



Semnan University



Research Article

Improving Image Spam Detection Using a New Image Texture Features Selection

Azam Shekari Shahrak ^a, Seyed Javad Mirabedini ^{b,*}, Nasser Mikaeilvand ^b, Seyed Hamid Haj Seyed Javadi ^c

^a Department of Computer Engineering, Borujerd Branch, Islamic Azad University, Borujerd, Iran

^b Department of Computer Engineering, Center Tehran Branch, Islamic Azad University, Tehran, Iran

^c Department of Mathematics and Computer Science, Faculty of Basic Sciences, Shahed University, Tehran, Iran

PAPER INFO

Paper history:

Received: 2024-02-25

Revised: 2024-05-13

Accepted: 2024-05-18

Keywords:

Spam;

Image;

Machine learning;

Neural network.

ABSTRACT

Spam is one of the problems that has plagued human societies. Although a lot of research has been done in this field, because spammers keep changing their methods like viruses, so there is always a need to provide new solutions in this field. The purpose of the research is to use image texture features to detect image spam. So far, 22 features of image texture have not been used in one place to detect image spam. In this paper, a hybrid method is used to extract key features. In the proposed hybrid method, the co-occurrence matrix of the gray level and chi-square and the threshold of changes in the value of the features are used. The steps mentioned have a great impact on the performance of the categories and improve the accuracy of detection. In the classification stage, the most widely used machine learning algorithms are used to detect image spams, and after obtaining the results of each category, the output of the algorithms used on spam and valid images is examined and compared. The obtained results show that with the help of the proposed method, good detection accuracy can be achieved compared to other methods. Among the reviewed algorithms, the neural network algorithm shows the best performance. The assumed algorithm in other articles shows a lower detection accuracy than the present article, but in the proposed method, it reaches 99.29% detection accuracy.

DOI: <https://doi.org/10.22075/jme.2024.33366.2627>

© 2024 Published by Semnan University Press.

This is an open access article under the CC-BY 4.0 license. (<https://creativecommons.org/licenses/by/4.0/>)

* Corresponding author.

E-mail address: J_mirabedini@iauctb.ac.ir

How to cite this article:

Shekari Shahrak, A., Mirabedini, S. J., Mikaeilvand, N., & Haj Seyed Javadi, S. H. (2024). Improving the detection of image spam using a new method in the selection of image texture features. *Journal of Modeling in Engineering*, 22(79), 211-221. doi: 10.22075/jme.2024.33366.2627

بهبود تشخیص هرزنامه‌های تصویری با استفاده از روشی نوین در انتخاب ویژگی‌های بافت

تصویر

اعظم شکاری شهرک^۱، سید جواد میرعابدینی^{۲*}، ناصر میکاییل‌وند^۳، سید حمید حاج سید جوادی^۳

اطلاعات مقاله	چکیده
دریافت مقاله: ۱۴۰۲/۱۲/۰۶	هرزنامه از معضلاتی است که جوامع بشری را درگیر خود کرده است. با اینکه تحقیقات زیادی در این زمینه صورت گرفته است اما چون هرزنامه‌نویسان مانند ویروس‌ها، مدام روش خود را تغییر می‌دهند، لذا همواره نیاز به ارائه راه کارهای جدید در این زمینه مشاهده می‌شود. هدف از این پژوهش، استفاده از ویژگی‌های بافت تصویر در تشخیص هرزنامه‌های تصویری می‌باشد. تاکنون از ۲۲ ویژگی بافت تصویر به صورت یکجا جهت تشخیص هرزنامه تصویری استفاده نشده است. در این مقاله، روشی ترکیبی جهت استخراج ویژگی‌های کلیدی استفاده می‌شود. در روش ترکیبی پیشنهادی، از ماتریس هم‌رخداد سطح خاکستری، مربع کای و آستانه تغییرات مقدار ویژگی‌ها استفاده می‌شود. مراحل ذکر شده تاثیر بسیار زیادی در عملکرد دسته‌بندی داشته و باعث بهبود دقت تشخیص می‌شود. در مرحله دسته‌بندی از پرکاربردترین الگوریتم‌های یادگیری ماشین برای تشخیص هرزنامه‌های تصویری استفاده می‌شود؛ همچنین پس از بدست آوردن نتایج هر دسته‌بندی به بررسی و مقایسه خروجی الگوریتم‌های بکار برده شده بر روی تصاویر هرزنامه و معتبر پرداخته می‌شود. نتایج بدست آمده نشان می‌دهد که می‌توان با کمک روش پیشنهادی به دقت تشخیص خوبی نسبت به سایر روش‌ها رسید. در بین الگوریتم‌های بررسی شده، الگوریتم شبکه عصبی بهترین عملکرد را از خود نشان می‌دهد. الگوریتم مفروض در سایر مقالات دقت تشخیص کمتری را نسبت به مقاله حاضر نشان می‌دهد اما در روش پیشنهادی به دقت تشخیص ۹۹.۲۹ درصد می‌رسد.
بازنگری مقاله: ۱۴۰۳/۰۲/۲۴	
پذیرش مقاله: ۱۴۰۳/۰۲/۲۹	
واژگان کلیدی: هرزنامه، تصویر، یادگیری ماشین، شبکه عصبی.	

DOI: <https://doi.org/10.22075/jme.2024.33366.2627>

© 2024 Published by Semnan University Press.

This is an open access article under the CC-BY 4.0 license. (<https://creativecommons.org/licenses/by/4.0/>)

۱- مقدمه

اجتماعی و شبکه‌های اشتراک فایل دیده می‌شود (Saidani, Adi, and Allili 2020) (El-Mawass, Yang et al.) (Honeine, and Vercoouter 2020) (Mubarak 2020). مطالعات زیادی در مورد هرزنامه‌ها صورت گرفته است که نشان می‌دهد، هر ساله میلیاردها دلار برای مقابله با هرزنامه هزینه می‌شود

هرزنامه نوعی سوء استفاده از سیستم انتقال پیام است که می‌تواند شامل اکثر وسایل انتشار رسانه‌ای یا سیستم‌های تحویل دیجیتال باشد. هرزنامه در رسانه‌هایی مانند ایمیل، گروه‌های خبری، موتورهای جستجو، وبلاگ‌ها، تبلیغات آنلاین، پیام‌های موبایل، انجمن‌های اینترنتی، شبکه‌های

* پست الکترونیکی نویسنده مسئول: J_mirabedini@iauctb.ac.ir

۱. گروه مهندسی کامپیوتر، واحد بروجرد، دانشگاه آزاد اسلامی، بروجرد، ایران
 ۲. گروه مهندسی کامپیوتر، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران
 ۳. گروه ریاضی و علوم کامپیوتر، دانشکده علوم پایه، دانشگاه شاهد، تهران، ایران

استناد به این مقاله:

شکاری شهرک، اعظم، میرعابدینی، سید جواد، میکاییل‌وند، ناصر، و حاج سید جوادی، سید حمید. (۱۴۰۳). بهبود تشخیص هرزنامه‌های تصویری با استفاده از روشی نوین در انتخاب ویژگی‌های بافت تصویر. مدل سازی در مهندسی، ۲۲(۷۹)، ۲۱۱-۲۲۱. doi: 10.22075/jme.2024.33366.2627

هرزنامه‌های تصویری ارائه می‌شود.

ساختار مقاله بدین صورت است که در بخش ۲ مقالات ارائه شده در زمینه پژوهش بررسی می‌شوند. در بخش ۳ روش پیشنهادی بیان می‌شود و به تشریح الگوریتم‌های بکار رفته پرداخته می‌شود؛ همچنین در این بخش مجموعه داده مورد استفاده بیان می‌شود. نتایج حاصل از اجرای روش پیشنهادی نیز در بخش ۴ بررسی می‌شود. در نهایت در بخش ۵، نتیجه‌گیری از روش پیشنهادی مطرح می‌شود.

۲- سوابق تحقیق

در عصر اطلاعات، شاهد تولید روزافزون اطلاعات به شکل‌های گوناگون می‌باشیم. تصویر از جمله اشکال ارائه اطلاعات می‌باشد؛ لذا برای رسیدن به دانش و استفاده مفید از تصاویر، نیاز به پردازش آن می‌باشد. هر تصویر شامل مجموعه‌ای از نقاط می‌باشد. هر نقطه بسته به ابعاد تصویر و رنگی یا خاکستری بودن آن، می‌تواند مقادیر خاصی را داشته باشد. روش‌های متفاوتی برای پردازش تصویر ارائه شده است (Salih and Dhannoon 2021). استخراج ویژگی‌ها اولین مرحله پردازش می‌باشد. الگوریتم تشخیص کاراکترهای نوری یکی از روش‌های استخراج ویژگی است. استفاده از ویژگی‌های سطح پایین نیز یکی دیگر از روش‌های کاربرد در پردازش تصاویر می‌باشد (Imam, Vassilakis, and Kolovos 2022).

استفاده از ویژگی‌های سطح پایین زمانی کارایی دارد که الگوریتم تشخیص کاراکترهای نوری Character Recognition قادر به تشخیص کاراکترهای داخل تصویر نباشد. دلایلی مانند اعمال نویزها، مبهم کردن محتوا و یا استفاده از کلمات تغییر شکل داده شده در تصویر، می‌تواند از جمله علل عدم تشخیص باشد (Sayallar, Sayar, and Babalık 2023). برای رفع این مشکل می‌توان با کمک ویژگی‌های سطح پایین به توصیف ویژگی‌های تصویر پرداخته و با تجزیه و تحلیل بافت تصویر به فیلتر هرزنامه‌های تصویری پرداخت (Sun et al. 2022).

یکی از روش‌های کاربرد در این زمینه، استفاده از هیستوگرام خاکستری یا رنگی می‌باشد که با کمک آن تصویر تحلیل می‌شود. هیستوگرام به اندازه‌گیری و شمارش شدت رنگ نقاط می‌پردازد. در هیستوگرام، محور افقی میزان روشنایی و محور عمودی تعداد نقاط را نمایش می‌دهد (Yaseen, Abbas, and Sana 2020) بنابراین می‌توان مدلی را ارائه کرد که از رنگ برای دسته‌بندی تصویر

(Tian et al. 2020) (Bosaeed, Katib, and Mehmood 2020) (Sun et al. 2022) (You et al. 2020) . از

دیگر مشکلاتی که وجود هرزنامه می‌تواند به همراه داشته باشد می‌توان به اتلاف ترافیک، فضای ذخیره‌سازی و قدرت محاسباتی اشاره نمود. همچنین هرزنامه علاوه بر ایجاد مزاحمت برای کاربران، می‌تواند حاوی موارد مخرب مانند ویروس نیز باشد؛ لذا توجه و مقابله با این پدیده ضروری می‌باشد.

در راستای مقابله با هرزنامه، اولین قدم تعیین ویژگی‌های کلیدی می‌باشد. طبق تحقیقات انجام شده، برای بررسی ویژگی‌ها، دو رویکرد مبتنی بر ویژگی‌های محتوایی و ویژگی‌های غیرمحتوایی مشاهده می‌شود. معمولاً متناسب با شرایط، امکانات و ویژگی‌هایی که قابل دسترس می‌باشند، یکی از رویکردها انتخاب می‌شود.

در رویکرد مبتنی بر محتوا، تمرکز بر روی متن پیام است و عمل فیلترینگ در سمت کاربر اتفاق می‌افتد. در این رویکرد به تجزیه و تحلیل محتوای پیام پرداخته می‌شود؛ لذا حریم خصوصی افراد نقض می‌شود اما کم هزینه‌ترین و پرکاربردترین روش در فیلتر هرزنامه‌ها می‌باشد (Komarasamy et al. 2023).

در رویکرد غیرمحتوایی، بر روی مشخصات شبکه، موقعیت مکانی و فرستنده پیام تمرکز می‌شود. این نوع فیلترینگ بیشتر در سمت سرور اتفاق می‌افتد و اغلب برای شناسایی هرزنامه‌نویس بکار می‌رود.

نوآوری‌هایی که در پژوهش حاضر در زمینه تشخیص هرزنامه صورت می‌گیرد عبارتند از:

- در استخراج ویژگی‌ها از ۲۲ ویژگی بافت تصویر استفاده می‌شود. تاکنون در هیچ مقاله‌ای ۲۲ ویژگی بافت تصویر به صورت یکجا بکار گرفته نشده است.
- انتخاب ویژگی‌های کلیدی با روشی ترکیبی انجام می‌گیرد. روش مذکور شامل بررسی روابط بین ویژگی‌ها، ماتریس هم‌رخداد سطح خاکستری و مربع کای می‌باشد. مرحله ذکر شده باعث بهبود عملکرد الگوریتم‌ها در تشخیص و دسته‌بندی می‌شود.
- روش پیشنهادی بر روی الگوریتم‌های پرکاربرد یادگیری ماشین بکار می‌رود. در انتها عملکرد الگوریتم‌های مورد استفاده در پژوهش، بررسی و مقایسه می‌شوند.
- در نهایت مناسب‌ترین الگوریتم جهت تشخیص

محل قرارگیری نقاط پرارزش تصاویر را نشان می‌دهد. به عبارت دیگر بافت، تصویر را بسته به تعداد جفت پیکسل‌های تصویر با مقادیر شدت معینی که در روابط فضایی خاصی مرتب شده اند، توصیف می‌کند. در ماتریس مذکور ۲۲ ویژگی بافت تصویر مورد بررسی قرار می‌گیرد که در ادامه برخی از آن‌ها ذکر می‌شوند (Abuzaid, and Abuhammad 2022):

۳-۱- انرژی

این ویژگی با کمک فرمول (۱) قابل محاسبه می‌باشد و به عنوان یکنواختی یا ممان دوم زاویه نیز شناخته می‌شود و از جمع مربعات ورودی‌ها در ماتریس GLCM بدست می‌آید. i_1 ابعاد تابع پیکسل‌های ماتریس $P(i,j)$ هستند. زمانی که یکنواختی تصویر خوب باشد یا پیکسل‌ها شبیه باشند، مقدار این ویژگی زیاد است.

$$Energy = \sum_i \sum_j p(i,j)^2 \quad (1)$$

۳-۲- همگونی

فرمول (۲) بیان‌گر همگونی یا ممان تفاضل معکوس، یک‌جورسازی محلی می‌باشد و زمانی که سطح خاکستری محلی، یکنواخت باشد، مقدار آن زیاد می‌شود؛ لذا اگر تصاویر هرزنامه، همگونی یکسانی داشته باشند، می‌توان برای تفکیک آن از تصاویر معتبر استفاده کرد.

$$Homogeneity = \sum_i \sum_j \frac{p(i,j)}{1 + |i - j|} \quad (2)$$

۳-۳- آنترپی

آنترپی میزان اطلاعات از دست رفته از تصویر را اندازه‌گیری می‌کند و با کمک فرمول (۳) قابل اندازه‌گیری می‌باشد.

$$Entropy = - \sum_i \sum_j p(i,j) \cdot \log(p(i,j)) \quad (3)$$

۳-۴- تفاوت روشنایی بین پیکسل‌ها

کنتراست معیاری از شدت تفاوت روشنایی بین پیکسل‌ها و همسایگی آن‌ها در کل تصویر می‌باشد. جهت محاسبه کنتراست از فرمول (۴) می‌توان استفاده نمود.

$$Contrast = \sum_i \sum_j |i - j|^2 p(i,j) \quad (4)$$

در فرمول‌های فوق $P(i,j)$ برابر با احتمال مولفه سطر i ام و ستون j ام ماتریس GLCM است.

استفاده شود (Salih and Dhannoon 2021). از طرف دیگر هیستوگرام شیب‌های جهت‌دار نیز با ارائه برداری از ویژگی‌های تصویر، می‌تواند روشی برای تشخیص و دسته‌بندی تصویر باشد (Jelodar, Mirabedini, and Haroonabadi 2015).

فیلترینگ هرزنامه می‌تواند به دو صورت دسته‌بندی و خوشه‌بندی صورت گیرد. روش دسته‌بندی در زمینه تشخیص هرزنامه بسیار پرکاربردتر از خوشه‌بندی می‌باشد؛ لذا فیلترینگ هرزنامه‌های تصویری از جمله کاربردهای دسته‌بندی به حساب می‌آید که امروزه بسیار مورد توجه قرار گرفته است (Jelodar, Mirabedini, and Haroonabadi 2015) و (Sadia et al. 2023). در بین روش‌های دسته‌بندی نیز روش‌های یادگیری ماشین بسیار پرکاربردتر از روش‌های یادگیری عمیق می‌باشند (Hossain, Uddin, and Halder 2021) و (Srinivasan et al. 2020). زیرا روش‌های یادگیری عمیق دارای پیچیدگی بالایی هستند، لذا سربار پردازشی دارند؛ اما دقت بهتری نسبت به روش‌های یادگیری ماشین دارند. بنابراین این پژوهش به دنبال یافتن راهی است تا بتواند هم پیچیدگی پردازش را کم کند و هم دقت تشخیص را بالا ببرد.

پژوهش حاضر، با توجه به اهمیت تصاویر و کاربردهای مختلف آن در تبادل اطلاعات، به دنبال ارائه راه‌کاری است تا با استفاده از رویکردی ترکیبی و جدید در حیطه یادگیری ماشین، به دنبال افزایش دقت تشخیص هرزنامه با کمترین پیچیدگی باشد (Abuzaid, and Abuhammad 2022). برای درک بهتر از مطالب ذکر شده در بخش سوابق تحقیق در جدول ۱ (روش پیشنهادی مقالات مذکور در بخش سوابق تحقیق) مقالات ذکر شده بطور مختصر تشریح می‌شوند.

۳- روش پیشنهادی

بافت، یک ویژگی بینایی یا لمسی از یک سطح می‌باشد؛ همچنین یک ویژگی مهم برای توصیف قسمت‌های مختلف یک تصویر است. هدف از بررسی بافت، پیدا کردن یک روش واحد برای توصیف ویژگی‌های اساسی و نمایش آن‌ها در چند فرم واحد و ساده می‌باشد که می‌تواند برای دسته‌بندی دقیق بکار رود.

برای این منظور از ماتریس هم‌رخداد سطوح خاکستری (GLCM) استفاده می‌شود. این ماتریس اطلاعات مربوط به

مقاله	مدل
جدول ۱- روش پیشنهادی مقالات مذکور در بخش سوابق تحقیق	
Komarasamy) (et al. 2023	این تحقیق، دقت تشخیص در ایمیل‌های هرز تصویری را به ۹۹٪ افزایش می‌دهد. در روش پیشنهادی از الگوریتم‌های RF, DT, KNN, SVM, NB و CNN استفاده می‌شود؛ همچنین از VGG-16 که یکی از مدل‌های CNN می‌باشد، برای استخراج ویژگی استفاده می‌شود.
Salih and) Dhannoon (2021	هدف پژوهش تشخیص هرزنامه در متن، ویژگی‌های تصویری و OCR می‌باشد. از مجموعه داده ISH استفاده می‌شود. برای دسته‌بندی Weighted K-NN بکار می‌رود و از GLCM برای استخراج ویژگی استفاده می‌شود. دقت تشخیص در روش پیشنهادی ۹۱٪ می‌باشد.
Imam,) Vassilakis, and Kolovos (2022	هدف تحقیق اصلاح غلط املائی در هرزنامه‌های شبکه اجتماعی می‌باشد. پژوهش با کمک OCR، ۵ غلط‌گیر، MCS و FRB انجام می‌شود. روش پیشنهادی شامل سه مرحله جستجو، بررسی و اصلاح می‌باشد و برای بدست آوردن نتایج از سه مجموعه داده استفاده می‌شود. مقاله دقت تشخیص ۹۱٪ را بدست می‌آورد.
Sayallar,) Sayar, and (Babalık 2023	مقاله به خواندن رسیدهای دیجیتالی با کمک روش OCR می‌پردازد. در این تحقیق از مجموعه داده‌ای شامل رسیدهای ترکیه‌ای استفاده می‌شود. تشخیص متن مورد نظر با کمک ماتریسی که از تصویر بدست می‌آید، صورت می‌پذیرد. از الگوریتم C-RNN جهت خواندن استفاده می‌شود؛ برای این کار ابتدا مناطق حاوی متن تشخیص داده می‌شوند و سپس تشخیص متن انجام می‌گیرد.
Sun et al.) (2022	هدف پژوهش پردازش تصویر با استفاده از روش تقسیم‌بندی دقیق لبه‌های جسم می‌باشد. روش پیشنهادی برای سنجش تصاویر از راه دور استفاده
Yaseen,) Abbas, and (Sana 2020	این مدل ترکیبی از تشخیص نوری کاراکتر، پردازش زبان طبیعی و الگوریتم یادگیری ماشین است. مجموعه داده مورد استفاده در پژوهش Mark Dredze می‌باشد. در این پژوهش دسته‌بندی تصاویر انجام می‌شود و هدف تشخیص متن نامعتبر درون تصاویر است. الگوریتم‌های بکار برده شده عبارتند از OCR، NLP و ML. دقت تشخیص در این مدل ۹۸٪ می‌باشد.
Jelodar,) Mirabedini, and Haroonabadi (2015	هدف تحقیق فیلتر وب سایت‌های تبلیغاتی در موتورهای جستجو است که با کمک ویژگی‌های آدرس اینترنتی و تعداد کلمات کلیدی انجام می‌شود. در مرحله دسته‌بندی از الگوریتم فازی استفاده می‌شود. ارزیابی روش پیشنهادی نیز با ابزار FIS در نرم‌افزار متلب انجام می‌شود.
Sadia et al.) (2023	در این مقاله تشخیص هرزنامه در توییتر با کمک مجموعه داده جمع‌آوری شده، انجام می‌گیرد. دسته‌بندی با استفاده از الگوریتم‌های LR, DT, SVM, NB و KNN صورت گرفته و پژوهش به دقت ۸۹٪ می‌رسد.
Hossain,) Uddin, and (Halder 2021	مقاله برای تشخیص ایمیل‌های هرزنامه از مجموعه داده UCI و الگوریتم‌های MNB, RF, KNN, GB, RNN, GD و ANN استفاده می‌شود. پژوهش به مقایسه ای بین الگوریتم‌های یادگیری ماشین و عمیق می‌پردازد.
Srinivasan et) (al. 2020	هدف تحقیق طبقه‌بندی هرزنامه‌های تصویری می‌باشد و با الگوریتم‌های یادگیری عمیق (VGG19) و (Xception) و یادگیری ماشین (SVM, RF, AB و KNN) و همچنین با کمک ۳ مجموعه داده (Dredze, ISH) و مجموعه داده تولیدی پژوهش انجام می‌شود. روش پیشنهادی به دقت ۹۹٪ می‌رسد.

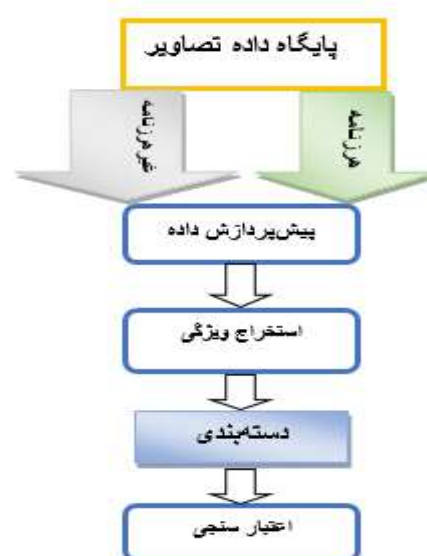
۳-۵- مجموعه داده

در این پژوهش از مجموعه داده ISH (ImageSpanHunter) استفاده می‌شود که از طریق

لینک

https://www.cs.jhu.edu/~mdredze/datasets/image_spam/ قابل دسترس است. این مجموعه داده شامل دو فایل می‌باشد. فایل personal_image_spam شامل ۳۲۹۹ تصویر هرزنامه و فایل personal_image_ham شامل ۲۰۲۱ تصویر معتبر می‌باشد.

در شکل (۱) فلوجارت روش پیشنهادی نمایش داده می‌شود.



شکل ۱- فلوجارت روش پیشنهادی

همان‌طور که در شکل (۱) مشاهده می‌شود مجموعه داده شامل دو فایل از تصاویر هرزنامه و معتبر می‌باشد که بصورت تصادفی بخشی از آن‌ها برای آموزش و بخشی دیگر برای آزمایش در نظر گرفته می‌شود. در روش پیشنهادی ابتدا بر روی تصاویر پیش‌پردازش صورت می‌گیرد و برای تسهیل در پردازش داده‌ها و وابسته نبودن پردازش به ابعاد عکس‌ها، تمام تصاویر به سایز 400×400 تغییر اندازه داده می‌شوند. سپس استخراج ویژگی‌های تصاویر انجام می‌شود.

برای استخراج ویژگی‌ها از ماتریس GLCM استفاده می‌شود. در حالت پیش‌فرض دو پیکسلی که به صورت افقی در کنار هم هستند، همسایه در نظر گرفته می‌شوند. این مقدار در زمان تنظیم offset مشخص می‌شود که در حالت پیش‌فرض $offset = [0 \ 1]$ می‌باشد، یعنی دو پیکسلی که

صفر سطر و ۱ ستون با هم فاصله دارند، همسایه هستند به عبارت دیگر همسایگی افقی دارند.

معمولاً offset را با یک زاویه معرفی می‌کنند که در حالت همسایگی افقی زاویه offset صفر درجه است. فاصله جهت‌یابی نیز به ازای هر پیکسل نسبت به پیکسلی که با زاویه صفر از آن قرار دارد، محاسبه می‌شود؛ به عبارت دیگر $\theta=0$ است. همچنین مناسب‌ترین تعداد سطوح خاکستری با توجه به نتایج بدست آمده در پژوهش‌های گذشته، ۶۴ در نظر گرفته می‌شود. پس از استخراج ماتریس، مقادیر به عنوان ورودی به توابع مورد نظر داده می‌شوند و مقدار ویژگی‌های مورد نظر بدست می‌آیند.

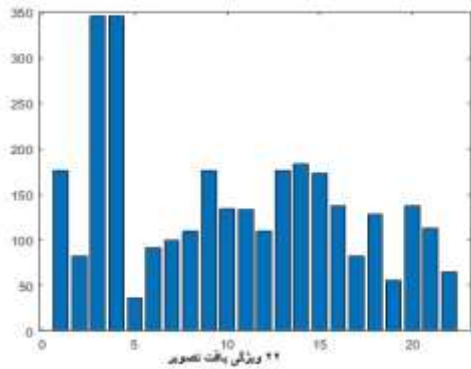
ویژگی‌های کلیدی براساس ماتریس GLCM و روابط بین آن‌ها انتخاب می‌شوند. در مرحله انتخاب کلیدها، ابتدا با کمک روش مربع کای، ویژگی‌های مذکور به ازای تصاویر معتبر و هرزنامه مقایسه می‌شوند و سپس بصورت نزولی مرتب و در نهایت ویژگی‌هایی که مقادیرشان بالاتر از آستانه تعریف شده باشد، انتخاب می‌شوند.

در مرحله بعد، نوبت به دسته‌بندی می‌رسد لذا ویژگی‌های انتخاب شده به عنوان ورودی به دسته‌بندها داده می‌شوند. در این پژوهش جهت دسته‌بندی، از پرکاربردترین الگوریتم‌های یادگیری ماشین و شبکه عصبی (NN) استفاده می‌شود. در بین الگوریتم‌های یادگیری ماشین درخت تصمیم، بی‌زین ساده و نزدیک‌ترین همسایه بسیار پرکاربرد هستند. در گام بعد خروجی الگوریتم‌های بکار رفته مورد بررسی قرار می‌گیرند. الگوریتم‌های مورد استفاده در این پژوهش عبارتند از: KNN، DT، LDA، NB و NN. در ابتدا روش پیشنهادی توسط درصدهای متفاوتی از مجموعه داده آموزش می‌بیند. دسته‌بندی بر روی داده‌های ورودی انجام و تصویر ورودی در یکی از دو دسته هرزنامه یا معتبر قرار می‌گیرد. آموزش ماشین پس از مرحله دسته‌بندی پایان می‌پذیرد.

در مرحله آزمایش عملیات بر روی باقی‌مانده مجموعه داده صورت می‌پذیرد؛ همچنین برای اعتبارسنجی از معیار Kfold استفاده می‌شود که در آن $K=4$ می‌باشد. در نهایت بهترین الگوریتم در روش پیشنهادی معرفی می‌شود.

۴- پیاده‌سازی و نتایج روش پیشنهادی

در این بخش مباحث مربوط به پیاده‌سازی و نتایج حاصل از آن تشریح می‌شود.



شکل ۴- میزان اختلاف ۲۲ ویژگی در تصاویر معتبر و هرز با کمک روش پیشنهادی

همان طور که در شکل (۴) ملاحظه می شود، برخی ویژگی ها از لحاظ تفکیف پذیری خیلی خوب عمل می کنند. می توان به وضوح دید که در ویژگی های ۱، ۳، ۴، ۹، ۱۳، ۱۴ و ۱۵ اختلاف میان نتایج بدست آمده از تصویر معتبر و هرزنامه بسیار متفاوت می باشد؛ بنابراین این ویژگی ها قابلیت تفکیک پذیری بالایی را دارند و به عنوان ویژگی های کلیدی انتخاب شده و به دسته بندها داده می شوند. البته ویژگی هایی که انتخاب می شوند کاملاً معقولانه هستند؛ زیرا به عنوان مثال آنتروپی بیانگر میزان بی نظمی در نقاط خاکستری در تصویر است که طبیعتاً در تصاویر معتبر مقدار نظم در نقاط بالاتر از هرزنامه است مانند تصاویری از مجموعه داده که قبلاً نمایش داده شدند.

۴-۲- دسته بندی

کلیدهای بدست آمده در مرحله قبل، ورودی های دسته بندها می شوند و به ازای درصدهای مختلفی از مجموعه داده بررسی می شوند.

جدول (دقت تشخیص دسته بندها به ازای درصدهای مختلفی از مجموعه داده) درصد تشخیص دسته بندها را نمایش می دهد. همان طور که مشاهده می شود، ۰.۶ و ۰.۷ از داده های ورودی برای آموزش و باقی مجموعه داده برای آزمایش روش پیشنهادی در نظر گرفته می شود.

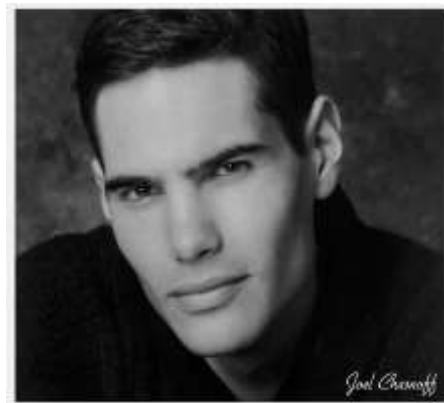
جدول ۲- دقت تشخیص دسته بندها به ازای درصدهای

مختلفی از مجموعه داده

Model	M=0.7	M=0.6
KNN	0.9915	0.9885
NB	0.9266	0.9218
DT	0.9837	0.9811
LDA	0.9301	0.9325
NN	0.9929	0.9918

۴-۱- استخراج ویژگی

استخراج ویژگی یکی از مهم ترین مراحل در پردازش داده ها می باشد. همان طور که قبلاً ذکر شد، در اولین گام اندازه تصاویر یکسان می شود تا بدست آمدن نتایج صحیح، وابسته به اندازه تصاویر نباشد. در مرحله استخراج ویژگی نیز از بافت تصویر استفاده می شود و با کمک فرمول هایی که در پیوست ۱ بیان می شود، مقادیر محاسبه می شوند. شکل (۲) یکی از تصاویر معتبر موجود در پایگاه داده نشان می دهد.



شکل ۲- تصویر معتبر

شکل (۳) نیز نمونه ای از تصاویر هرزنامه موجود در پایگاه داده می باشد.



شکل ۳- هرزنامه

در مرحله بعد با کمک روش مربع کای ابتدا میزان جهش مقادیر در بین ۲۲ ویژگی مفروض بدست می آید. این عمل به ازای تصاویر معتبر و هرزنامه انجام می شود. سپس میانگین مقادیر محاسبه و آستانه ای جهت انتخاب کلیدها تعیین می شود. در نهایت مقادیر مرتب سازی شده و ویژگی های کلیدی انتخاب می شوند.

داده می‌شود و بیشتر برای داده‌های نامتوازن کاربرد دارد.

$$F1 - Score = 2 \times \frac{Precision \cdot Recall}{Precision + Recall} \quad (9)$$

- پارامترهایی که در فرمول‌های فوق ذکر شده‌اند از طریق ماتریس سردرگمی قابل محاسبه می‌باشد. ماتریس مذکور یک جدول دو بعدی است که شامل مقادیر واقعی و پیش‌بینی شده برای دسته‌بندی می‌باشد. در فرمول‌های فوق، TP نشان می‌دهد که چه میزان از هرزنامه‌ها به درستی در دسته هرزنامه قرار گرفته‌اند. TN نیز بیانگر این است که چقدر از پیام‌های معتبر به درستی در دسته‌بندی شده‌اند؛ در مقابل عبارت FP میزان هرزنامه‌هایی که به اشتباه دسته‌بندی شده‌اند و FN نیز میزان پیام‌های معتبری را نشان می‌دهد که در دسته اشتباهی قرار گرفته‌اند. در ادامه هر دسته‌بند بطور مجزا مورد بررسی قرار می‌گیرد.
- NB: همان‌طور که در جدول (معیارهای ارزیابی طبقه بند بیزین ساده به ازای درصدهای مختلفی از مجموعه داده) مشاهده می‌شود در تمامی آموزش‌ها دقت تشخیص بیش از ۹۰ درصد را نشان می‌دهد؛ بنابراین می‌توان گفت روش پیشنهادی با کمک الگوریتم بیزین بسیار خوب جواب می‌دهد و الگوریتم بیزین به عنوان یکی از بهترین الگوریتم‌ها جهت تشخیص هرزنامه در روش پیشنهادی به حساب می‌آید.

جدول ۳- معیارهای ارزیابی طبقه بند بیزین ساده به ازای درصدهای مختلفی از مجموعه داده

	NB	K=0.7	K=0.6
Cross Validation		0.0764	0.0805
Precision		0.7371	0.6953
Recall		0.6460	0.6138
Accuracy		0.9266	0.9218
Specificity		0.9669	0.9636
F1-Score		0.6886	0.6520

- DT: در جدول (معیارهای ارزیابی طبقه‌بند درخت تصمیم به ازای درصدهای مختلفی از مجموعه داده) نشان داده می‌شود که این دسته‌بند دارای نوسان کمی می‌باشد اما عملکرد بهتری نسبت به الگوریتم NB دارد.

همان‌طور که ملاحظه می‌شود، استخراج ویژگی به نحوی مجموعه داده را آماده می‌کند که تمام الگوریتم‌های مورد بررسی به دقت تشخیص بالای ۹۰ درصد می‌رسند. کیفیت استخراج ویژگی تصاویر در این پژوهش بسیار مهم است و مزیت اصلی روش پیشنهادی را بیان می‌کند.

در پژوهش حاضر جهت بررسی عملکرد دسته‌بندها از ۶ معیار استفاده می‌شود. معیارهای مفروض عبارتند از: Cross Validation, Precision, Recall, Accuracy, Specificity و F1-Score. در ادامه هر کدام بصورت مختصر شرح داده می‌شود.

- معیار اعتبار سنجی متقابل (Cross Validation) داده‌ها را به K دسته تقسیم می‌کند و آزمایش K بار تکرار می‌شود. در هر بار آزمایش یکی از دسته‌ها برای تست و باقی دسته‌ها برای آموزش استفاده می‌شوند. با کمک این معیار در مجموعه داده‌های کوچک، نتیجه مطمئن‌تری به دست می‌آید.
- فرمول (۵) معیار یادآوری را نشان می‌دهد که بیان می‌کند چقدر از کل نمونه‌ها به درستی به عنوان هرزنامه تشخیص داده شده‌اند.

$$Recall = \frac{TP}{TP + FN} \quad (5)$$

- معیار دقت در فرمول (۶) میزان هرزنامه‌هایی که در دسته به درستی تشخیص داده شده‌اند را نشان می‌دهد.

$$Precision = \frac{TP}{TP + FP} \quad (6)$$

- معیار اختصاصی بودن نیز در فرمول (۷) نشان می‌دهد که چه میزان از تصاویر معتبر به درستی دسته‌بندی شده‌اند.

$$Specificity = \frac{TN}{TN + FP} \quad (7)$$

- معیار صحت که در فرمول (۸) نمایش داده می‌شود، درصد کل تشخیص‌های درست روش پیشنهادی را بیان می‌کند.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (8)$$

- معیار F1-Score میانگین هندسی از معیارهای صحت و دقت می‌باشد که در فرمول (۹) نمایش

• **KNN**: دسته‌بند **K** نزدیک‌ترین همسایه، نوسان زیادی از خود نشان می‌دهد؛ اما مطابق جدول معیارهای ارزیابی طبقه‌بند نزدیک‌ترین همسایه به ازای درصدهای مختلفی از مجموعه داده) دارای دقت تشخیص خوب و بالای ۹۰ درصد می‌باشد.

جدول ۷- معیارهای ارزیابی طبقه‌بند نزدیک‌ترین همسایه به ازای درصدهای مختلفی از مجموعه داده

	KNN	K=0.7	K=0.6
Cross Validation		0.0377	0.0495
Precision		0.9560	0.9396
Recall		0.9775	0.9655
Accuracy		0.9915	0.9885
Specificity		0.9935	0.9916
F1-Score		0.9666	0.9524

۵- نتیجه‌گیری

در این پژوهش جهت تشخیص تصاویر هرزنامه، از ویژگی‌های محتوایی تصاویر استفاده می‌شود. لذا ۲۲ ویژگی از تصاویر استخراج می‌شوند؛ سپس با روشی ترکیبی توسط ماتریس GLCM، روش مربع کای و بررسی روابط بین مقادیر ویژگی‌ها در تصاویر معتبر و هرزنامه، انتخاب ویژگی‌های کلیدی صورت می‌گیرد. در مرحله بعد با استفاده از دسته‌بندهای مختلف عمل تشخیص و دسته‌بندی تصاویر به دو دسته هرزنامه و معتبر صورت می‌پذیرد.

روش پیشنهادی، رویکردی جدید در شناسایی تصاویر هرزنامه می‌باشد زیرا تا کنون از ۲۲ ویژگی بافت تصویر به صورت یکجا برای شناسایی تصاویر هرزنامه استفاده نشده است؛ از طرف دیگر با کمک روش ترکیبی ارائه شده برای تعیین کلمات کلیدی، به دقت بالایی در تشخیص می‌توان رسید؛ همچنین استفاده از ویژگی‌های محتوایی بر روی تصاویر گرچه زمان پیش‌پردازش و استخراج ویژگی‌ها را بالا می‌برد اما در دسته‌بندی نتایج بسیار خوبی را نشان می‌دهد. مقایسه نتایج بدست آمده از روش پیشنهادی نسبت به روش‌های قبل بیانگر این می‌باشد که روش پیشنهادی با دقت بسیار خوبی دسته‌بندی می‌کند. این پژوهش با استفاده از الگوریتم NN و ویژگی‌های بافت تصویر، می‌تواند به دقت ۹۹.۲۹ درصدی برای تشخیص هرزنامه‌های تصویری برسد. همان‌طور که در جدول ۸ مشاهده می‌شود، سایر پژوهش‌ها به این دقت از تشخیص نرسیده‌اند.

جدول ۴- معیارهای ارزیابی طبقه‌بند درخت تصمیم به ازای درصدهای مختلفی از مجموعه داده

DT	K=0.7	K=0.6
Cross Validation	0.0411	0.0497
Precision	0.9281	0.9296
Recall	0.9438	0.9103
Accuracy	0.9837	0.9811
Specificity	0.9895	0.907
F1-Score	0.9359	0.9199

• **NN**: همان‌طور که در جدول (معیارهای ارزیابی طبقه‌بند شبکه عصبی به ازای درصدهای مختلفی از مجموعه داده) مشاهده می‌شود الگوریتم شبکه عصبی در کلیه معیارها نتایج مطلوبی را نشان می‌دهد و در هر دو موردی که بررسی شد، دارای دقت تشخیص بالای ۹۹ درصد می‌باشد.

جدول ۵- معیارهای ارزیابی طبقه‌بند شبکه عصبی به ازای درصدهای مختلفی از مجموعه داده

NN	K=0.7	K=0.6
Precision	0.9719	0.9787
Recall	0.9719	0.9517
Accuracy	0.9929	0.9918
Specificity	0.9959	0.9972
F1-Score	0.9719	0.9650

• **LDA**: این دسته‌بند با اینکه دقت تشخیص بالای ۹۰ درصد را دارد اما با افزایش داده‌های ورودی سیر نزولی را نشان می‌دهد؛ لذا در جدول (معیارهای ارزیابی در طبقه‌بند آنالیز تشخیص خطی) قابل مشاهده است که برای داده‌های کم عملکرد بهتری از خود نشان می‌دهد.

جدول ۶- معیارهای ارزیابی در طبقه‌بند آنالیز تشخیص خطی

LDA	K=0.7	K=0.6
Cross Validation	0.0755	0.0798
Precision	0.7801	0.7944
Recall	0.6179	0.5862
Accuracy	0.9301	0.9325
Specificity	0.9749	0.9794
F1score	0.6896	0.6746

جدول ۸- جدول مقایسه دقت تشخیص در مقالات

Studies	Model	Accuracy
Proposed Method	NN	99.26
[20]	ETC (Extra tree classifier)	97.77
[21]	SVM	98.56

- الگوریتم NN بر روی تصاویر خوب کار می‌کند و در هر دو مورد دقت تشخیص بالای ۹۹٪ می‌باشد.
- الگوریتم DT عملکرد خوبی داشته و توانسته است به دقت ۹۸ درصد برسد.
- الگوریتم LDA، سیر نزولی دارد و برای داده‌های تعداد کم، به دقت تشخیص خوبی می‌رسد. این الگوریتم با وجود میانگین تشخیص حدود ۸۰٪ بالاترین مقدار واریانس را از خود نشان می‌دهد. از جمله اشکالاتی که در مدل پیشنهادی وجود دارد این است که موارد جدید پیش‌بینی و تشخیص داده شده به مجموعه داده قبلی اضافه نمی‌شوند و مجموعه داده بروزرسانی نمی‌شود؛ بنابراین تکرار مدل تأثیری در بهبود روند تشخیص نمی‌تواند داشته باشد. با افزودن این قابلیت می‌توان مدل پیشنهادی را بهبود داد.
- به عنوان پیشنهاد برای پژوهش‌های آتی می‌توان موارد زیر را نیز در نظر گرفت:
- در این پژوهش تصاویر بصورت یکپارچه در نظر گرفته شده‌اند. می‌توان در پژوهش آتی متون درون تصاویر را نیز به صورت مجزا مورد بررسی قرار داد.
- روش پیشنهادی را می‌توان با کمک الگوریتم‌های یادگیری عمیق و تکاملی نیز بررسی نمود.
- می‌توان روش پیشنهادی را بر روی پردازنده‌های موازی نیز جهت بهبود عملکرد و افزایش سرعت تشخیص به کار برد تا بررسی شود که آیا مدل پیشنهادی قابلیت استفاده برای دنباله‌های داده‌ای را دارد یا خیر.

- در (Sumathi, and Raja 2023) برای انتخاب ویژگی‌های کلیدی، یک جنگل تصادفی با کمک مجموعه‌ای از درخت‌های تصمیم ایجاد می‌شود. دسته‌بندی نیز با کمک رای‌گیری از نتایج چندین الگوریتم یادگیری ماشین مانند KN, NB, ETC, RF, SVC, LR, XGB, DT, and VC انجام می‌شود.
 - در (KAŞOĞLU, and YAMAN 2023) استخراج ویژگی مبتنی بر LBP و با کمک روش‌های آماری انجام می‌شود. مجموعه داده استفاده شده در پژوهش مذکور نیز مانند مجموعه داده مورد استفاده در روش پیشنهادی ISH می‌باشد. در این مقاله، پس از استخراج ویژگی از الگوریتم SVM جهت دسته‌بندی استفاده می‌شود؛ اما همان‌طور که ملاحظه می‌شود به دقت تشخیص پایین‌تری نسبت به روش پیشنهادی می‌رسد.
- با توجه به خروجی روش پیشنهادی می‌توان به نتایج زیر رسید:

مراجع

- [1] N. Saidani, K. Adi, and M.S. Allili. "A semantic-based classification approach for an enhanced spam detection." *Computers & Security* 94 (2020): 101716.
- [2] N. El-Mawass, P. Honeine, and L. Vercoeur. "SimilCatch: Enhanced social spammers detection on twitter using Markov random fields." *Information Processing & Management* 57, no. 6 (2020): 102317.
- [3] J. Yang, T. Li, G. Liang, Y.P. Wang, T.Y. Gao, and F.D. Zhu. "Spam transaction attack detection model based on GRU and WGAN-div." *Computer Communications* 161 (2020): 172-182.
- [4] H. Mubarak, A. Abdelali, S. Hassan, and K. Darwish. "Spam detection on arabic twitter." In *Social Informatics: 12th International Conference, SocInfo 2020, Pisa, Italy, October 6-9, 2020, Proceedings 12*, pp. 237-251. Springer International Publishing, 2020.
- [5] S. Bosaeed, I. Katib, and R. Mehmood. "A fog-augmented machine learning based SMS spam detection and classification system." In *2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC)*, pp. 325-330. IEEE, 2020.
- [6] Y. Tian, M. Mirzabagheri, P. Tirandazi, and S.M. Hosseini Bamakan. "A non-convex semi-supervised approach to opinion spam detection by ramp-one class SVM." *Information Processing & Management* 57, no. 6 (2020): 102381.

- [7] L. You, Q. Peng, Z. Xiong, D. He, M. Qiu, and X. Zhang. "Integrating aspect analysis and local outlier factor for intelligent review spam detection." *Future Generation Computer Systems* 102 (2020): 163-172.
- [8] N. Sun, G. Lin, J. Qiu, and P. Rimba. "Near real-time twitter spam detection with machine learning techniques." *International Journal of Computers and Applications* 44, no. 4 (2022): 338-348.
- [9] D. Komarasamy, O. Duraisamy, S. Krishnamoorthy, S.K. Rajendran, and M.K. Dharani. "Spam Email Filtering using Machine Learning Algorithm." In *2023 7th International Conference on Computing Methodologies and Communication (ICCMC)*, pp. 1-5. IEEE, 2023.
- [10] A.M. Salih, and B.N. Dhannoon. "Weighted k-Nearest Neighbour for Image Spam Classification." *Iraqi Journal of Science* (2021): 1036-1045.
- [11] N.H. Imam, V.G. Vassilakis, and D. Kolovos. "OCR post-correction for detecting adversarial text images." *Journal of Information Security and Applications* 66 (2022): 103170.
- [12] C. Sayallar, A. Sayar, and N. Babalık. "An OCR engine for printed receipt images using deep learning techniques." *International Journal of Advanced Computer Science and Applications* 14, no. 2 (2023).
- [13] L. Sun, S. Cheng, Y. Zheng, Z. Wu, and J. Zhang. "SPANet: Successive pooling attention network for semantic segmentation of remote sensing images." *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing* 15 (2022): 4045-4057.
- [14] Y.K. Yaseen, A.K. Abbas, and A.M. Sana. "Image spam detection using machine learning and natural language processing." *Journal of Southwest Jiaotong University* 55, no. 2 (2020).
- [15] H. Jelodar, S.J. Mirabedini, and A. Haroonabadi. "Presenting a Fuzzy System for Identifying Persian Advertising Websites." *Modern Applied Science* 9, no. 1 (2015): 129.
- [16] A. Sadia, F. Bashir, R.Q. Khan, and A. Khalid. "Comparison of Machine Learning Algorithms for Spam Detection." *Journal of Advances in Information Technology* 14, no. 2 (2023): 178-184.
- [17] F. Hossain, M.N. Uddin, and R.K. Halder. "Analysis of optimized machine learning and deep learning techniques for spam detection." In *2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*, pp. 1-7. IEEE, 2021.
- [18] S. Srinivasan, V. Ravi, V. Sowmya, M. Krichen, D.B. Nouredine, S. Anivilla, and K.P. Soman. "Deep convolutional neural network based image spam classification." In *2020 6th Conference on Data Science and Machine Learning Applications (CDMA)*, pp. 112-117. IEEE, 2020.
- [19] N.N. Abuzaid, and H.Z. Abuhammad. "Image SPAM Detection Using ML and DL Techniques." *International Journal of Advances in Soft Computing & Its Applications* 14, no. 1 (2022).
- [20] M. Sumathi, and S.P. Raja. "Machine learning algorithm-based spam detection in social networks." *Social Network Analysis and Mining* 13, no. 1 (2023): 104.
- [21] A. Kaşoğlu, and O. Yaman. "LBP Feature Extraction and Statistical Pooling-Based Image Spam Detection Model." *Computer Science* 8, no. 1 (2023): 24-35.