بررسی کارآیی الگوریتم SIFT در تشخیص اثرانگشت پنهان شده در تراکنش‌های تجارت الکترونیک

مریم زارع زاده[1]، محمد علی دوستاری[2]، الهام زارع زاده[3]
۱ کارشناسی ارشد مهندسی فناوری اطلاعات، دانشگاه شاهد، m.zarezadeh@shahed.ac.ir
۲ استادیار گروه مهندسی کامپیوتر، دانشگاه شاهد
۳ کارشناسی ارشد مهندسی کامپیوتر، دانشگاه علم و هنر یزد
تاریخ دریافت: ۹۳/۲/۲۷ تاریخ پذیرش: ۹۳/۵/۵

چکیده

تجارت الکترونیک نتیجه گسترش و جهانی شدن فناوری اطلاعات، در تمام عرصه‌های زندگی بشری است. حفظ امنیت داده‌ها و حریم خصوصی افراد، نقش مهمی در تقویت تجارت الکترونیک ایفا می‌کنند. فناوری بیومتریک، به عنوان راه‌حلی برای تصدیق هویت افراد در تراکنش‌های تجارت الکترونیک به کار می‌رود. اما سرقت اطلاعات بیومتریک به عنوان مسئله چالش برانگیز، مطرح است. ارسال داده محرمانه به همراه اثرانگشت، می‌تواند از چنین وضعیتی خودداری کند. در این مقاله ابتدا به کمک رمزنگاری RSA و دیفی-هلمن، داده محرمانه، رمز شده و در تصویر اثرانگشت، پنهان‌نگاری شده است. سپس با به‌کارگیری الگوریتم SIFT، به استخراج نقاط متناظر در دو مجموعه داده تصاویر اثرانگشت حاصل از پنهان‌نگاری و تصویر اولیه، خواهیم پرداخت تا میزان کارایی این توصیفگر در تطابق اثرانگشت بررسی گردد. نتایج نشان داده‌اند که الگوریتم SIFT، به ترتیب به میزان ۸۸/۲۳ درصد و ۹۶/۱۵ درصد تطابق صحیح، داشته است. بنابراین با پنهان‌نگاری داده محرمانه در اثرانگشت، علاوه بر اینکه دسترسی افراد مجاز به اطلاعات بیومتریک فراهم می‌شود، کیفیت تصاویر مربوطه نیز تغییر چندانی نخواهد کرد.

کلیدواژه

بیومتریک، اثرانگشت، الگوریتم SIFT، تجارت الکترونیک.

مقدمه

تجارت الکترونیک انجام فعالیت‌های تجاری از طریق شبکه‌های الکترونیکی می‌باشد که با هدف نهایی یک مبادله صورت گیرند. در واقع، تجارت الکترونیک شامل تراکنش‌هایی است که به واسطه آن‌ها، اطلاعات تجاری مربوط به محصولات و خدمات مبادله می‌شوند. در این تعاملات، محافظت از داده‌ها و اطلاعات شخصی افراد در تجارت الکترونیک حائز اهمیت می‌باشد. پیشرفت‌های اخیر در فناوری اطلاعات و شبکه‌های ارتباطی، امکان ذخیره و استفاده از حجم زیادی از داده‌های شخصی را افزایش داده است. از سوی دیگر امکان اینکه بخشی از این داده‌ها و اطلاعات شخصی، توسط اشخاص غیرمجاز جعل و یا روی آنها پردازش‌های غیرمجاز صورت پذیرد نیز به همان میزان افزایش یافته است.

یکی از راه‌های شناسایی افراد مجاز به کارگیری سیستم بیومتریک در تجارت الکترونیک است. اصطلاح بیومتریک در اصل از دو واژه یونانی، «زندگی[1]» و «اقدامات[2]» بوده و تحت‌اللفظی به معنی «سنجش زندگی[3]» است. در امنیت شبکه، بیومتریک به تکنیک‌های تصدیق هویت که متکی بر روی ویژگی‌های فیزیکی قابل سنجش و قابل بررسی خودکار هستند، اشاره دارد [۷]. سیستم بیومتریک، سیستمی است که از طریق آن می‌توان تشخیص داد که کدام فرد با توجه به ویژگی‌های خود است. سیستم بیومتریک، مسئله اساسی در تراکنش‌های تجارت الکترونیک که شامل امنیت، شناسایی[4] و تأیید[5] می‌باشد را حل می‌کند [۸]. هر اطلاعات بیومتریک که می‌تواند بین افراد، تفکیک قائل شود، به عنوان روش بیومتریک مدنظر است. باید اطلاعات بیومتریک دارای ویژگی‌های زیر باشند [۷].

جامعیت[6]: باید تمام افراد با اطلاعات بیومتریک، تشخیص داده شوند.

منحصر به فرد بودن[7]: این اطلاعات تا جایی که امکان دارد، برای دو فرد متفاوت باشد.

ثبات[8]: اطلاعات در تمام زندگی افراد، دائمی باشد.

قابلیت جمع‌آوری[9]: می‌توان اطلاعات بیومتریک را به شیوه‌ای آسان، جمع‌آوری کرد.

مقبولیت[10]: امکان استفاده واقعی از اطلاعات بیومتریک، توسط کاربران مربوطه باشد.

از جمله پرکاربردترین اطلاعات بیومتریک در تراکنش‌های تجارت الکترونیک، اثرانگشت می‌باشد. یکی از مسائل به‌کارگیری

1.Bios
2 .Metron
3 .Measurement of life

4. Identification
5 .Verification
6 .Universality
7 .Uniqueness
8 .Permanency
9 .Collectability
10 .Acceptability

اثرانگشت، امکان جعل اثرانگشت است. به بیانی دیگر، به دلیل نامعلوم بودن هویت طرفین مبادله، امکان ارسال اثرانگشت نامعتبر وجود دارد. در این پژوهش، پیشنهاد شده است که به همراه اثرانگشت، داده محرمانه نیز ارسال شود. این داده با الگوریتم رمزنگاری، رمز شده و سپس در تصویر مربوط به اثرانگشت پنهان‌نگاری می‌شود. سپس دریافت‌کننده اثرانگشت با الگوریتم تطبیق SIFT تصاویر متناظر در دو مجموعه تصاویر حاصل از پنهان‌نگاری داده و تصویر اولیه را تطبیق خواهد دهد.

از این رو در مقاله، کارآیی الگوریتم SIFT در تطابق صحیح بررسی گردیده است. مقاله بدین صورت سازماندهی شده است. در ابتدا مروری بر کاربردهای الگوریتم SIFT صورت گرفته است. در ادامه، شیوه پنهان‌نگاری[11] داده رمز شده در تصویر اثرانگشت بررسی خواهد شد. همچنین، به منظور درک بهتر عملکرد الگوریتم SIFT، جزئیات مربوطه تشریح می‌شود. در پایان، مراحل اجرای مربوط به پنهان‌نگاری و عملگر SIFT و همچنین نتایج، بیان می‌شود.

مروری بر کاربردهای الگوریتم SIFT

الگوریتم تبدیل مستقل از مقیاس ویژگی[12] (SIFT)، توسط لو[13] [۱] [۲]، پیشنهاد شده است. الگوریتم SIFT، در استخراج ویژگی‌های ثابت و متمایز، براساس تطابق ویژگی که شامل تشخیص شی[14]، تخمین وضعیت[15]، بازیابی تصویر و غیره می‌باشد، موفق بوده است. تاکنون الگوریتم SIFT، به طور گسترده در مسائل تشخیص شی، تصدیق هویت مبتنی بر بیومتریک و کاربردهایش در تصدیق چهره و تأیید اثرانگشت، مورد مطالعه قرار گرفته است.

پارک[16] و همکاران [۳]، با کمک عملگر SIFT، یک طرح[17] تطابق و نمایش برای اثرانگشت ارائه داده‌اند. در این طرح، نقاط ویژگی SIFT در فضای مقیاس[18]، استخراج شده‌اند.

سپس تطابق براساس اطلاعات الگو، در نزدیکی نقاط ویژگی، با عملگر SIFT صورت گرفته است. در این روش، تطابق اثرانگشت در دو مرحله انجام می‌گیرد. نتایج پژوهش نشان داده است که روش پیشنهادی، نمایش اثرانگشت مبتنی بر جزئیات[19] را تکمیل می‌کند. همچنین ترکیب SIFT و سیستم معمولی مبتنی بر جزئیات، به طور قابل توجهی عملکرد بهتری از هر دو طرح منحصر به فرد خواهد داشت.

چن[20] و مون[21] [۴]، شیوه‌ای نوین برای تصدیق هویت ارائه داده‌اند. محققان، ابتدا SIFT را با هدف تصدیق دست[22]، به کار برده‌اند.

11 .Steganography
12 .Scale Invariant Feature Transformation
13. Lowe
14. Object recognition
15 .Pose estimation
16 .Park
17 .Scheme
18 .Scale space
19 .Minutiae based
20 .Chen
21 .Moom

سپس تطابق نقطه‌وار[23] برای تطابق نقاط کلیدی SIFT و استخراج شده از تصاویر دست، به کار رفته است. در مرحله بعد، یک تکنولوژی سری زمانی[24]، برای داده دو بعدی و به منظور نمایش و تطابق دست بسط داده شده است. نتایج نشان داده‌اند که ترکیب دو شیوه می‌تواند به دقت خوبی در تصدیق هویت دست یابد.

محققان در [۵]، الگوریتمی به منظور تأیید اثرانگشت با استفاده از SIFT ارائه داده‌اند. الگوریتم پیشنهادی از درجه بالایی از خاصیت موازی در لایه منحصر به فرد شبکه عصبی سلولی[25]، بهره‌برداری می‌کند. در این روش، نقاط مشخصه ویژگی SIFT، در فضای مقیاس استخراج شده و براساس اطلاعات الگو در نزدیکی نقاط با عملگر SIFT، تطابق صورت می‌گیرد. نتایج ارزیابی، دقت سیستم تأیید اثرانگشت را نشان می‌دهد.

مولارس[26] و همکاران [۶]، برای استخراج ویژگی از تصاویر دست بدون تماس، دو شیوه‌ی SIFT و ویژگی‌های ترتیبی خط متعامد[27] (OLOF) را بررسی کرده‌اند. براساس نتایج، SIFT برای تصاویر دست بدون تماس بهتر از OLOF، که در اوایل برای تصاویر دست متداول به کار می‌رفته، بهتر عمل می‌کند.

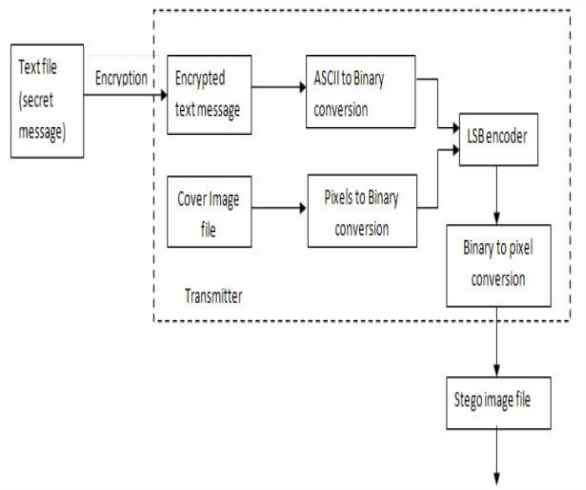
همانطور که مطالعات نشان می‌دهند، الگوریتم SIFT به طور گسترده در تشخیص اطلاعات بیومتریک به کار می‌رود. از این رو در ادامه مقاله، عملکرد الگوریتم SIFT در تشخیص اثرانگشت همراه با داده پنهان‌نگاری شده، ارزیابی می‌شود.

پنهان‌نگاری داده در تصویر اثرانگشت

پنهان‌نگاری، هنر پنهان کردن اطلاعات به طریقی است که از تشخیص پیام‌های محرمانه، خودداری کند. این روش‌ها شامل لینک‌های نامرئی، امضاهای دیجیتالی، گسترش ارتباطات طیف و غیره است. پنهان‌نگاری داده و رمزنگاری، مشابه یکدیگر هستند. رمزنگاری، پیام را به طریقی دستکاری می‌کند که تغییر در پیام درک نشود. در صورتی که پنهان‌نگاری داده، پیام را مخفی کرده تا دیده نشود. به عبارتی یک پیام رمز شده، ممکن است در طرف گیرنده ایجاد تردید کند. در حالی که پیامی که با شیوه‌های پنهان‌نگاری ایجاد شده، غیر قابل مشاهده است [۹].

روش‌های مختلف پنهان‌نگاری داده مطرح شده است. از جمله این روش‌ها، روش بیت کم ارزش[28] (LSB) است. در این روش، بیت کم اهمیت را با بیت داده جایگزین می‌کند. روش LSB، یکی از مهم‌ترین و متداول‌ترین روش‌ها در پنهان‌نگاری تصاویر می‌باشد. فرآیند پنهان‌نگاری با روش LSB در شکل ۱، نمایش داده شده است [۱۰].

22. Palmprint Authentication
23 .Point-wise matching
24 .Time series technology
25 .Cellular Neural Network
26 .Morales
27 .Orthogonal Line Ordinal Features
28 .Least Signifcant Bit



شکل ۱. فرآیند پنهان‌نگاری با روش LSB [۱۰].

روش LSB در برابر نهان‌کاوی[۲۹] آسیب‌پذیر است. بنابراین قبل از جایگزین کردن داده، ابتدا داده با الگوریتم رمزنگاری، رمز شده و سپس در تصویر تعبیه خواهد شد. هر چند رمزنگاری، پیچیدگی زمان را افزایش می‌دهد، اما امنیت بهبود خواهد یافت. به منظور امنیت بالاتر، داده‌های رمز شده که به فرمت اسکی بوده به فرمت دودویی تبدیل می‌شوند. همچنین به طور همزمان، پیکسل‌های تصویر به فرمت دودویی تبدیل خواهند شد. سپس کد کننده LSB، مقادیر LSB پیکسل را با داده‌های رمز شده، جایگزین می‌کند. تصویر تغییر داده شده، به اصطلاح تصویر پوشش[۳۰]، نامیده می‌شود [۱۰].

الگوریتم SIFT

به طور کلی مراحل استفاده از توصیفگر SIFT به ۴ بخش زیر تقسیم می‌شود [۲].

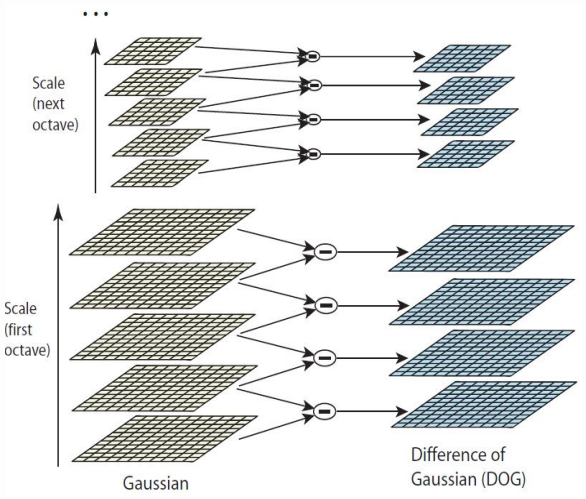
الف. ایجاد فضای مقیاس[۳۱]:

مرحله اول، یافتن نقاط کلیدی است. در این روش از کرنل گوسی، که به عنوان بهترین کرنل برای فضای مقیاس در تصاویر است، استفاده می‌شود. فضای مقیاس، حاصل کانولوشن تصویر $I(x,y)$ با یک تابع مقیاس متغیر گوسی $G(x,y)$ است و با $L(x,y)$ نمایش داده می‌شود. فرآیند یافتن این نقاط، با ساخت یک هرم از تصاویر و ایجاد یک فضای مقیاس برای تصویر، انجام می‌گیرد.

$$L(x,y,\sigma) = G(x,y,\sigma) * I(x,y) \quad (۱)$$

$$G(x,y,\sigma) = \frac{1}{2\pi\sigma^2} e^{-(x^2+y^2)/2\sigma^2} \quad (۲)$$

برای تشخیص نقاط اکسترمم مطابق شکل ۲، از تابع تفاضل گوسی[۳۲] (DOG)، استفاده می‌شود.



شکل ۲. هرم تصویری با DOG [۲].

فضای مقیاس DOG، با تفریق سطوح مجاور یکدیگر و براساس رابطه ۳، حاصل می‌شود.

$$D(x,y,\sigma) = \big(G(x,y,k\sigma) - G(x,y,\sigma)\big) * I(x,y) = L(x,y,k\sigma) L(x,y,\sigma) \quad (۳)$$

در مرحله بعد عمل اکسترمم‌یابی، انجام می‌گیرد. این مرحله با مقایسه مقادیر شدت خاکستری هر پیکسل با ۸ پیکسل مجاور آن و همچنین با ۹ پیکسل در تصاویر مجاور بالایی و پایینی (که از تابع DOG، حاصل شده است و از لحاظ σ با هم اختلاف دارند.) صورت می‌گیرد. اگر مقدار این پیکسل از ۲۶ پیکسل همسایه، کوچکتر یا بزرگتر بود، آن نقطه، به عنوان نقطه مورد نظر انتخاب می‌شود .

ب. تعیین راستا[۳۳]:

در این مرحله به طور دقیق، موقعیت هر نقطه از لحاظ مختصات تعیین می‌گردد و نقاطی که دارای کنتراست کم می‌باشند، حذف خواهند شد. سپس مقدار شیب (گرادیان تابع) و همچنین زاویه شیب با استفاده از تصاویر تفاضل گوسین، به صورت زیر محاسبه می‌شود.

$$m(x,y) = \sqrt{\big(L(x+1,y) - L(x-1,y)\big)^2 + \big(L(x,y+1) - L(x,y-1)\big)^2} \quad (۴)$$

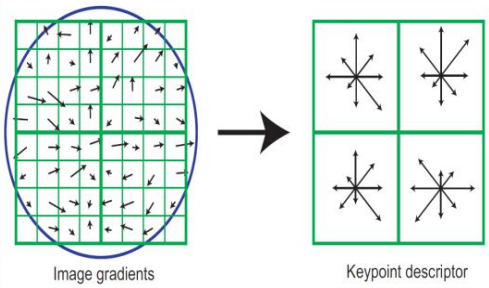
29 .Steganalysis
30 .Cover image
31 .Scale-space extrema detection

32 .Difference of Gaussian
33 .Orientation Assignment

$$\theta(x,y) = \tan^{-1}\left(\frac{(L(x,y+1)-L(x,y-1))}{(L(x+1,y)-L(x-1,y))}\right) \quad (۵)$$

ج. توصیف نقاط کلیدی[۳۴]:

برای اینکه هر ویژگی، به طور منحصر به فرد قابل شناسایی باشد یک بردار مشخصه به آن تخصیص داده می‌شود تا در کارهای بعدی از جمله، تطابق ویژگی مورد استفاده قرار بگیرد. یک تابع گوسی با انحراف معیاری که اندازه آن برابر با نصف طول پنجره مورد نیاز برای تخصیص بردار مشخصه می‌باشد[۳۵]، تولید می‌شود. سپس نقاط اطراف نقطه ویژگی، با آن وزن‌دهی شده و همانند شکل ۳، پنجره حاصل به چهار قسمت تقسیم می‌گردد.



شکل ۳. نحوه تعیین بردار مشخصه برای هر ویژگی [۲].

وزن‌دهی با تابع DOG، باعث شده که بردار مشخصه حساسیت کمتری نسبت به تغییر مکان پنجره مشخصه نشان بدهد و از سوی دیگر ضریب زاویه‌ای نقاط دورتر تأثیر کمتری در بردار مشخصه داشته باشد. پس از آن، اطلاعات هر یک از این هیستوگرام‌ها به دنبال هم قرار می‌گیرند که در بردار شکل بالا یک بردار ۳۲ تایی تشکیل می‌دهد. البته در عمل، تصویر به ۱۶ زیر پنجره (یک آرایه ۴×۴) تقسیم می‌شود و از آنجا هر زیر پنجره، یک هیستوگرام ۸ قسمتی دارد. پس بردار مشخصه دارای ۱۲۸= ۸×۴×۴ عنصر خواهد بود که بهترین جواب را می‌دهد.

د. جستجوی مبتنی بر بردار مشخصه

تطبیق بردارهای ویژگی به دو روش نزدیک‌ترین همسایه[۳۶] و ضرب داخلی بردارها، انجام می‌گیرد، البته روش دوم از نظر محاسباتی، کم‌هزینه‌تر است. برای تطابق یک بردار مشخصه، ضرب داخلی آن با تمامی بردارهای موجود در پایگاه داده محاسبه می‌شود. سپس اندیس ضرب برداری با بیشترین مقدار مشخص شده و تطابق مورد نظر بر اساس آن انجام می‌گیرد.

34 .Keypoint descriptor

۳۵.در اینجا پنجره مشخصه ۸×۸ است بنابراین داریم ۴ =σ

36 . Nearest neighbor

ارزیابی عملکرد SIFT در تطابق تصاویر اثرانگشت

با توجه به کارایی الگوریتم SIFT در تناظریابی و تشخیص دقیق اشیاء، در این مقاله از این توصیفگر به منظور بررسی میزان تطابق صحیح هر اثرانگشت حاصل از پنهان‌نگاری داده رمز شده با الگوریتم RSA[۳۷] [۱۱] و دیفی-هلمن[۳۸] [۱۲]، با تصویر اثرانگشت متناظرش استفاده شده است. طراحی و اجرا، طی مراحلی صورت گرفته است که در ادامه بیان خواهد شد.

بررسی کارایی الگوریتم SIFT در تشخیص اثرانگشت حاوی پیام رمز شده با الگوریتم RSA

الف) ابتدا پیام محرمانه با محتوای "biometric in e-commerce" با الگوریتم RSA رمز شده است. پارامترهای الگوریتم RSA، براساس جدول ۲، در نظر گرفته شده‌اند.

جدول ۲. پارامترهای الگوریتم RSA

پارامترهای الگوریتم RSA	مقدار
عدد اول p:	۱۰۴۶۵۹
عدد اول q:	۱۰۴۷۲۹
تابع فی $(\varphi(n))$:	۱۰۹۶۰۶۲۳۰۲۴
کلید عمومی (e) :	۵
کلید خصوصی (d) :	۲۱۹۲۱۲۴۶۰۵

37 .Rivest, Shamir, Adleman

38 .Diffie-Helman

جدول ۳. نتایج اجرای الگوریتم SIFT در تشخیص اثرانگشت با داده رمز شده با الگوریتم RSA

نتایج اجرای الگوریتم SIFT	اثرانگشت نوع ۱	اثرانگشت نوع ۲	اثرانگشت نوع ۳	اثرانگشت نوع ۴	اثرانگشت نوع ۵	اثرانگشت نوع ۶
اثرانگشت نوع ۱ رمز شده	۲	۲	۰	۰	۰	۰
اثرانگشت نوع ۲ رمز شده	۰	۸	۰	۰	۰	۰
اثرانگشت نوع ۳ رمز شده	۰	۰	۸	۰	۰	۰
اثرانگشت نوع ۴ رمز شده	۰	۲	۰	۱	۰	۰
اثرانگشت نوع ۵ رمز شده	۰	۰	۰	۰	۳	۰
اثرانگشت نوع ۶ رمز شده	۰	۰	۰	۰	۰	۸

ب) پیام رمز شده به روش LSB، در تصاویر پنهان‌نگاری شده است. تصاویر از ۶ اثرانگشت، که از هر اثرانگشت ۸ مورد انتخاب شده است.

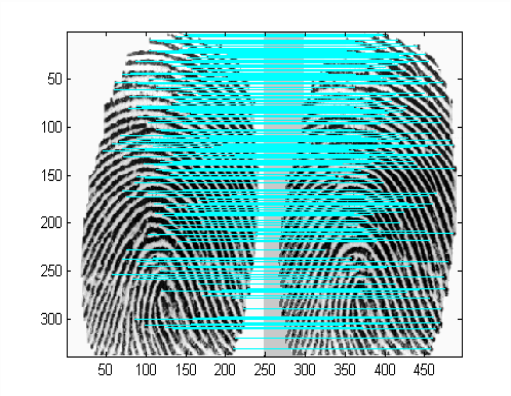
ج) بررسی تعداد نتایج صحیح حاصل از اجرای الگوریتم SIFT در تشخیص اثرانگشت.

جدول ۳، نتایج حاصل از اجرای الگوریتم را نشان می‌دهد. در این جدول سطرها، نمایانگر نتایج حاصل از پنهان نگاری متن رمز شده با الگوریتم RSA در تصویر اثرانگشت و ستون‌های آن، بیانگر تصویر اثرانگشت است. براساس جدول ۳، الگوریتم SIFT تقریباً ۸۸/۲۳ درصد، اثرانگشت مربوط به هر فرد را از میان تطابق‌های انجام شده، به درستی تشخیص می‌دهد. محاسبه درصد تشخیص صحیح الگوریتم SIFT بر روی اثرانگشت مطابق رابطه ۶، صورت گرفته است.

$$\frac{\text{تعداد تشخیص صحیح}}{\text{تعداد کل تطابق الگوریتم}} \times 100 = \frac{30}{34} \times 100 = 88.23\ \% \quad (۶)$$

در رابطه ۶، تعداد تشخیص صحیح الگوریتم معادل با مجموع اعداد بر روی قطر اصلی ماتریس بالاست.

شکل ۴، نمونه‌ای از اجرای الگوریتم در اثرانگشت را نشان می‌دهد. نتایج نشان می‌دهد که با عملگر SIFT، ۸۸/۲۳ درصد تشخیص صحیح صورت گرفته است. این در حالی است که در مطالعه پارک و همکاران [۳]، عملکرد SIFT در تطابق اثرانگشت و بدون داده رمز شده، تقریباً برابر با ۹۸/۹۷ درصد بوده است. بنابراین، با وجود به کارگیری الگوریتم RSA برای رمزنگاری داده، درصد تشخیص در مقایسه با روش پارک و همکاران [۳]، تفاوت چندانی ندارد. پس با پنهان کردن داده رمز شده در اثرانگشت، کیفیت تصویر تغییر چندانی نخواهد کرد و تغییری در اثرانگشت درک نمی‌شود.



شکل ۴. نحوه تشخیص اثرانگشت رمز شده با الگوریتم RSA

بررسی کارایی الگوریتم SIFT در تشخیص اثرانگشت حاوی پیام رمز شده با دیفی- هلمن

الف) ابتدا پیام با محتوای "biometric in e-commerce" را با الگوریتم دیفی- هلمن و براساس پارامترهای جدول ۴، رمز شده است.

جدول ۴. پارامترهای الگوریتم دیفی-هلمن

پارامترهای الگوریتم دیفی-هلمن	مقدار
عدد اول p:	۱۰۴۷۲۹
مولد g:	۶۸۷۳۰۳
مقدار مخفی a:	۱۷۰۱۴۱۱
مقدار مخفی b:	۸۳۴۶۰۴۶
کلید رمزنگاری ($k = g^{ab} mod\ p$):	۷۹۱۴۳

ب) پیام رمز شده در LSB تصاویر، پنهان‌نگاری شده است. تصاویر از ۶ اثرانگشت که از هر کدام ۸ مورد در نظر گرفته شده است.

ج) بررسی تعداد نتایج صحیح حاصل از اجرای الگوریتم SIFT در تشخیص اثرانگشت.

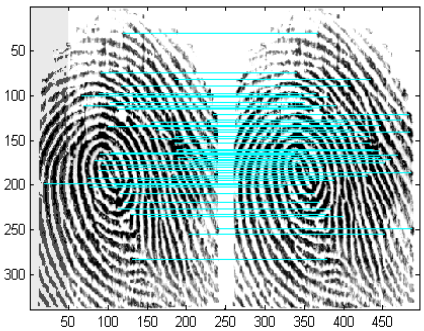
جدول ۵. نتایج اجرای الگوریتم SIFT در تشخیص اثرانگشت با داده رمز شده با الگوریتم دیفی-هلمن

نتایج اجرای الگوریتم SIFT	اثرانگشت نوع ۱	اثرانگشت نوع ۲	اثرانگشت نوع ۳	اثرانگشت نوع ۴	اثرانگشت نوع ۵	اثرانگشت نوع ۶
اثرانگشت نوع ۱ رمز شده	۰	۰	۱	۰	۰	۰
اثرانگشت نوع ۲ رمز شده	۰	۸	۰	۰	۰	۰
اثرانگشت نوع ۳ رمز شده	۰	۰	۸	۰	۰	۰
اثرانگشت نوع ۴ رمز شده	۰	۰	۰	۱	۰	۰
اثرانگشت نوع ۵ رمز شده	۰	۰	۰	۰	۳	۰
اثرانگشت نوع ۶ رمز شده	۰	۰	۰	۰	۰	۵

جدول ۵، نتایج حاصل از اجرای الگوریتم را نشان می‌دهد در این جدول سطرها، نمایانگر نتایج حاصل از پنهان نگاری متن رمز شده در تصویر اثرانگشت و ستون‌های آن نشان دهنده تصویر اثرانگشت است. مطابق جدول ۵، الگوریتم SIFT تقریباً ۹۶/۱۵ درصد، اثرانگشت مربوط به هر فرد را از میان تطابق‌های انجام گرفته، به طور صحیح تشخیص می‌دهد. درصد تشخیص صحیح الگوریتم SIFT بر روی اثرانگشت براساس رابطه ۷ محاسبه شده است.

$$\frac{\text{تعداد تشخیص صحیح}}{\text{تعداد کل تطابق الگوریتم}} \times 100 = \frac{25}{26} \times 100 = 96.15\ \% \quad (۷)$$

شکل ۵، نمونه‌ای از اجرای الگوریتم SIFT در تطابق اثرانگشت حاوی داده رمز شده و اثرانگشت نشان می‌دهد. مطابق با نتایج بدست آمده، با وجود ارسال داده رمز شده حاصل از الگوریتم دیفی-هلمن و در مقایسه با روش پارک و همکاران [۳]، الگوریتم SIFT دارای عملکرد مناسبی در تطابق تصاویر است.



شکل ۵. نحوه تشخیص اثرانگشت رمز شده با الگوریتم دیفی- هلمن

ارزیابی نتایج تجربی

الگوریتم SIFT یکی از قوی‌ترین الگوریتم‌های آشکارسازی و تناظریابی نقاط در حوزه پردازش تصویر است و همان‌طور که انتظار می‌رفت در بررسی‌های تجربی انجام شده در این تحقیق نیز عملکرد مناسبی را نشان می‌دهد. براساس اجرای الگوریتم SIFT بر روی تصاویر اثرانگشت با داده رمز شده، خلاصه‌ای از نتایج الگوریتم و مقایسه با پژوهش پارک و همکاران [۳]، در جدول ۶ بیان شده است.

جدول ۶. مقایسه نتایج اجرای الگوریتم SIFT در تشخیص اثرانگشت با پژوهش پارک و همکاران [۳]

نتایج اجرای الگوریتم SIFT	اثر انگشت بدون داده رمز شده [۳]	اثرانگشت با داده رمز شده با الگوریتم RSA	اثرانگشت با داده رمز شده با الگوریتم دیفی-هلمن
درصد تشخیص	٪ ۹۸/۹۷	٪ ۸۸/۲۳	٪ ۹۶/۱۵

همان‌طور که از جدول ۶ استنتاج می‌شود، پنهان‌نگاری داده محرمانه در تصویر اثرانگشت تأثیر چندانی در عملکرد SIFT نداشته است. با توجه به آنچه که بیان شد، عملگر SIFT براساس نقاط کلیدی، تطابق تصاویر را انجام می‌دهد. از این رو، مطابق با نتایج حاصل، ارسال داده رمز شده به همراه تصاویر اثرانگشت، نقاط کلیدی را چندان حذف نخواهد داد. بنابراین کیفیت تصویر اثرانگشت براساس پنهان‌نگاری داده محرمانه، تغییر نمی‌کند. این مسئله زمانی حائز اهمیت است که در نظر داشته باشیم، تبادل اطلاعات مربوط به تراکنش‌های تجارت الکترونیک بر روی کانال‌های بیسیم صورت می‌گیرد. ماهیتاً این کانال‌ها در معرض شنود و جعل اشخاص غیرمجاز می‌باشند. ارسال داده محرمانه‌ای که تنها طرفین مبادلات تجاری از آن اطلاع دارند، ریسک جعل تصاویر بیومتریک همچون اثرانگشت را کاهش می‌دهد. از سوی دیگر، تغییر ناچیز کیفیت تصویر منجر به ایجاد تردید و تحریک در فرد شنود کننده و تلاش برای کشف داده محرمانه نخواهد شد. بنابراین رمز کردن داده محرمانه و ارسال با تصویر اثرانگشت نه تنها تراکنش‌های تجاری بر روی کانال بیسیم را امن می‌کند، بلکه تغییرات در تصویر اثرانگشت درک نخواهد شد.

نتیجه‌گیری

امروزه به علت اهمیت روز افزون تجارت الکترونیک و تمایل افراد به امنیت اطلاعات در تراکنش‌های مالی، شیوه‌های مختلفی برای تصدیق هویت به کار رفته است. سیستم بیومتریک، با هدف فراهم کردن امکان شناسایی افراد، به طور گسترده مورد استفاده قرار می‌گیرد. با این وجود، تبادل اطلاعات بیومتریک در تراکنش‌های تجارت الکترونیک، در معرض سرقت و جعل قرار دارد. یکی از راه‌های حفظ اطلاعات بیومتریک، به کار بردن داده محرمانه با این اطلاعات است. می‌توان با الگوریتم رمزنگاری، داده محرمانه را رمز و با اثرانگشت ارسال کرد. در این پژوهش، ابتدا داده با الگوریتم RSA و دیفی- هلمن رمز شده‌اند و به روش LSB در تصاویر اثرانگشت پنهان‌نگاری شده‌اند. سپس به منظور بررسی عملکرد الگوریتم SIFT در تطابق اثرانگشت با حضور داده رمز شده در تصویر، الگوریتم مربوطه اعمال شده است. نتایج نشان می‌دهد که در مقایسه با عملکرد SIFT در تشخیص تصویر بدون داده محرمانه، الگوریتم SIFT در تطبیق تصویر حاوی داده رمز شده با تصویر اصلی به خوبی عمل خواهد کرد. به عبارتی رمز کردن داده با الگوریتم رمزنگاری و پنهان کردن آن در تصویر تأثیر چندانی در کیفیت نداشته است. بنابراین رمز کردن داده و ارسال آن با اطلاعات بیومتریک همچون اثرانگشت، اطلاعات بیومتریک را حفظ کرده و از سویی دیگر تبادل اثرانگشت به منظور تصدیق هویت در تراکنش‌های تجارت الکترونیک با قابلیت اطمینان بیشتر انجام خواهد گرفت.

مرجع‌ها

[1] D. G. Lowe, "Object recognition from local scale-invariant features," in Computer vision, 1999. The proceedings of the seventh IEEE international conference on, 1999, pp. 1150-1157.

[2] D. G. Lowe, "Distinctive image features from scale-invariant key points," International journal of computer vision, vol. 60, pp. 91-110, 2004 .

[3] U. Park, S. Pankanti, and A. K. Jain, "Fingerprint verification using SIFT features," in SPIE, 2008, p. 69440K

[4] J. Chen and Y.-S. Moon, "Using SIFT features in palmprint authentication," in Pattern Recognition, 2008. ICPR 2008. 19th International Conference on, 2008, pp. 1-4 .

[5] G. Iannizzotto and F. L. Rosa, "A SIFT-based fingerprint verification system using cellular neural networks," Pattern Recognition Techniques, Technology and Applications, pp. 523-536, 2008.

[6] A. Morales, M. A. Ferrer, and A. Kumar, "Improved palmprint authentication using contactless imaging," in Biometrics: Theory Applications and Systems (BTAS), 2010 Fourth IEEE International Conference on, pp.1-6.

[7] M. El-Abed, C. Charrier, and C. Rosenberger, "Evaluation of Biometric Systems," in New Trends and Developments in Biometrics, J. Yang, S. J. Xie, InTech, Chapter 7, November 2012.

[8] A. Bajpai, J. Kaur, D. Aggarwal, and K. Agarwal, "Biometric System: Fingerprinting Trait," International Journal of Emerging Trends in Computer Science, vol. 1, 2013.

[9] N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," IEEE computer, vol. 31, pp. 26-34, 1998.

[10] S. Gupta, A. Goyal, and B. Bhushan, "Information Hiding Using Least Significant Bit Steganography and Cryptography," International Journal of Modern Education and Computer Science (IJMECS), vol. 4, p. 27, 2012.

[11] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, vol. 21, pp. 120-126, 1978.

[12] W. Diffie and M. Hellman, "New directions in cryptography," Information Theory, IEEE Transactions on, vol. 22, pp. 644-654, 1976.