؛

ب- نمایش های مختلف درون هسته [2] مورد استفاده از ساختارهایی برای پردازش آسان با زبان برنامه نویسی C ، C^{++} ویا جاوا استفاده می کند؛

پ- طیف وسیعی از وسایل در پیاده سازی این قالب ها مورد استفاده قرار می‌گیرد؛

ت- نمایش های درون هسته آسانتر بر روی ماشین ها که معماری سخت افزاری big-Endian ندارند؛

ث- یک شرح آسان قابل فهم از مقادیر در قالب ها؛

علم نحو مطلق تعیین شده در این پیوست از ASN.1 (استاندارد ISO 8824-1) استفاده می کند.رمزگذاری استاندارد داده نشانه/امضاء پردازش شده پویا توسط کاربرد قوانین کدگذاریASN.1 بسته بندی شده به دست می آید.(طبق استاندارد ISO 8825-2).رمزگذاری های حاصل با رمزگذاری‌های تعیین شده در بدنه این استاندارد یکسان می باشد.

با استفاده از خلاصه تحلیل به عنوان یک برنامه، ابزارها می توانند بین هر رمزگذاری مقادیر و نمایش‌های درون هسته بر روی هر معماری سخت افزار و برای هر زبان برنامه نویسی تبدیل شوند.به ابزارهایی که این ویژگی ها را به ساختارهای داده زبان برنامه نویسی تبدیل می کنند، کامپایلرهای ASN.1 گفته می شود و توسط جریانهای عادی که بین مقادیردرون هسته و هرنوع رمزگذاری مطلوب در استاندارد ISO 8825 تبدیل می شود، پشتیبانی می گردد(این شامل رمزگذاری هایXML می شود).این ابزارتوسط ارائه دهنده های مختلف پشتیبانی می گردد.به ویژه ابزارهایی که بین رمزگذاری استاندارد داده نشانه/امضاء پردازش شده پویا و نمایش های درون هسته مقادیر تبدیل می شوند برای بیشتر معماری های سخت افزار و بیشتر زبانهای برنامه نویسی در دسترس می باشد.

1- Abstract syntax

2- IN-CORE

ب-۲) قالب داده نشانه/امضاء پردازش شده پویا

```
Signature/signSignDynamicFormatModule
{iso standard 19794 signature/sign-sign-processed-dynamic(11)
modules(0) version(0)}
DEFINITIONS
PER INSTRUCTIONS
-- This specifies that PER Encoding Instructions are to be
applied
AUTOMATIC TAGS ::=
BEGIN
Signature/signSignDynamicBlock ::= SEQUENCE {
header GeneralHeader,
body Body }

GeneralHeader ::= SEQUENCE {
formatId [NULL] IA5String ("SPD"),
standardVersion [NULL] IA5String (SIZE (3)),
-- " 10" (space-one-zero) for this version
lengthofRecord [SIZE 32]INTEGER,
numberofRepresentations [SIZE 16]INTEGER,
certificationFlag [SIZE 8]INTEGER}
Body ::= SEQUENCE {
representation RepresentationHeaderValues,
RepresentationBodyValues}
RepresentationHeaderValues ::= SEQUENCE {
ReprsentationLength [SIZE 32] INTEGER (1..MAX)
captureDateTime CaptureDateTimeValues,
captureDeviceTechId INTEGER (0..255),
captureDeviceVendId INTEGER (0..65535),
captureDeviceTypeId INTEGER (0..65535),
qualityRecord QualityBlockValues,
certificationRecord INTEGER (0),
xchannelScaling ScalingValue,
ychannelScaling ScalingValue,
tchannelScaling ScalingValue,
fchannelScaling ScalingValue,
numberofDynamicEvents [SIZE 32] INTEGER (1..MAX)
numberofAveragingSamples INTEGER (1..255)}
CaptureDateTimeValues ::= OCTETSTRING (SIZE (9))
-- The Octet String shall contain the 9 bytes specified in
ISO/IEC 19794-1
QualityBlockValues ::= SEQUENCE {
numberof Qualityblocks [SIZE 8] INTEGER (0..255),
```

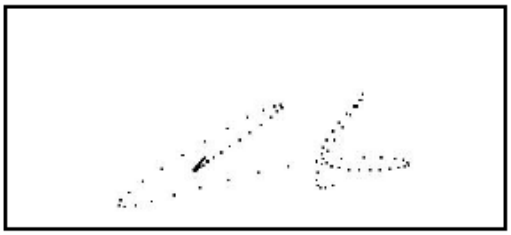
```
SEQUENCE OF {
qualityScore [SIZE 8] INTEGER (0..100,255),
qualityalgorithmVendId [SIZE 16] INTEGER (1..65535),
qualityalgorithmId [SIZE 16] INTEGER (1..65535)} }
ScalingValue ::= SEQUENCE {
exponent INTEGER (-16..15),
fraction INTEGER (0..2047)}
RepesentationBodyValues ::= SEQUENCE {
DynamicEventData,
FeatureData,
extendedData [LENGTH 16] OCTET STRING OPTIONAL}
DynamicEventData ::= SEQUENCE {
xCoordinate INTEGER (-32768..32767),
yCoordinate INTEGER (-32768..32767),
fValue INTEGER (0..65535),
timeValue INTEGER (0..65535)
typeofEvent [SIZE 8] INTEGER (0..255)}
FeatureData ::= SEQUENCE {
totalTime INTEGER (0..65535),
meanValues OverallMeanValues,
sdValues StandardDeviation,
cCoefficient INTEGER (1 65535) }
OverallMeanValues ::= SEQUENCE {
meanX INTEGER (-32768..32767),
meanY INTEGER (-32768..32767),
meanF INTEGER (0 65535) }
StandardDeviation ::= SEQUENCE {
sdX INTEGER (0 65535),
sdY INTEGER (0 65535),
sdF INTEGER (0 65535) }
END
```

پیوست پ
(اطلاعاتی)
نشانه/امضاهای مناسب برای کاربرد احراز هویت

محتوای داده یک نشانه/امضاء آن را برای سندیت مناسب می سازد.بنابراین‌کدام جنبه نشانه/امضاء است که‌می تواند جهت اطمینان از مناسب بودن محتوای داده مورد اندازه گیری قرار گیرد؟
سه جنبه شناخته شده جهت تهیه یک شاخص خوب به شرح زیر می باشد:
۱- کمیت داده؛
۲- پیچیدگی نشانه/امضاء ؛
۳- سازگاری نشانه/امضاء ؛

پ.۱) کمیت داده

آیا تعداد مناسبی از مختصات رقمی شده برای تجزیه و تحلیل وجود دارد؟این جنبه کمیت می‌تواند به درجه تفکیک پذیری رقمی کننده مرتبط باشد اما مهمتر اینکه به سرعت نوشتن نشانه/امضاء توسط انسان مرتبط است.اگر این سرعت زیاد باشد، مختصات ناکافی در نتیجه اطلاعات ناکافی برای تجزیه وتحلیل ثبت می شود.به طور نوعی از نشانه های افراد همراه با حروف نخستین نام خانوادگی به صورت سریع ناشی می شود.با وجود داده های عددی ناکافی جهت راه اندازی الگوریتم های تحلیل نشانه/امضاء پویا، حروف نخستین ممکن است به اندازه کافی پیچیده و خیلی سازگار باشند.بنابراین بهتر است این قبیل نشانه/امضاء در مرحله ثبت نام، رد شوند.این یک محدودیت مشابه در سیستم های احرازهویت رمز عبوری با حداقل تعداد رقم می باشد.برای مثال ۷ یا ۸ تلاش جهت اطمینان از سطح کافی امنیت



شکل پ.۱ – مثالی از یک نشانه/امضاء که به اندازه کافی پیچیده می باشد اما ارزش داده ناکافی است .

کمیت داده به عنوان یک ابزار اندازه گیری مناسب به راحتی توسط شمارش تعداد نقاط رقمی ثبت شده و اطمینان از بالاتر بودن از حداقل قابل قبول، اندازه گیری می شود.

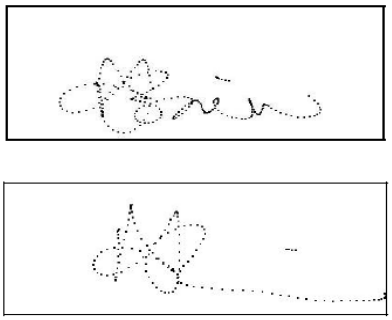
پ.۲)پیچیدگی نشانه/امضاء

چرا به پیچیدگی نشانه/امضاء اهمیت می دهیم؟هرچند تجزیه وتحلیل پویایی های نشانه /امضاء جعل اسناد را مشکل می سازد اما هنوز نیاز به داده با پیچیدگی کافی جهت توسعه احتمالات پویایی وجود دارد.این به چه معنا

می باشد؟پیچیدگی نشانه/امضاء می‌تواند به این صورت باشد که سیستم های تصدیق،کاربرها را از انتخاب کدهای ساده مثل ۱۲۳۴یا ۹۹۹۹ به دلیل ساده و قابل حدس بودن منصرف کند و یا کلمه عبورهایی مثل کاراکترهای حرفی با حروف بزرگ و حروف کوچک و برخوردار از اعداد و کاراکترهای ویژه باشد.
بنابراین چه چیزی پیچیده می باشد؟توضیح اینکه چه چیزی ساده می باشد آسانتر می باشد.
همه افراد ساده بودن یک ضربدر را قبول دارند حتی با تحلیل های پویا یک "علامت" یا نشانه/امضاء به راحتی جعل می شود و بنابراین امنیت پایین را در یک سیستم تصدیق ارائه می کند.چیزی که نشانه/امضاء را پیچیده می سازد حلقه‌ها هستند.این حلقه‌ها هستند که تنوع پویایی را تضمین می‌کنند وگوناگونی سرعت، شتاب،کاهش سرعت، بردار را به وجود می آورد.یک ضربدرساده فاقد داده حلقه یا تعداد کمی داده حلقه می باشد بنابراین درجه پویایی بسیار کم وپیچیدگی ناکافی می باشد.پیچیدگی ناکافی در یک سیستم تصدیق به صورت ایمن مورد توجه قرار می‌گیرد.بنابراین بهتراست این قبیل نشانه/امضاء در مرحله ثبت نام پذیرفته نشود.اندازه گیری مناسب به راحتی توسط شمارش تعداد حلقه های ثبت شده و اطمینان از بیشتر بودن از حداقل قابل قبول، اندازه گیری می شود.

پ.۳) سازگاری نشانه /امضاء

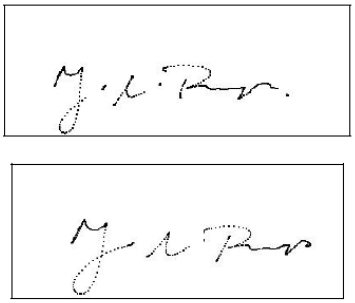
دلیل بررسی سازگاری نشانه/امضاء یک فرد چیست؟ مطمئناً تمام نقاط هر سیستم زیست سنجی نشانه/امضاء قابل اجرا جایی است که از عهده تنوع نشانه های فرد برآید.هرسیستم زیست سنجی نشانه/امضاء کاربردی باید از عهده تغییرات طبیعی نشانه های هر فرد برآید.هرچند بهتر است هر سیستم نشانه/امضاء زیست سنجی اطمینان دهد که تنوع تحلیل های حاصل، نشانه/امضاء زیست سنجی یک فرد را جهت بهره برداری توسط افراد دغل باز به صورت آزاد قرار نمی‌دهد.این تغییرات زیاد سطح امنیت را به گونه ای پایین می آورد که به جعل کننده‌ای ضعیف، این اجازه را خواهد داد تا به طور نادرست مورد قبول واقع گردد.
به طور یکسان بهتر است هر سیستم نشانه/امضاء همکاری ثبت نام را اجبار نماید یا کاربر را بدون همکاری در حین ثبت نام،نپذیرد.آشکاراست‌که‌کسی‌که نمایش‌های ثبت‌نام نشانه/امضاء مثل "fred"، "john"، "bill"،"jack" را تهیه می کند بهتر است در مرحله ثبت نام پذیرفته نشود.تبدیل این قبیل‌اسامی به نشانه /امضاء ناسازگار می باشد.آنها تنوع بسیار زیادی در خارج از توزیع نرمال قابل انتظاراز تنوع نشانه/امضاء دارند.
این توزیع نرمال است که‌درمرکز برقراری سازگاری یک نشانه/امضاء قرار می‌گیرد.هرخصیصه پویای یک نشانه/امضاء از یک توزیع نرمال پیروی می کند.توصیه می شود هر نشانه/امضاء دارای خصیصه های پویای‌کافی (که به صورت خوشه درآمده اند) جهت اطمینان از یگانگی آن باشند تا فرصت لازم برای تایید شدن در یک سیستم تصدیق را به دست آورد. اگر تعداد بسیار زیادی از خصیصه های پویا اندازه گیری شود و تحلیل ها بسیار متنوع باشند ویا خوشه بندی ناکافی باشد آنگاه بهتراست نشانه/امضاء ناسازگار فرض شود یا در مرحله ثبت نام بسیار متنوع درنظرگرفته شود.برای مجاز بودن این چنین نشانه/امضایی جهت تکمیل ثبت نام به گونه ای که نشانه /امضاء کاربر قابل بهره برداری توسط دغل بازان باشد، سیستم زیست سنجی در عین حال می تواند حتی با وجود نشانه/امضاهای متفاوت، با موافقت آنها از عهده آن برآید.



شکل پ.۲ – مثال نشانه /امضاء یکسان با تغییر پذیری قابل توجه

اگر تنها یک یا دو نشانه/امضاء متنوع قابل توجه در تمامی نشانه/امضاهای ارائه شده در طول ثبت نام وجود داشته باشد آنگاه آنها می توانند به طور فردی به عنوان الگوهای پرت[1] مورد پذیرش قرار نگیرند.اگر تمام یا اکثریت نمایش‌های نشانه/امضاء ناسازگاری بسیار زیادی را بیان کنند آنگاه بهتر است نشانه/امضاء به عنوان"بسیار تغییر پذیر" مردود گردد.

سازگاری نشانه/امضاء سخت‌ترین اندازه‌گیری کیفیت می باشد زیرا مسئله مهم توازن بین قابلیت استفاده وامنیت می‌باشد.برای مثال توازن تعداد نمایش های نشانه/امضاء گرفته شده از کاربر در واحد زمان جهت ثبت نام‌همراه با همکاری پیوسته کاربر.اگرچه یک کاربر در طول ثبت نام ممکن است توانایی عدم پذیرش یک نمایش ویژه را به دلیل خارج از حالت عادی بودن‌داشته باشد، تجربه در آزمایش ها نشان می دهد به صورت نادراین کار انجام می شود.



شکل ۳.پ) مثال نشانه/امضاء با ۲ کیفیت

همکاری واقعی کاربر برای کیفیت مناسب ثبت نام لازم می باشد و به کاربران این اطمینان را خواهد داد که نیاز به وجود آنها جهت توسعه یک نشانه/امضاء سازگار با پیچیدگی کافی را درک کنند.کمیت داده یک عنصر مهم وقابل توجه ساختار کاربر در هر سیستم زیست سنجی نشانه/امضاء می باشد.

1- Outliers

کتاب شناسی

ISO/IEC 8824-1, *Information technology — Abstract Syntax Notation One (ASN.1): Specification of basic notation*

ISO/IEC 8825-2, *Information technology — ASN.1 encoding rules: Specification of Packed Encoding Rules (PER)*

ISO/IEC 8825-6, *Information technology — ASN.1 encoding rules: Registration and application of PER encoding instructions*

ISO/IEC 19794-7, *Information technology — Biometric data interchange formats — Part 7: Signature/sign time series data*