

**'**

**پیاده‌سازی الگوریتم ماشین بردار پشتیبانی برای تشخیص ایمیل‌های اسپم**

**استاد:علی تورانی**

**دانشجویان:**

**محّمد پورقنبر مقدم 960122680113**

**امیرحسین قدس 9612268101**

**فهرست مطالب**

[1- مقدمه 1](#_Toc61269151)

[2- الگوریتم ماشین بردار پشتیبان 3](#_Toc61269152)

[3- معرفی مجموعه داده‌ی استفاده شده 9](#_Toc61269153)

[4- پیش پردازش 11](#_Toc61269154)

[5- معیار‌های ارزیابی 12](#_Toc61269155)

[6- تحلیل و ارزیابی نتایج الگوریتم پیشنهادی بر روی مجموعه داده spam base 14](#_Toc61269156)

[7- جمع‌بندی نتایج 16](#_Toc61269157)

**فهرست شکل‌ها**

[شکل 1- ترسیم داده‌ها در فضای n بعدی در الگوریتم ماشین بردار پشتیبان 3](#_Toc61294888)

[شکل 2- مرز خطی بهینه برای حالتی که دو کلاس کامل از یکدیگر جدا هستند 4](#_Toc61294889)

[شکل 3- فراوانی هرزنامه و ایمیل عادی در مجموعه داده Spam base 10](#_Toc61294890)

[شکل 4- درصد فراوانی هرزنامه و ایمیل عادی در مجموعه داده Spam base 10](#_Toc61294891)

[شکل 5- کد مربوط به بخش خواندن اطلاعات و پیش پردازش 11](#_Toc61294892)

[شکل 6- مفاهیم اولیه ارزیابی روش پیشنهادی در تشخیص ایمیل های اسپم 12](#_Toc61294893)

[شکل 7-نتایج بدست آمده توسط الگوریتم بر روی مجموعه داده spam base بر اساس چهار معیار 15](#_Toc61294894)

**فهرست جدول‌ها**

[جدول 1- توابع کرنل در ماشین بردار پشتیبان 7](#_Toc61295032)

[جدول 2- نتایج اجرای الگوریتم ها بر روی مجموعه داده spam base 14](#_Toc61295033)

1- مقدمه

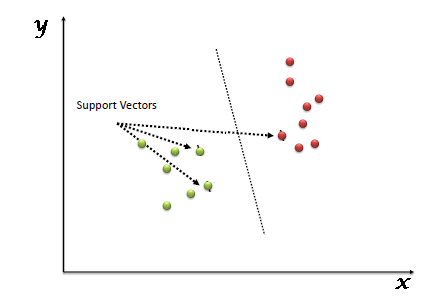
امروزه بسیاری از افراد و سازمان‌ها از ایمیل‌ها برای اهداف تجاری و تبلیغاتی استفاده می‌کنند و در نتیجه ایمیل‌های غیر ضروری در صندوق ورودی کاربران به نام اسپم ایجاد می‌شود. به طوری که ایمیل‌های اسپم یکی از مشکلات اصلی اینترنت محسوب می‌شود. علاوه بر این ایمیل‌های اسپم تأثیر منفی قابل توجهی بر افراد و سازمان‌ها دارد و باعث اتلاف جدی در منابع ، زمان ، ظرفیت ذخیره‌سازی و پهنای باند شبکه می‌شود. در کل فیلتر کردن ایمیل‌های اسپم کار پیچیده‌ای و حل آن بسیار مشکل است. تهدیدهای ایمیل‌های اسپم سالانه در حال افزایش است و بیش از 77 درصد از کل ترافیک ایمیل جهانی را به خود اختصاص داده است. در واقع ایمیل‌های اسپم منجر به استفاده غیرمجاز از منابع در سرورهای ساده انتقال ایمیل می‌شوند، زیرا آن‌ها مجبورند حجم قابل توجهی از ایمیل‌های ناخواسته را پردازش كنند.

یک روش سنتی در اکثر سیستم‌های ایمیل روش‌های ساده فیلترینگ است که می‌تواند ایمیل‌های ناخواسته را بر اساس برخی کلمات کلیدی تعریف شده توسط کاربر مسدود کند. اما این سسیتم‌های ساده به دلیل حجم بالای ایمیل‌های اسپم و تغییر زیاد در ساختار و محتوای ایمیل‌های اسپم و سایر پارامترها قادر نیستند که یک دسته‌بندی درستی از ایمیل‌های اسپم و غیر اسپم ارائه دهند. لذا نیازمند سیستمی است که به طور خودکار این کار را به دقت بالا انجام دهد. البته در سال‌های اخیر از روش‌های متفاوت برای تشخیص ایمیل‌های استفاده شده است که مهم‌ترین روش شامل: روش فیلتر مبتنی بر محتوا که معمولاً برای ایجاد قوانین فیلتر خودکار استفاده می‌شود و از الگوریتم‌های یادگیری ماشین، مانند دسته‌بندی‌کننده بیز ساده، ماشین بردار پشتیبان، شبکه‌های عصبی و غیر استفاده می‌کند. فیلتر پایه نمونه یکی از روش‌های دیگر فیلترینگ اسپم است. در این روش ابتدا، تمام ایمیل‌های اسپم از هر ایمیل کاربر با استفاده از مدل جمع‌آوری شده استخراج می‌شوند و سپس یک سری عملیات پیش پردازش و انتخاب ویژگی انجام می‌گیرد و در نهایت، الگوریتم یادگیری ماشین برای آموزش داده و تست آن‌ها برای تصمیم‌گیری در مورد این‌که آیا ایمیل‌های دریافتی اسپم یا غیر اسپم هستند استفاده می‌شود. روش‌های فیلترینگ اسپم مبتنی بر قاعده از قوانین ایجاد شده برای ارزیابی تعداد زیادی از الگوهایی ایجاد می‌شود. چندین الگوی مشابه امتیاز یک پیام را افزایش می‌دهند. در مقابل, اگر هیچ یک از الگوها همخوانی نداشته باشند, امتیاز حذف می‌شود. اما مشکل این روش‌ها این است که باید به طور مداوم قوانین جدید باید به روزسانی شود. در نهایت رویکرد مبتنی بر روش‌های فیلتر اسپم مبتنی بر شباهت که از روش‌های یادگیری ماشین مبتنی بر حافظه مانند دسته‌بند k نزدیکترین همسایه برای دسته‌بندی ایمیل‌های دریافتی بر اساس شباهت آن‌ها به نمونه‌های ذخیره‌شده استفاده می‌کند.

تکنیک‌های یادگیری ماشین توانایی یادگیری و شناسایی ایمیل‌های اسپم و پیام‌های فیشینگ از طریق تجزیه و تحلیل چنین پیام‌هایی در سراسر مجموعه وسیعی از کامپیوترها را دارند. الگوریتم‌های یادگیری ماشین با استفاده از تکنیک خودکار و انطباقی این کار را انجام می‌دهند. در واقع بسیاری از محققان از تعداد زیادی از روش طبقه‌بندی در یادگیری ماشین استفاده می‌کنند تا ایمیل‌های اسپم را فیلتر کنند. اما هنوز تحقیقات در این زمینه ادامه دارد تا تقسیم‌بندی درستی و با سرعت بالایی از ایمیل‌های اسپم را انجام دهند. لذا تاکنون بسیاری از الگوریتم‌های یادگیری ماشین برای جلوگیری از ایمیل‌های اسپم ایجاد شدند و توانسته تا حدودی زیادی به طبقه‌بندی ایمیل‌های اسپم بپردازند. در این پژوهش به پیاده سازی الگوریتم ماشین بردار پشتیبان روی مجموعه داده اسپم به نام spam base پرداخته می‌شود.

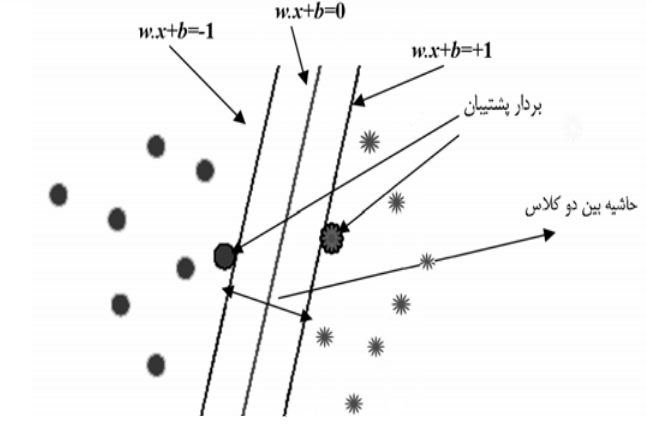
2- الگوریتم ماشین بردار پشتیبان

ماشین بردار پشتیبان[[1]](#footnote-1) یک الگوریتم نظارت‌شده یادگیری ماشین است که در سال 1979 توسط وپنیک[[2]](#footnote-2) ارائه گردید که برای مسائل طبقه‌بندی و مسائل رگرسیون قابل استفاده است. با این حال از آن بیش‌تر در مسائل طبقه‌بندی استفاده می‌شود. در الگوریتم SVM، هر نمونه داده را به عنوان یک نقطه در فضای n-بعدی روی نمودار پراکندگی داده‌ها ترسیم کرده (n تعداد ویژگی‌هایی است که یک نمونه داده دارد) و مقدار هر ویژگی مربوط به داده‌ها، یکی از مؤلفه‌های مختصات‌ نقطه روی نمودار را مشخص می‌کند. سپس، با ترسیم یک خط راست، داده‌های مختلف و متمایز از یکدیگر را دسته‌بندی می‌کند (مطابق شکل 1). به بیان ساده، بردارهای پشتیبان در واقع مختصات یک مشاهده منفرد هستند. ماشین بردار پشتیبان مرزی است که به بهترین شکل دسته‌های داده‌ها را از یکدیگر جدا می‌کند.



شکل 1- ترسیم داده‌ها در فضای n بعدی در الگوریتم ماشین بردار پشتیبان

ماشین بردار پشتیبان مبتنی بر مینیمم سازی ساختاری ریسک می‌باشد که از تئوری آموزش آماری گرفته شده است. ماشین بردار پشتیبان در واقع یک طبقه بندی کننده دودویی است. در مورد دو کلاس، روش SVM سعی دارد یک ابر صفحه ایجاد نماید که فاصله هر کلاس را تا ابرصفحه حداکثر نماید. داده‌های نقطه‌ای که به ابرصفحه نزدیک‌ تر هستند، برای اندازه‌گیری این فاصله به کار می‌روند. از این رو، این داده‌های نقطه‌ای را بردارهای پشتیبان می‌نامند. در شکل 2دو کلاس و بردارهای پشتیبان مربوط به آن‌ها نشان داده شده است.



شکل 2- مرز خطی بهینه برای حالتی که دو کلاس کامل از یکدیگر جدا هستند

فرض کنید داده‌ها از دو کلاس تشکیل شده و کلاس‌ها در مجموعه دارای Xi , i=1,2,3,…,L نقطه آموزشی باشند که Xi یک بردار است. این دو کلاس با Yi=±1 برچسب زده می‌شوند. برای محاسبه مرز تصمیم‌گیری دو کلاس کاملا جدا از هم، از حاشیه بهینه استفاده می‌شود. در این روش مرز خطی بین دو کلاس به گونه‌ای محاسبه می‌شود که:

1. تمام نمونه‌های کلاس 1+ در یک طرف مرز و تمام نمونه‌های کلاس 1- در طرف دیگر مرز واقع شوند.
2. مرز تصمیم گیری به گونه‌ای باشد که فاصله نزدیک ترین نمونه‌های آموزشی هر دو کلاس از یکدیگر در راستای عمود بر مرز تصمیم‌گیری تا جایی که ممکن است حداکثر شود.

یک مرز تصمیم‌گیری خطی را در حالت کلی می‌توان به صورت زیر نوشت:

|  |  |
| --- | --- |
| (1-1) |  |

 یک نقطه روی مرز تصمیم گیری و  یک بردار n بعدی عمود بر مرز تصمیم گیری است. b فاصله مبدا تا مرز تصمیم گیری و بیانگر ضرب داخلی دو بردارو  است. از آن جا که با ضرب یک ثابت در دو طرف (‏1‑1) باز هم تساوی برقرار است، برای تعریف یکتای مقدار b و w شرایط زیر روی آن‌ها اعمال می‌شود:

|  |  |
| --- | --- |
| (1-2) | اگر Xi یک بردار پشتیبان باشد  اگر Xi یک بردار پشتیبان نباشد |

اولین مرحله برای محاسبه مرز تصمیم گیری بهینه، پیدا کردن نزدیک‌ترین نمونه‌های آموزشی دو کلاس است. در مرحله بعد فاصله آن نقاط از هم در راستای عمود بر مرزهایی که دو کلاس را به طور کامل جدا می‌کنند محاسبه می‌شود. مرز تصمیم‌گیری بهینه، مرزی است که حداکثر حاشیه را داشته باشد. مرز تصمیم‌گیری بهینه با حل مسئله بهینه‌سازی زیر محاسبه می‌شود:

|  |  |
| --- | --- |
| (1-3) |  |

با توجه به (‏1‑3) و انجام یک سری عملیات ریاضی، رابطه بالا به رابطه زیر تبدیل می‌شود:

|  |  |
| --- | --- |
| (1-4) |  |

حل کردن مسئله بهینه سازی (‏1‑4) کار مشکلی است. برای ساده‌تر کردن آن با استفاده از روش ضرایب نامعین لاگرانژ این مسئله بهینه‌سازی را می‌توان به فرم زیر تبدیل کرد که ها ضرایب لاگرانژ می‌باشند.

|  |  |
| --- | --- |
| (1-5) |  |

پس از حل مسئله بهینه‌سازی بالا و یافتن ضرایب لاگرانژ، W با استفاده از رابطه زیر محاسبه می‌شود:

|  |  |
| --- | --- |
| (1-6) |  |

مربوط به بردارهای پشتیبان بزرگتر از صفر و  مربوط به سایر نقاط صفر خواهد بود. بنابراین با توجه به (‏1‑6) و صفر بودن  مربوط به هایی که بردار پشتیبان نیستند، برای بدست آوردن مرز تصمیم‌گیری فقط نیاز به تعدادی محدود از نقاط آموزشی که همان بردارهای پشتیبان هستند می‌باشد و همه آن‌ها لازم نیستند. در نتیجه پس از یافتن W با استفاده از رابطه زیر مقدار b به ازای بردارهای پشتیبان مختلف محاسبه شده و b نهایی با میانگین‌گیری از b های حاصل بدست می‌آید.

|  |  |
| --- | --- |
| (1-7) |  |

در نتیجه طبقه‌بندی کننده‌های نهایی از طریق رابطه زیر بدست می‌آیند:

|  |  |
| --- | --- |
| (1-8) |  |

الگوریتم بالا مرز خطی دو کلاس کاملا جدا از هم را نشان می‌دهد، اما در حالتی که کلاس‌ها با هم همپوشانی داشته باشند جدا کردن کلاس‌ها به وسیله مرز تصمیم‌گیری خطی همواره با خطای زیادی همراه خواهد بود. برای حل این مشکل می‌توان ابتدا داده‌ها را از فضای اولیه  با استفاده از یک تبدیل غیرخطی ، به فضای  با ابعاد بیشتر منتقل کرد که در فضای جدید کلاس‌ها تداخل کمتری با یکدیگر داشته باشند. سپس در فضای جدید با استفاده از معادلات قبلی و جایگزینی  با  و در نظر گرفتن مقداری خطا مرز تصمیم‌گیری بهینه محاسبه می‌شود. با توجه به این امر و (‏1‑5) در این حالت یافتن مرز تصمیم‌گیری بهینه از حل مسئله بهینه‌سازی (‏1‑9) بدست می‌آید.

|  |  |
| --- | --- |
| (1-9) |  |

در این مسئله مقدار C یک عدد ثابت است. اگر ، مسئله بهینه‌سازی به سمت یافتن یک مرز برای کلاس‌های با تداخل بسیار زیادتر پیش می‌رود. از طرفی اگر ، مسئله بهینه‌سازی به سمت یافتن مرز بهینه جدا‌کننده کلاس‌های با تداخل بسیار کم پیش خواهد رفت. در رابطه (‏1‑9) به جای استفاده از ، از یک تابع کرنل که به صورت زیر تعریف می‌شود، استفاده می‌گردد.

|  |  |
| --- | --- |
| (1-10) |  |

پس از تعیین یک در (1-10) به جای ، تابع قرار داده شده و مسئله بهینه‌سازی حل می‌شود. در واقع یک تابع در فضای اولیه می‌باشد که برابر با ضرب داخلی دو بردار در فضای ویژگی است. برای معادل بودن تابع با ضرب داخلی دو بردار در فضای ویژگی، باید یک تابع معین و مثبت متقارن بوده و در مرسر صدق کند [42]. برخی از مهم‌ترین توابع کرنل یا هسته که در این شرط صدق می‌کنند، عبارتند از:

جدول 1- توابع کرنل در ماشین بردار پشتیبان

|  |  |
| --- | --- |
| **کرنل خطی** |  |
| **کرنل چند جمله‌ای** |  |
| **کرنل گوسین** |  |
| **کرنل سیگموئید** |  |

میزان کارایی ماشین بردار پشتیبان به ازای هر نوع تابع کرنل متفاوت می‌باشد. این‌که کدام تابع کرنل بهترین نتیجه را برای یک سری داده ارائه می‌دهد، به درستی معلوم نیست وباید از طریق آزمون و خطا مشخص شود. ماشین بردار پشتیبان یک طبقه‌بندی کننده دودویی است. بنابراین در حالتی که بیش از دو کلاس وجود داشته باشد نمی‌توان مستقیما از آن استفاده کرد. در حالت کلی برای استفاده از طبقه‌بندی کننده‌های دودویی در حالت چند کلاسه باید ابتدا چند طبقه‌بندی کننده دودویی طراحی شود. طبقه‌بندی نهایی با استفاده از ادغام اطلاعات طبقه‌بندی کننده‌های دودویی انجام می‌گیرد.

3- معرفی مجموعه داده ی استفاده شده

در این کار از مجموعه داده معتبر ایمیل‌های اسپم به نام Spam base استفاده خواهیم کرد. این مجموعه داده مناسب و پرکاربرد در زمینه هرزنامه است که جهت ارزیابی الگوریتم‌های داده­کاوی و یادگیری ماشین مورد استفاده قرار گرفته می­شود. این مجموعه داده ویژگی­های مهم و مرتبط با متن ایمیل­ها را مورد توجه قرار داده و کلمات کلیدی هرزنامه­ها را با نرخ تکرار آنها در متن در نظر گرفته است. به عنوان نمونه اگر مقدار ویژگی کاراکتر $ برابر 10 باشد یعنی در حدود 10% از متن ایمیل از این کاراکتر استفاده شده است. هر ویژگی دارای مقادیری درصدی بین بازه [0،1] است که نشان دهنده تکرار کلمه یا کاراکتر مورد نظر در متن ایمیل است. این مجموعه داده 4601 رکورد و 58 ویژگی ورودی و خروجی مختلف دارد.

57 ویژگی این مجموعه داده به عنوان ویژگی ورودی و ویژگی 58-ام آن به عنوان ویژگی خروجی در نظر گرفته می­شود. در این مجموعه داده اگر خروجی برابر صفر یا یک باشد به ترتیب نشان دهنده ایمیل عادی یا هرزنامه است. نتایج تجزیه و تحلیل مقدار ویژگی خروجی نشان می­دهد که از 4601 رکورد 2788 ایمیل عادی و 1813 ایمیل از نوع هرزنامه هست که در شکل 3 و 4 به ترتیب فراوانی مقادیر ویژگی خروجی و درصد آن‌ها را نشان داده است.

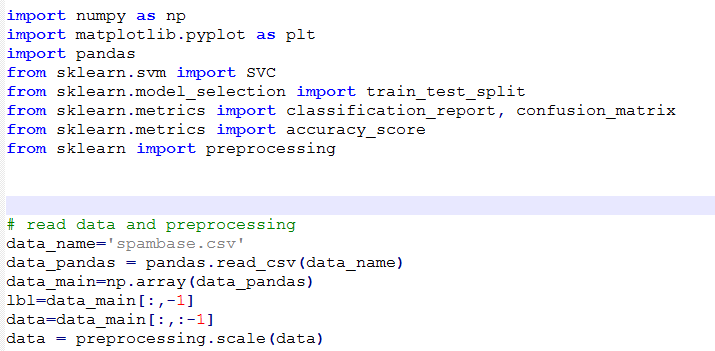
شکل 3- فراوانی هرزنامه و ایمیل عادی در مجموعه داده Spam base

شکل 4- درصد فراوانی هرزنامه و ایمیل عادی در مجموعه داده Spam base

4- پیش پردازش

در این بخش به معرفی روش‌ها و علمیات استفاده شده جهت آماده‌سازی مجموعه داده‌ها برای استفاده در الگوریتم پرداخته می‌شود. چنان‌چه در مجموعه داده تولید شده از مجموعه داده spam base کاراکتر وجود داشته باشد یا در صورت وجود خانه‌های خالی در داده‌ها از عملیات پیش پردازش که شامل پر کردن خانه‌های خالی با مقداری معین مانند صفر یا در صورت وجود کاراکتر در داده‌ها عملیات تبدیل این کاراکتر به نوع عددی صورت می‌گیرد. همچنین بعد از سپری شدن این مراحل از تابع نرمالایزر استفاده شده و داده‌ها را برای درک بهتر الگوریتم بین اعداد 0 و1 تبدیل می‌شوند. سپس عملیات جداسازی برچسب ها از داده‌ها انجام می‌پذیرد و داده‌ها برای استفاده در الگوریتم آماده می‌شوند.

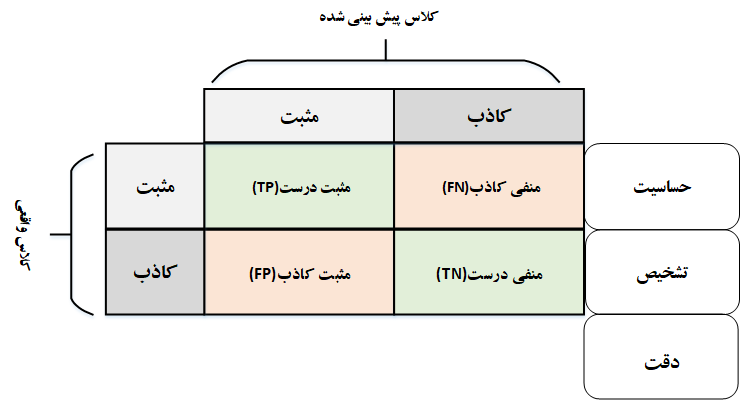
کد مربوط به بخش خواندن اطلاعات و پیش پردازش در شکل 5 آمده است:



شکل 5- کد مربوط به بخش خواندن اطلاعات و پیش پردازش

5- معیار های ارزیابی

در این پیاده‌سازی جهت ارزیابی الگوریتم طبقه‌بندی از چهار معیار حساسیت[[3]](#footnote-3)، دقت[[4]](#footnote-4)، امتیاز f1[[5]](#footnote-5) و صحت[[6]](#footnote-6) استفاده شده است. برای محاسبه این معیار‌ها، پاسخ‌های تشخیص ایمیل‌های اسپم در الگوریتم‌ها در چهار دسته نمونه­های صحیح مثبت[[7]](#footnote-7) (TP)، نمونه‌های غلط منفی[[8]](#footnote-8)FN))، نمونه‌های غلط مثبت[[9]](#footnote-9)FP)) و نمونه­های صحیح منفی[[10]](#footnote-10)TN)) قرار می‌گیرد که در شکل 6 این چهار مفهوم نمایش داده شده است.



شکل 6- مفاهیم اولیه ارزیابی روش پیشنهادی در تشخیص ایمیل های اسپم

این جدول را اصطلاحا ماتریس درهم ریختگی[[11]](#footnote-11) می‌گویند. جدول یا ماتریس درهم ریختگی، نتایج حاصل از طبقه‌بندی را بر اساس اطلاعات واقعی موجود، نمایش می‌دهد. حال بر اساس این مقادیر می‌توان معیارهای مختلف ارزیابی دسته بند و اندازه‌گیری دقت را تعریف کرد. طبق شکل 6، پاسخ‌های تشخیص ایمیل‌های اسپم و ایمیل‌های عادی در الگوریتم‌ها در چهار دسته زیر قابل تعریف است:

1. جواب صحیح مثبت: این دسته شامل نمونه‌هایی هستند که مثبت هستند و توسط دسته‌بندها یا روش پیشنهادی در دسته مثبت قرار گرفته است. به‌ عنوان مثال یک نمونه مربوط به ایمیل عادی بوده و به درستی توسط روش پیشنهادی از نوع عادی تشخیص داده است.
2. جواب صحیح منفی: این دسته شامل نمونه‌هایی هستند که منفی هستند و توسط الگوریتم‌ها در دسته منفی قرار گرفته است. به‌ عنوان مثال یک نمونه مربوط به نوع اسپم بوده و به درستی توسط روش پیشنهادی از نوع اسپم تشخیص داده است.
3. جواب غلط مثبت: این دسته شامل نمونه‌هایی هستند که مثبت هستند و توسط الگوریتم‌ها در دسته منفی قرار گرفته است. به‌ عنوان مثال یک نمونه مربوط به نوع عادی بوده و به درستی توسط روش پیشنهادی از نوع اسپم تشخیص داده است.

جواب غلط منفی: این دسته شامل نمونه‌هایی هستند که منفی هستند و توسط الگوریتم‌ها در دسته مثبت قرار داده شده است. به‌ عنوان مثال یک نمونه مربوط به نوع اسپم بوده و به درستی توسط روش پیشنهادی ازعادی تشخیص داده است.

نحوه محاسبه معیارهای دقت، صحت، حساسیت و امتیاز F1 در زیر بیان شده است.

|  |  |
| --- | --- |
| (1-11) |  |

|  |  |
| --- | --- |
| (1-12) |  |

|  |  |
| --- | --- |
| (1-13) |  |

|  |  |
| --- | --- |
| (1-14) |  |

با توجه به رابطه‌های (1-11) تا (1-14) می توان مشاهده نمود که مقادیر دقت، صحت، حساسیت و امتیاز F1 از پارامتر‌های شکل 6 بدست می آیند. همچنین معیار زمان نیز که نشان‌دهنده ی میزان زمان سپری شده برای اجرای هر الگوریتم می باشد نیز از معیار های ارزیابی روش پیشنهادی می‌باشد.

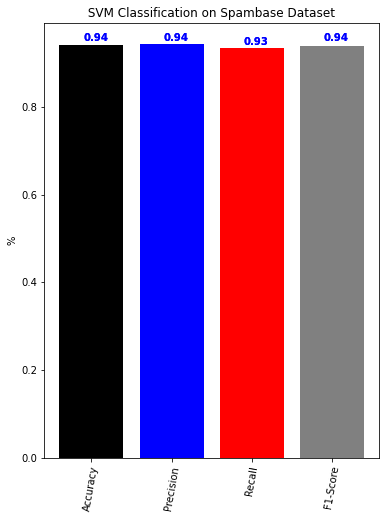
6- تحلیل و ارزیابی نتایج الگوریتم پیشنهادی بر روی مجموعه داده spam base

در این بخش به بررسی و تحلیل نتایج بدست آمده از اجرای الگوریتم SVM بر روی مجموعه داده یspam base پرداخته می شود. در ادامه در جدول 2 نتایج کلی بدست آمده توسط الگوریتم به نمایش گذاشته شده است.

جدول 2- نتایج اجرای الگوریتم ها بر روی مجموعه داده spam base

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **F1 ترکیبی** | **حساسیت** | **صحت** | **دقت** | **نام الگوریتم** |
| 0.94 | 0.93 | 0.94 | 0.94 | **SVM** |

در شکل 7 می‌توان نتایج بدست آمده توسط الگوریتم را به صورت نموداری مشاهده نمود.



شکل 7-نتایج بدست آمده توسط الگوریتم بر روی مجموعه داده spam base بر اساس چهار معیار

با توجه به شکل 7 می‌توان مشاهده نمود که پیاده سازی الگوریتم ماشین بردار پشتیبان روی مجموعه داده spam base عملکرد خوبی داشته و توانسته مقادیر بالایی را برای هر چهار معیار دقت، صحت، حساسیت و امتیاز F1 بدست آورد. پیاده‌سازی الگوریتم SVM روی مجموعه داده Spam base توانسته برای معیارهای دقت، صحت و امتیاز F1 مقداری برابر با 94/0 را بدست آورد. همچنین برای مقدار حساسیت نیز مقدار 93/0 بدست آمده است.

7- جمع بندی نتایج

امروزه بسیاری از افراد و سازمان‌ها از ایمیل‌ها برای اهداف تبلیغات تجاری استفاده می‌کنند و در نتیجه ایمیل‌های غیر ضروری در صندوق ورودی کاربران به نام اسپم ایجاد می‌شود و به طوری که ایمیل‌های اسپم یکی از مشکلات اصلی اینترنت محسوب می‌شود. تکنیک‌های یادگیری ماشین توانایی یادگیری و شناسایی ایمیل‌های اسپم و پیام‌های فیشینگ از طریق تجزیه و تحلیل چنین پیام‌هایی در سراسر مجموعه وسیعی از کامپیوترها را دارند. برای افزایش دقت و سرعت تشخیص ایمیل های اسپم می توان از الگوریتم های یادگیری ماشین در تشخیص ایمیل های اسپم استفاده کرد. در این پژوهش پیاده سازی الگوریتم SVM روی مجموعه داده Spam base انجام گرفته شده و برای معیارهای دقت، صحت و امتیاز F1 مقداری برابر با 94/0توسط الگوریتم بدست آمد. همچنین برای مقدار حساسیت نیز مقدار 93/0توسط الگوریتم ماشین بردار پشتیبان بدست آمد. نتایج پیاده‌سازی الگوریتم ماشین بردار پشتیبان روی مجموعه داده Spam base نشان می‌دهد که با استفاده از الگوریتم‌های یادگیری ماشین می‌توان به دقت بالایی در تشخیص اسپم دست یافت.

1. Support Vector Machine (SVM) [↑](#footnote-ref-1)
2. Vapnik [↑](#footnote-ref-2)
3. recall [↑](#footnote-ref-3)
4. accuracy [↑](#footnote-ref-4)
5. F-Score [↑](#footnote-ref-5)
6. precision [↑](#footnote-ref-6)
7. . True Positive [↑](#footnote-ref-7)
8. . True Negative [↑](#footnote-ref-8)
9. . False Positive [↑](#footnote-ref-9)
10. . False Negative [↑](#footnote-ref-10)
11. Confusion matrix [↑](#footnote-ref-11)