راهکاری مقرون به صرفه و کارا برای حفاظت از مالکیت و اصالت اسناد مالی با استفاده از اختفای اطلاعات تصویری بیومتریک صاحبان حساب های بانکی

A cost-effective approach to protect ownership and integrity of financial documents using hidden biometric images of bank account owners

میر شهریار امامی
فوق دکترای کامپیوتر و استادیار دانشگاه آزاد اسلامی
(واحد رودهن)
shemami86@gmail,com

چکیده

اطلاعات بیومتریک اشخاص نظیر: اثر انگشتان دست، اسکن عنبیه چشم ، DNA، و غیره اطلاعاتی منحصر به فرد به حساب می آیند به گونه ای که این اطلاعات از شماره ملی، شماره حساب بانکی، شماره بیمه و نظایر آن طبیعت منحصر به فرد تر دارند زیرا اطلاعات بیومتریک اشخاص به طبیعت بشر بر می گردد و نه به قوانین موضوعه توسط انسان. در این میان، با گسترش بین المللی تجارت الکترونیک و بانکداری الکترونیک، حفظ مالکیت و اصالت اسناد مالی مبادله شده بین بانک ها، بین بانک ها و شرکت های تجاری، بین شرکت های تجاری با یکدیگر، و بین مشتریان با بانک ها و شرکت های تجاری یک امر ضروری است. در این خصوص، فناوری های اختفای اطلاعات راهکارهای موثری برای حفاظت از اسناد دیجیتالی را ارائه داده است. در این مقاله راهکاری مقرون به صرفه بر اساس اطلاعات تصویری بیومتریک اشخاص و اختفای آنها در اسناد بانکی و مالی صادر شده برای حفاظت از مالکیت و اصالت اینگونه اسناد پیشنهاد شده است. راهکار پیشنهادی با داده کاوی در بردار ویژگی های ناشی از نظم و سازگاری طبیعی در اطلاعات تصویری بیومتریک اشخاص محقق می گردد.

واژه‌های کلیدی: بانکداری الکترونیک، اطلاعات بیومتریک، اختفای اطلاعات، حفظ مالکیت ، حفظ اصالت، اسناد بانکی، اسکن اثر انگشت.

۱- مقدمه

امروزه حرکت به سمت سیستم های بدون کاغذ (Paperless)یکی از اهداف مهم همه سازمان ها، بانک ها، شرکت‌های خصوصی و دانشگاه ها می باشد. این موضوع نتنها منجر به کاهش مصرف کاغذ و کاسته شدن هزینه های خرید و سرویس نگهداری دستگاه های چاپگر می گردد بلکه سبب کاهش هزینه های مربوط به اعمال حفاظت های فیزیکی روی اسناد و مدارک صادر شده، که اغلب بسیار پر هزینه بوده و بیشتر مواد و تجهیزات وارداتی هستند، می شود. در این بین، با گسترش تجارت الکترونیک و بانکداری الکترونیک در داخل کشور و در سطح بین الملل، حفظ مالکیت و اصالت اسناد مالی مبادله شده بین بانک ها، بین بانک ها و شرکت های تجاری، بین شرکت های تجاری با یکدیگر، و بین مشتریان با بانک ها و شرکت های تجاری از اهمیت بالاتری برخوردار است.

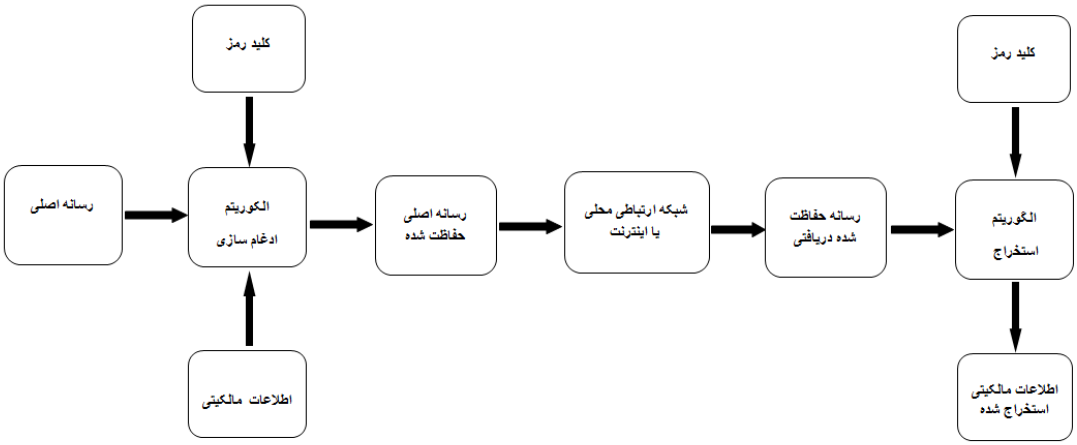
هدف اصلی از ارائه این کار پژوهشی اختفای مشخصه های بیومتریک، با تاکید بر تصویر اثر انگشت صاحبان اسناد بانکی و مالی در داخل اسناد بانکی و مالی دیجیتالی صادر شده برای آنها مانند: ضمانت نامه های بانکی الکترونیک، چک الکترونیک ، سفته الکترونیک و ... می باشد که این امر با هدف حفاظت از مالکیت و اصالت اسناد دیجیتالی مذکور انجام می پذیرد تا بصورت کاراتر و با هزینه کمتر از بروز جعل، تغییر، و یا بروز هر گونه تخلفات دیگر ممانعت به عمل آید و از همه مهمتر اینکه تفاوت معنی داری میان بروز تخلف روی اسناد دیجیتالی، و وقوع اتفاقات ناخواسته روی اسناد دیجیتالی از جمله: بروز نویز و پارازیت، فشرده سازی فایل اسناد و امثال آن وجود داشته باشد.

ساختار اجمالی این مقاله شامل مواردی بدین شرح است: در بخش (۱) به مقدمه ، بیان انگیزه ها و اهداف پرداخته شده است. در بخش (۲) مرور ادبیات پژوهش و خلاصه ای از فعالیتهای مرتبط بیان شده است. در بخش (۳) روش تحقیق شامل: مراحل کار، روشها، محاسبات، جامعه آماری و متدهای ارزیابی بیان گردیده است. بخش (۵) به یافته ها و نتایج آزمایشات اختصاص یافته است. بخش (۶) شامل جمع بندی و خلاصه نتایج حاصل از تحقیق می باشد. در آخر بخش (۷) به ذکر منابع مورد استفاده در این کار پژوهشی پرداخته شده است.

۲- ادبیات پژوهش

دانش اختفای اطلاعات (Information Hiding)[۱] به پنهان سازی انواع داده های متنی، تصویری و صوتی در داخل یک سند دیگر متنی، تصویری، صوتی و یا ویدیویی با هدف اعمال انواع مکانیسم های حفاظتی از اسناد (Watermarking)[2,3]، و یا حمل مخفیانه اطلاعات (Steganography)[2,3] می پردازد که از بین این دو، دو کاربرد حفاظت از مالکیت اسناد، و حفاظت از اصالت اسناد با شیوه غیره دیداری (Invisible)مد نظر است.

دانش واترمارکینگ به بیش از ۷۰۰ سال قبل یعنی زمانی که تولید کنندگان کاغذ برای حفظ قابلیت شناسایی برند کاغذهای تولیدی خود از این دانش استفاده می نمودند، بر می گردد اما امروزه کاربردهای متعددی از این دانش وجود دارد که دو مورد حفاظت از مالکیت اسناد دیجیتالی و حفاظت از اصالت اسناد دیجیتالی مورد توجه این کار پژوهشی است. تصویر (۱) فرایند عمومی واترمارکینگ را برای این منظور نشان می دهد.



تصویر۱ – فرایند کلی واترمارکینگ.

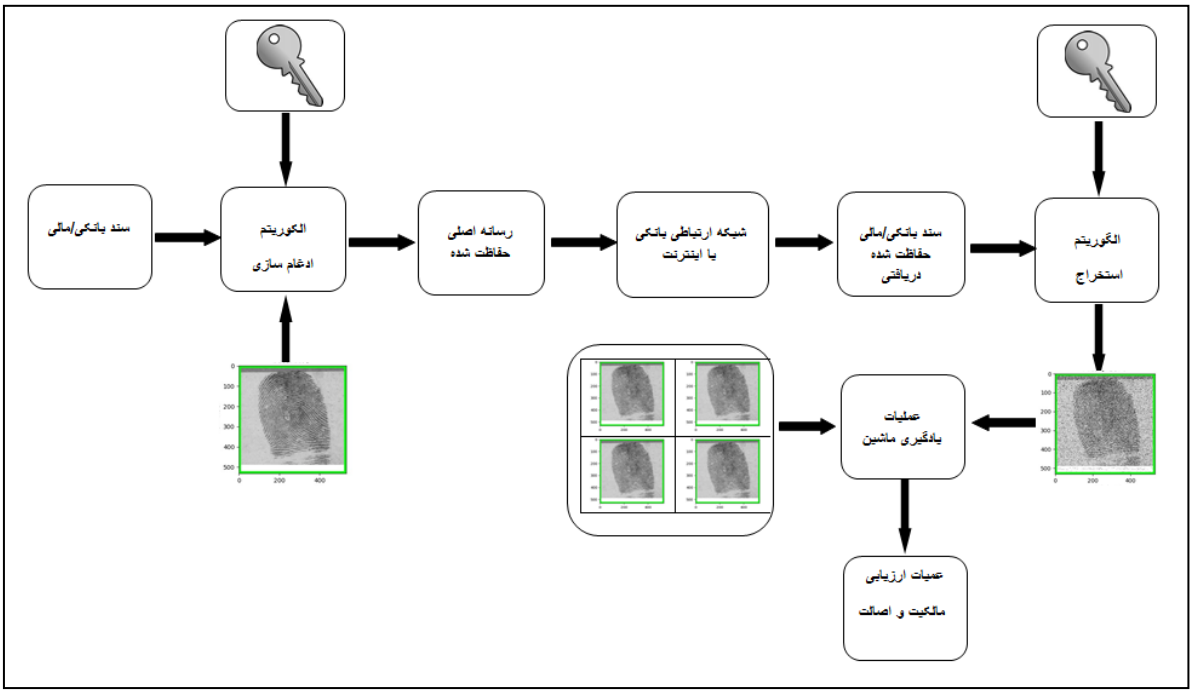
همانطور که در تصویر (۱) مشاهده می گردد رسانه ای که قرار است محافظت گردد بر اساس یک (یا چند) کلید رمز و به کمک یک الگوریتم ادغام ساز (Embedding Algorithm) [1,4,5]، اختفای اطلاعات مالکیتی در داخل سند مورد نظر انجام می پذیرد. در ادامه سند حفاظت شداز طریق شبکه های ارتباطی محلی و یا اینترنت عبور نموده و در نهایت سند حفاظت شده دریافتی در مقصد توسط یک (یا چند)کلید رمز و به کمک یک الگوریتم استخراج (Extracting Algorithm)، اطلاعات مالکیتی بازیافت می گردد و بر اساس این اطلاعات، مالکیت و در شرایطی اصالت سند مذکور قابل ارزیابی است.

تاکنون پژوهش های زیادی در حوزه واترمارکینگ صورت گرفته است. با مطالعه این پژوهش ها، روش های واترمارکینگ به لحاظ دامنه را می توان به سه گروه: مدل تبدیلی (Transform Domain) [6]، مدل فضایی (Spatial Domain)[6,7]، و مدل ترکیبی (Hybrid Domain)[۸] طبقه بندی نمود که از میان این سه مدل، از یک طرف مدل فضایی ساده تر و سریع تر می باشد و از طرف دیگر برای رسیدن به هر دو هدف این پژوهش یعنی: حفاظت از مالکیت و اصالت اسناد بانکی و مالی، مدل فضایی می تواند مناسب تر باشد. با اینهمه مدل های فضایی در مقایسه با مدل های تبدیلی و ترکیبی اغلب در مقابل تهاجم های تعامدی و غیر تعامدی، مقاومت کمتری از خود نشان می دهند. نویسنده این مقاله برای رفع این ضعف، گروهی از روش ها را تحت عنوان روش های مبتنی برآمار (Statistical based)[4,7,9] مطرح ساخته است که مبنای آن شناسایی مالک اسناد حفاظت شده بر اساس باقیمانده اطلاعات حاصل از تهاجم صورت گرفته می باشد. تقریبا در همه پژوهش های مذکور از انواع لوگوها مانند آرم شرکت ها و سازمان ها و یا اطلاعات متنی ساده استفاده شده است و ارزیابی مالکیت بر اساس اینگونه از اطلاعات صورت پذیرفته است. این در حالی است که اطلاعات تصویری بیومتریک مانند اسکن اثر انگشت دست اشخاص می تواند ویژگی های خاص تر و متفاوت تر و منحصر به فرد تری را دارا باشد که این امر می تواند حتی در صورت بروز انواع تهاجم، همچنان امکان شناسایی مالکان اسناد بانکی و مالی را فراهم آورد.

۳- روش تحقیق

روش ارائه شده در این کار پژوهشی روش واترمارکینگ فضایی غیر دیداری (EISB)[۹] مبتنی بر اطلاعات

مالکیتی تصویری بر اساس تصویر اثر انگشت مالکان اسناد بانکی و مالی می باشد و با روش آموزنده بردار پشتیبان (Support Vector Machine) و روش آماری L2Norm [۹] می باشد (تصویر ۲).

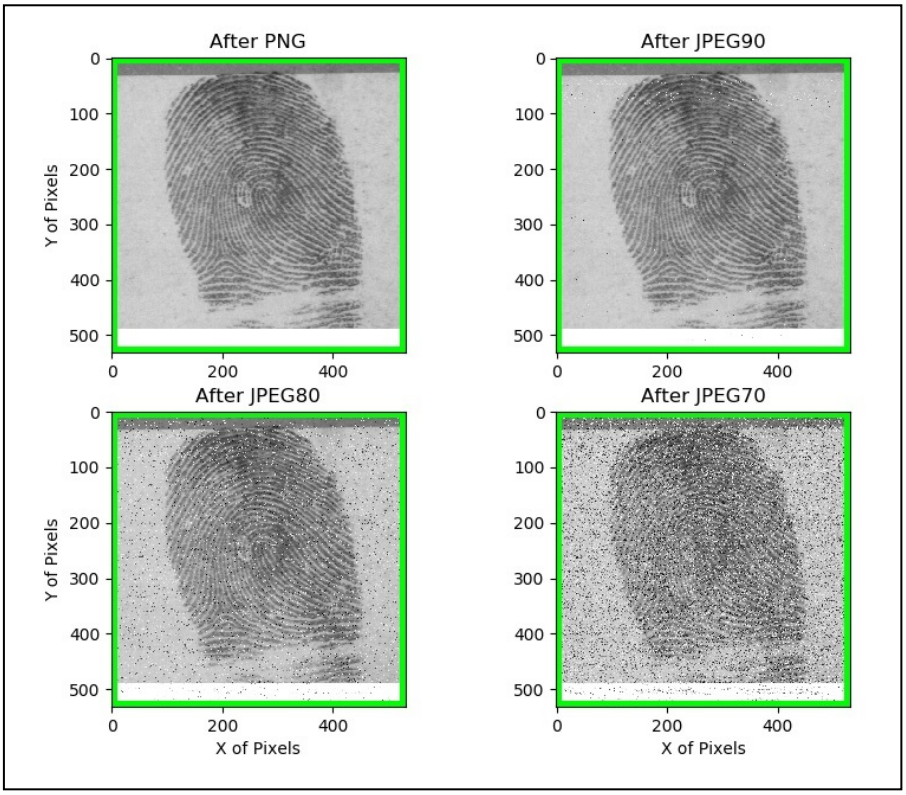


تصویر۲ – بلوک دیاگرام روش پیشنهادی.

جامعه آماری این پژوهش پایگاه داده های استاندارد اثر انگشت موسسه ملی استانداردها و تکنولوژی (NIST) [10] مربوط به وزارت بازرگانی دولت ایالات متحده آمریکا (US Department of Commerce) می باشد که شامل تصاویر اثر انگشت با فرمت PNG با اندازه 512 X 512 پیکسل است که فرمت اصلی این فایل با قالب AN2 بوده است که عمل تبدیل به فرمت PNG به کمک ابزار an2ktool صورت پذیرفته است. متد ارزیابی بصورتمقایسه ای و بر اساس طبقه بندی (Classification)بر مبنای روش آموزنده مبتنی بر ناظر (Supervised Learning) و روش آماری L2Norm مبتنی بر هیستوگرام [۹] می باشد. نسخه اولیه برنامه نوشته شده برای انجام آزمایشات اولیه، با زبان جاوا در محیط NetBeans 8.0 و نسخه نهایی برنامه نوشته شده برای انجام نهایی آزمایشات، با زبان برنامه نویسی Python 3.6 64-bit و در محیط PyCharm 2017.1.2 x64 انجام گرفته است و اجرای همه آزمایشات روی کامپیوتر Intel Core i5 و تحت سیستم عامل Windows 8.0 صورت گرفته است.

۴- یافته ها و نتایج

یک نمونه از تصویر اثر انگشت استخراج شده پس از بروز تهاجم های فشرده سازی PNG، JPEG90، JPEG80 و JPEG70 و شناسایی موفق مالک توسط روش پیشنهادی در تصویر ۳ نشان داده است. اطلاعات مربوط به شناسایی ۱۰ تصویر آزمایش شده در جدول ۱ نشان داده شده است که در تمام موارد مالک اصلی اسناد به درستی شناسایی شده است.

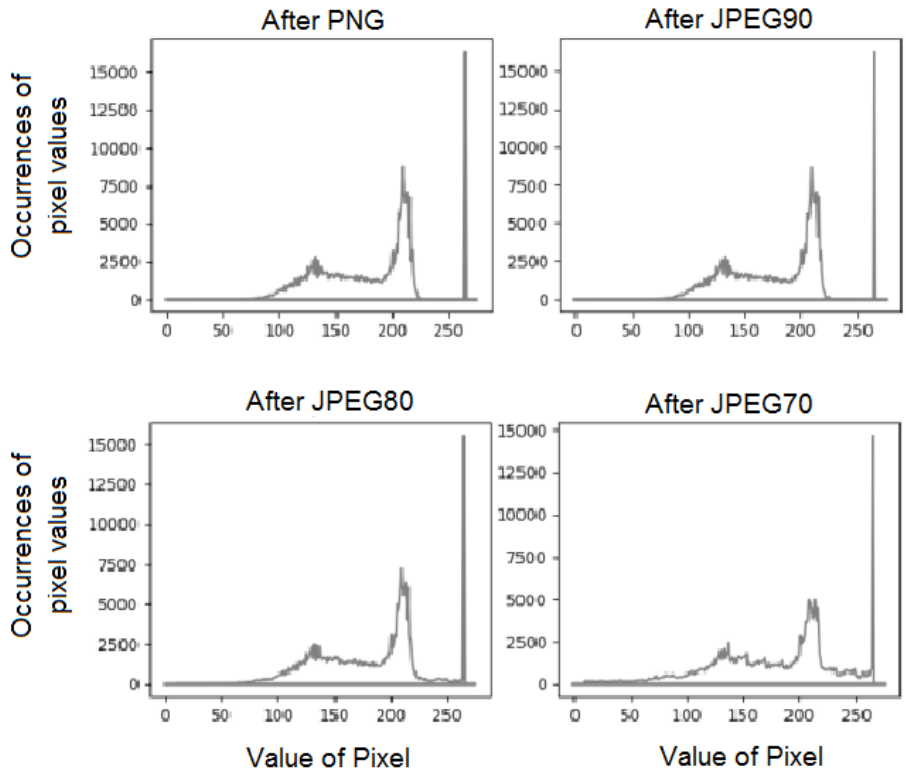


تصویر۳ – یک نمونه از تصویر اثر انگشت استخراج شده پس از بروز تهاجم های فشرده سازی PNG، JPEG90، JPEG80، و JPEG70 و شناسایی موفق مالک توسط روش پیشنهادی.

جدول ۱– شناسایی مالک پس از عمل تهاجم با روش یادگیری ماشین بردار پشتیبان (SVM)

	نوع تهاجم و شناسایی شماره حساب بانکی مالک تصویر			
شماره تصویر	PNG	JPEG90	JPEG80	JPEG70
1	1	1	1	1
2	2	2	2	2
3	3	3	3	3
4	**4**	**4**	**4**	**4**
5	5	5	5	5
6	6	6	6	6
7	7	7	7	7
8	8	8	8	8
9	9	9	9	9
10	10	10	10	10

یک نمونه از هیستوگرام تصویر اثر انگشت استخراج شده پس از بروز تهاجم های فشرده سازی PNG، JPEG90، JPEG80 و JPEG70 و شناسایی موفق مالک اسناد توسط روش پیشنهادی در تصویر ۴ ملاحظه می گردد.



تصویر۴ –یک نمونه از هیستوگرام تصویر اثر انگشت استخراج شده پس از بروز تهاجم های فشرده سازی PNG، JPEG90، JPEG80، و JPEG70 و شناسایی موفق مالک توسط روش پیشنهادی.

در جدول ۲ از یک روش تخمینی مبتنی بر L2Norm که توسط مولف این مقاله در منبع [۹] پیشنهاد شده است، بهره برداری شده است که در این روش، شناسایی تخمینی مالک اسناد حفاظت شده بر اساس بازیافت باقیمانده اطلاعات و ترسیم هیستوگرام این اطلاعات پس از انواع تهاجم ها می باشد. نتایج آزمایشات صورت گرفته با روش آموزنده SVM در جدول 1 نشان داد که بیشترین میزان شباهت تصویراثرانگشت بازیابی شده متعلق به مالک دارنده حساب بانکی شماره ۴ است. ارزیابی های صورت گرفته با روش تخمینی مبتنی بر L2Norm نیز دقیقا همین نتیجه را به لحاظ آماری بیان می دارد؛ یعنی مقدار حداکثر شباهت مربوط به تصویر اثر انگشت متعلق به مالک دارنده حساب بانکی شماره ۴ است.

جدول ۲– شناسایی مالک بر اساس بیشترین شباهت آماری اثر انگشت با روش **L2Norm** [۹]

	نوع تهاجم و میزان شباهت آماری تصویر اثر انگشت			
شماره تصویر اثر انگشت	PNG	JPEG90	JPEG80	JPEG70
1	0.90650636	0.90687162	0.91493815	0.92822552
2	۰,۹۲۵۲۹۱۶۶	۰,۹۲۵۶۷۳۴۳	۰,۹۳۲۶۹۳۷۲	۰,۹۴۱۲۹۶۴۶
3	۰,۹۳۰۱۲۶۰۷	۰,۹۳۰۱۱۳۸۵	۰,۹۳۱۶۴۲۴۱	۰,۹۳۰۳۴۱۴۲
4	**1.00000000**	**۰,۹۹۹۹۰۴۲۶**	**۰,۹۸۵۹۱۱۳۱**	**۰,۹۶۱۷۴۰۲**
5	۰,۹۲۵۳۳۸۹۸	۰,۹۲۵۷۴۰۳۶	۰,۹۳۴۲۰۹۸۲	۰,۹۴۶۴۲۳۶۵
6	۰,۹۲۵۹۲۱۱۴	۰,۹۲۶۲۵۳۲۶	۰,۹۳۴۰۰۱۵۱	۰,۹۴۵۷۳۲۸۹
7	۰,۹۳۶۲۲۴۳۴	۰,۹۳۶۵۷۲۰۲	۰,۹۴۳۷۲۸۵۱	۰,۹۴۲۳۲۲۰۷
8	۰,۹۴۴۹۸۳۰۶	۰,۹۴۹۷۵۴۵۹	۰,۹۴۵۶۵۱۷۶	۰,۹۳۶۹۲۶۳۶
9	۰,۸۹۳۵۷۶۹۲	۰,۸۹۴۰۰۹۵۳	۰,۹۰۲۷۹۲۳۹	۰,۹۱۸۰۹۳۰۹
10	۰,۸۹۸۹۴۷۰۶	۰,۸۹۹۳۲۴۴۲	۰,۹۰۷۳۹۶۵۵	۰,۹۲۰۹۶۴۴۸
مقدار ماکزیمم	**1.00000000**	**۰,۹۹۹۹۰۴۲۶**	**۰,۹۸۵۹۱۱۳۱**	**۰,۹۶۱۷۴۰۲**

جمع بندی

در این مقاله یک روش کارا و مقرون به صرفه واترمارکینگ فضایی غیر دیداری (EISB) مبتنی بر اطلاعات بیومتریک براساس تصاویر بیومتریک از نوع اثر انگشت دست مالکان اسناد بانکی و مالی ارائه شده است. این روش پیشنهادی با زبان برنامه نویسی Python 3.6 64-bit و در محیط PyCharm 2017.1.2 x64 پیاده سازی شد. نتایج آزمایشات روی مجموعه دادگان استاندارد NIST نشان داد که حتی پس از بروز تهاجم های فشرده سازی PNG، JPEG90، JPEG80، و JPEG70 روی فایل های مربوط به اسناد بانکی، شناسایی مالک اصلی این اسناد بانکی با روش آموزنده بردار پشتیبان (Support Vector Machine) و روش آماری L2Norm، با موفقیت قابل انجام بوده است.

منابع

[1] Parnas, D.L. (2002). The Secret History of Information Hiding. Springer, Software Pioneers, 398-409.
[2] Cox, I., Miller, M. L., Bloom, J. A., Fredrich, J., Kalker, T. (2008). *Digital watermarking and steganography* (2nd ed.). Elsevier, pp. 39ت40.
[3] Shih, F.Y. (2008). *Digital watermarking and steganography Fundamentals and Techniques.* CRC Press, Tailor and Francis Group.
[4] Emami, M.Sh., Omar Kh. (2013). *A low-cost method for reliable ownership identification of medical images using SVM and Lagrange duality*. Elsevier, Expert Systems with Applications, 40, 7579ت7587.
[5] Al-Haj, A.M. (2010*). Advanced Techniques in Multimedia Watermarking, Image Video, and Audio Applications.* Information Science Reference. USA.
[6] Emami, M. Sh., Sulong, B.S., Binti Seliman, S. (2012). *A Novel Multiple Semi-Blind Enhanced ISB Watermarking Algorithm using Watermark bit-Pattern Histogram for Copyright Protection.* International Journal of Innovative Computing, Information and Control. March, 8, No. 3 (A). Japan.
[7] Mahule, R. V., Dhawale, C. A. (2015). *Analysis of Image Security Techniques using Digital Image Watermarking in Spatial Domain* .International Journal of Computer Applications, 0975 ت8887.
[8] Yadav, K., Kaushik, A. (2013). *A Review of hybrid digital watermarking*, International Journal of Engineering Trends and Technology (IJETT), July, 4(7).
[9] Emami, M. Sh., Sulong, B.S. (2011). *A Statistical Method based on L2Norm Technique for EISB Information Watermarking Scheme*, International Conference on Future Information Technology, September, 13. Singapore.
[10] NIST. https://www.nist.gov/itl/iad/image-group/resources. USA.