نخستین همایش ملی مهندسی کامپیوتر، علوم کامپیوتر و فناوری اطلاعات
قم - دانشگاه علمی کاربردی استانداری قم – خرداد ماه ۱۳۹۵

مروری بر شناسایی و دسته بندی فیلترینگ هرزنامه‌های ایمیل

مصطفی امیری[۱]، مجتبی فیروزی[۲]، محبوبه شمسی[۳]
دانشگاه صنعتی قم
shamsi@qut.ac.ir ، mojtabafirozy@gmail.com ، Seddiq2003@gmail.com

چیکده
اینترنت یکی از مهم‌ترین دستاوردهای بشری است که راه ارتباط مورد نیاز دنیای امروزی را فراهم کرده است. یکی از پر استفاده‌ترین امکاناتی که در این بستر صورت می‌گیرد پست الکترونیکی می‌باشد. به دلیل هزینه اندک، سرعت در ارسال و دریافت، سهولت استفاده و بسیاری از کاربردهایی که دارد مورد استقبال کاربران قرار گرفته است. کاربرد بالای آن باعث شده تا یک مشکل مهم در امنیت کامپیوتر برای گسترش تهدیدات، از جمله ویروس های کامپیوتری، کرم ها و فیشینگ به حساب آید که با استفاده از ارسال گسترده نامه‌های زائد و یا بعضا مخرب صورت می‌گیرد و در بین کاربران با عنوان هرزنامه از آن یاد می‌شود. الگوریتم‌های مختلفی برای شناسایی هرزنامه‌ها ارائه شده است که هر یک دارای محاسن و معایب مربوط به خود است و آشنایی با هر یک از روش‌های موجود، شناخت دقیق‌تری از مبارزه با هرزنامه‌ها را پیش روی مبارزین با آن قرار می‌دهد. در این مکتوبه، بر آن هستیم تا ضمن آشنایی با ماهیت این مهمانان ناخوانده، شناسایی آن‌ها را به همراه دسته بندی فیلترینگ آن مرور نماییم.

واژه‌های کلیدی: هرزنامه- فیلترینگ- دسته بندی- الگوریتم- ایمیل

۱- مقدمه

یکی از رایج‌ترین وسایل ارتباطی برای سازمان‌ها و کاربران اینترنت، در حال حاضر ایمیل می‌باشد. ایمیل‌ها توسط بسیاری از افراد روی زمین استفاده می شود. تخمین زده می شود که بیش از ۳ میلیارد صندوق پست الکترونیکی (تقریبا نیمی از جمعیت جهان) وجود دارد و انتظار می رود به مرز ۴ میلیارد ایمیل تا سال ۲۰۱۵ برسد.[5]

هرزنامه[۴] و یا ایمیل‌های ناخواسته[۵] که با نام UCE[۶] هم بکار برده می‌شوند[1,20]، به یک مشکل مهم برای کاربران ایمیل تبدیل شده‌اند. در سه ماهه اول سال ۲۰۱۰، به طور متوسط ۱۸۳ میلیارد پیام های اسپم در هر روز ارسال می‌شده است[35] (بر اساس گزارش [36] Commtouch). برخی عقیده دارند حدود ۷۰ درصد[6] و برخی نیز ۸۷/۶ درصد[7] از تمام پیام‌های ایمیل را هرزنامه تشکیل می‌دهد، گرچه تعداد آن‌ها را تا ۹۰ درصد و بیش از آن نیز ذکر کرده‌اند. روند شناسایی و مبارزه با هرزنامه‌ها دارای افت و خیزهایی در سال‌های مختلف بوده است که آمار فراوانی هرزنامه‌ها می‌تواند به این نکته اشاره داشته باشد. با توجه به این که ۳۶٪ از ایمیل‌های دریافتی را در سال ۲۰۰۲ هرزنامه‌ها به خود اختصاص داده بودند، در سال ۲۰۱۰ به ۹۵٪ و در سال ۲۰۱۳ در حدود ۷۰٪ گزارش شده است[9] این نکته حاکی از میزان هرزنامه و همچنین میزان مبارزه با هرزنامه‌ها در سال‌های مختلف می‌باشد. هرزنامه‌ها، نه تنها برای کاربران آن مشکل‌ساز هستند بلکه، به‌عنوان یک مشکل

---

[۱] دانشجوی کارشناسی ارشد مهندسی نرم افزار دانشگاه صنعتی قم
[۲] دانشجوی کارشناسی ارشد مهندسی نرم افزار دانشگاه صنعتی قم
[۳] استادیار و عضو هیات علمی دانشگاه صنعتی قم

[4] Spam
[5] Junk
[6] Unsolicited Commercial Email

بزرگ امنیتی، میلیاردها دلار ضرر و زیان به همراه دارند[5,19]. علاوه بر آن، از آن به‌عنوان وسیله‌ای تبلیغاتی ارزان قیمت و همچنین برای فیشینگ[۷] نیز استفاده می‌شود[19] و از طرفی، وسیله‌ای برای گسترش برنامه‌های مخرب[8] (مانند ویروس‌های کامپیوتری، اسب‌های تروجان، نرم‌افزارهای جاسوسی و کرم‌های اینترنتی) می‌باشد. فیلتر هرزنامه یکی از مسایل مهم در زمینه داده کاوی است[35].

با توجه به نیاز آشنایی با هرزنامه‌ها و فیلترینگ آن‌ها، تا کنون تعاریف، اشارات و دسته بندی‌های مختلفی ارائه شده است، ولی در این مقاله سعی شده است که یک دسته‌بندی بصورت خلاصه اما کامل تر ارائه شود تا خواننده با مروری بر آن بتواند تصویری ملموس‌تر از دسته‌بندی هرزنامه‌های ایمیل و فیلترینگ آن بدست آورد و با دیدی کلی و اشتیاقی بیشتر برای مطالعات کاربردی و تمرکز بر روی روش‌ها و الگوریتم‌های خاص گام بردارد. در این جا لازم است اشاره‌ای شود به زحمات تمامی عزیزانی که در این زمینه قدم برداشته‌اند و از همه آن‌ها سپاسگزاری گردد و امید است افرادی دیگر، تلاش خود را برای بهبود و تکمیل تحقیقات موجود بکار ببرند. در بخش دوم این مقاله، به تاریخچه هرزنامه اشاره می‌شود و در بخش سوم به انواع هرزنامه، اهداف تولید کنندگان آن و انواع فیلترینگ هرزنامه‌ها مرور می‌شود و در بخش چهارم هم نتیجه‌گیری از مطالب گفته شده و نهایت در بخش پنجم منابع استفاده شده درج گردیده است.

۲- تاریخچه

تاریخچه هرزنامه‌ها را می‌توان در سه مقطع زمانی مختلف بیان کرد[3]:

مقطع اول که از سال ۱۹۸۷ با انتشار اولین هرزنامه شروع می‌شود و تا سال ۱۹۹۰ را به عنوان یک دوره از آن نام برد، در این مقطع هرزنامه‌ها به صورت دستی فرستاده می‌شدند. برای ارسال هرزنامه‌ها به تعداد زیادی از منابع انسانی نیاز بود و به دلیل هزینه بالای آن امکان ارسال به تعداد کاربران زیاد امکان پذیر نبود.

در سال ۱۹۹۴ با طراحی یک برنامه نرم افزاری هرزنامه‌نویسی آغاز شد. همزمان با این موضوع، تلاش برای مبارزه با هرزنامه‌ها نیز شروع گردید. به همین دلیل در سال ۱۹۹۷ ، اولین نرم افزار فیلترکردن هرزنامه‌ها پا به عرصه وجود گذاشت[10].

شاید اولین مقاله قابل ذکر در مورد مبارزه با هرزنامه‌ها که تغییر اساسی در مبارزه با هرزنامه‌ها را آغاز کرد در سال ۲۰۰۲ توسط پل گراهام نوشته شده باشد[11]. در این مقاله روش استفاده از یادگیری ماشین و تفکیک کننده‌های آماری برای فیلترکردن هرزنامه‌ها پیشنهاد شد. با استفاده از این شیوه، مشخصات و صفات نامه‌های کاربران مد نظر قرار می‌گرفت و روند فیلترکردن هرزنامه‌ها با سرعت و پیشرفت قابل ملاحظه‌ای برخوردار بود و این نخستین شیوه‌ای بود که امکان آزمودن فیلترها را قبل از فرستادن هرزنامه‌ها برای هرزنامه‌نویسان غیر ممکن ساخت. این مقطع را می‌توان به عنوان دوره مبارزه هرزنامه‌نویسان و مقابله کنندگان با آن نام برد، در این مبارزه تلاش می‌شود تا با استفاده از روش‌های یادگیری ماشین و دسته‌بندی‌های آماری، این هرزنامه‌ها را تشخیص و فیلتر نمایند[12]. در حال حاضر روش‌های بسیاری ابداع شده تا بصورت خودکار و به دنباله مبارزه ماشینی با هرزنامه‌ها و هرزنامه‌نویسان عمل فیلترینگ را به نحو بهتری به انجام برسانند.

[7] Phishing

۳- انواع هرزنامه

در دسته‌بندی هرزنامه‌ها تحقیقات مختلفی صورت گرفته است که متداول‌ترین آن‌ها اسپم وب[۸]، اسپم ایمیل[۹] [24,25]، اسپم محتوا[۱۰]، اسپم پیوند[۱۱] و اسپم نظرات[۱۲] می‌باشد.

اسپم وب، برای فریب دادن موتورهای جستجو در ارتقاء رتبه‌بندی[۱۳] صفحات وب بکار می‌رود که در دسته بندی اسپم‌های محتوا و پیوند قرار می‌گیرد[26,27,29].

اسپم ایمیل، در واقع ایمیل‌های ناخواسته‌ای است که به منظور و هدفی خاص برای کاربران اینترنت ارسال می‌شود [28,29].

اسپم محتوا، کلماتی متداول - ولی نامربوط- در صفحات وب است که باعث فریب موتورهای جستجو در درخواست‌های جستجو[۱۴] می‌شود[21,24].

اسپم پیوند، در واقع همان لینک‌های[۱۵] تبلیغاتی است که استفاده آن در فروم‌های[۱۶] رسانه‌های اجتماعی متداول است[24].

اسپم نظرات[۱۷]، نظرات غیرصادقانه و یا جعلی است که در مورد استفاده و یا عدم استفاده از محصولات و یا یک سرویس خاص تجاری یا غیر تجاری بکار می‌رود[4].

۴- اهداف تولیدکنندگان هرزنامه‌های ایمیل

به دلیل ازدیاد و حجم وسیع هرزنامه‌ها، اهداف تولیدکنندگان را می‌توان برحسب معیارهای متفاوتی دسته بندی کرد. از آن جمله می‌توان دلایل عقیدتی، کلاهبرداری اطلاعاتی وتبلیغاتی را نام برد. برهمین اساس برخی، اهداف تولیدکنندگان هرزنامه‌ها را به ۳ دسته تقسیم کرده‌اند[30] ولی در این مقاله به ۶ دسته‌بندی مختلف اشاره شده است.

۴-۱- هرزنامه‌های تجاری

این نوع هرزنامه‌ها برای تبلیغ له و یا علیه محصولات و یا خدمات شرکت تجاری خاصی به کار می‌روند و یکی از مهم‌ترین علل گستردگی آن، هزینه پایین تبلیغات نسبت به روش‌های دیگر است.

۴-۲- هرزنامه‌های مالی

این نوع هرزنامه‌ها با سناریوهای مختلف سعی در فریب کاربران و دریافت پول از آن‌ها را دارد، بعنوان مثال، به کاربر گفته می‌شود که در فلان قرعه کشی برنده شده‌اید ومی‌بایست برای دریافت جایزه هزینه‌ای را بپردازید[30].

---

[8] Web spam
[9] Email spam
[10] Content spam
[11] Link spam
[12] Openion spam
[13] Ranking
[14] Search queries
[15] Hyperlinks
[16] Forum
[17] Reviews spam

۴-۳- هرزنامه‌های کلاهبرداری

هدف این هرزنامه‌ها دسترسی به اطلاعات شخصی و محرمانه کاربران مانند نام کاربری و رمزعبور کارت اعتباری آن‌ها است که عملیات فیشینگ یکی از آن موارد است[30].

۴-۴- هرزنامه‌های اطلاعاتی

با توجه به تعداد زیاد صندوق‌های پست الکترونیکی و کاربران متعدد آن، بستر مناسبی برای اطلاع رسانی و بالعکس آن، زمینه‌ای برای جاسوسی اطلاعات از سیستم‌های مختلف است که هرزنامه‌ها می‌تواند این هدف را برای تولید کنندگان آن با کم‌ترین زمان و پایین‌ترین هزینه مهیا سازد.

۴-۵- هرزنامه‌های مخرب

دسته‌ای از هرزنامه‌های موجود برای ایجاد خلل در سیستم‌های کامپیوتری طراحی شده‌اند که با تکثیر ویروس‌های مخرب و انتشار کرم‌های اینترنتی خسارات فراوانی برای شرکت‌ها، سازمان‌ها و کاربران اینترنتی بوجود می‌آورند.

۴-۶- هرزنامه‌های عقیدتی

این نوع هرزنامه‌ها در واقع برای تضعیف عقاید مذهبی مخاطبین خود و با جهت‌گیری خاص محتوایی تهیه و ارسال می‌شوند و غالبا طیف جوان و نوجوان را مورد هدف قرار داده تا حداقل نسبت به اعتقادات دینی خود سست و یا شبهه‌ای در ذهن آنان بوجود بیاورند.

۵- انواع فیلترینگ هرزنامه‌های ایمیل

گرچه اینترنت روش‌های ارتباطی جدیدی را عرضه کرده است ولی سیل هرزنامه‌ها و هرزنامه‌نویسان[۱۸] روز به روز در حال افزایش و تغییر ماهیت هستند و راه‌های فیلترینگ هوشمند و خودکار همچنان ضروری به نظر می‌رسد[27].

از آنجا که فیلترینگ هرزنامه را می‌توان گونه‌ای از دسته‌بندی متون به حساب آورد، بسیاری از الگوریتم‌های یادگیری ماشین که در دسته‌بندی متون کاربرد دارند در شناسایی هرزنامه نیز می‌توانند مفید باشند[14]. فیلتر کردن هرزنامه‌هایی که بر اساس محتوای آن‌ها صورت می‌گیرد حالت خاصی از دسته بندی متون محسوب می‌شود که در آن دو کلاس نامه‌های معتبر(Ham) و هرزنامه(Spam) مد نظر خواهند بود[33]. تفکیک نامه‌های معتبر از نامه‌های هرز در فیلترینگ هرزنامه‌ها اهمیت زیادی دارد و به عنوان ارزیابی در کارایی الگوریتم‌ها شناخته می‌شود، ولی باید اذعان داشت که هزینه به اشتباه فیلتر کردن یک نامه عادی بیشتر از آن است که یک نامه هرز از فیلتر عبور نماید[1]. برخی از این الگوریتم‌ها درخت تصمیم، شبکه عصبی، بیزین، ماشین بردار پشتیبان، یادگیری جمعی و غیره می‌باشند.

[18] Spammer

یادگیری ماشین یکی از حوزه‌های مهم هوش مصنوعی است. الگوریتم‌هایی در این حوزه قرار دارند که قابلیت یادگیری را داشته باشند و باعث افزایش کارایی خود در واحد زمان می‌شوند [15].

موفقیت روش‌های یادگیری ماشین در دسته بندی متون باعث شد تا در فیلترینگ هرزنامه‌ها از الگوریتم‌های یادگیری ماشین بهره برده شود[32]. هدف این الگوریتم‌ها ایجاد تمایز بین هرزنامه‌ها و نامه‌های معتبر می‌باشد. این روش‌ها توانایی استخراج دانش از یک مجموعه داده[19] یا مجموعه مستندات را دارا بوده و در حقیقت دانشی را که از یک مجموعه داده استخراج می‌کنند برای شناسایی هرزنامه‌های جدید مورد استفاده قرار می دهند(شکل۲).

این فیلترینگ‌ها همانند فیلترینگ‌های مبتنی بر قانون، از الگوها و قوانین ثابتی جهت تشخیص هرزنامه‌ها استفاده می‌کنند. پیاده‌سازی اینگونه فیلترینگ‌ها اصولاً کاری ساده است و توانایی تشخیص هرزنامه‌ها پایین است. روش‌هایی مانند لیست سیاه وسفید از دسته فیلترینگ‌ها می‌باشند[16].

لیست سیاه یک روش بسیار ساده‌ای است که به‌طور گسترده در بسیاری از روش‌های فیلترینگ استفاده می‌شود. درحالی‌که لیست سفید، فهرستی از ایمیل فرستندگان خاص ارائه می‌دهد که به منظور کاهش تعداد اشتباه ایمیل طبقه‌بندی شده‌اند[17]. یکی دیگر از روش‌های محبوب برای این به اصطلاح روش طرد شده در فهرست سیاه DNS (شکل ۱) است که در آن آدرس میزبان در لیستی از شبکه ها و یا سرورهای شناخته‌شده برای توزیع هرزنامه بررسی می‌شود[18]، با این وجود DNS را می‌توان در لیست فیلترینگ مبتنی بر دامین[13] نیز دسته بندی کرد.

در سیستم‌های مبتنی بر امضا، برای هر پیام هرزنامه شناخته‌شده، یک مقدار منحصر به فرد ایجاد می‌کنند (به‌عنوان‌مثال، یک خلاصه پیام). مزیت اصلی این نوع از روش ها کاهش تولید false positives است.

نمونه‌هایی از سیستم فیلترینگ اسپم مبتنی بر امضا عبارت‌اند از: Cloudmark، پیاده‌سازی تجاری یک فیلتر مبتنی بر امضا که با ایمیل سرور ادغام‌شده است. Razor یکی دیگر از سیستم‌های فیلترینگ است که با استفاده از یک روش توزیع‌شده و مشارکتی به‌منظور گسترش امضا استفاده می‌شود(شکل ۱).

این روش‌های ساده دارای کاستی‌هایی نیز هستند. روش اول، روش فهرست سیاه به میزان بسیار بالایی false positives دارد که به‌عنوان یک راه حل غیر قابل اعتماد شناخته شده است. روش دوم، سیستم‌های مبتنی بر امضا قادر به شناسایی هرزنامه‌ها هستند که پیام‌های ناخواسته شناسایی شده می‌باشند.

به‌منظور پیدا کردن یک راه‌حل برای این مشکل، پژوهشگران، کارهای زیادی انجام داده‌اند. ازآنجاکه روش‌های یادگیری ماشین در مسائل طبقه‌بندی متن موفق هستند[19]، در سیستم فیلتر هرزنامه نیز استفاده شده‌اند. در طبقه‌بندی Naive Bayes کار قابل‌توجهی انجام‌گرفته و با مطالعات انجام‌شده در فیلتر ضد اسپم مؤثر بوده است. روش دیگری که به‌طور گسترده در حوزه یادگیری ماشین است، روش SVM[20] می‌باشد[19]. مزایای استفاده از SVM این است که علی‌رغم ویژگی‌های زیاد آن، دقیق است و برای فیلتر هرزنامه بسیار استفاده می‌شود. به همین ترتیب، روش مبتنی بر حافظه[21][20]، Kامین نزدیک‌ترین همسایه، شبکه عصبی، درخت‌های تصمیم‌گیری[22] و روش پیشرفته تر آن که درخت تصمیم گیری فازی نام گرفته

[19] Data mining
[20] Support Vector Machines
[21] Memory based
[22] Decision Trees

و روش‌های متعدد دیگری برای فیلتر کردن هرزنامه ها استفاده می‌شود. الگوریتم‌های یادگیری جمعی یا ماشین رایزن[۲۳] که از چند الگوریتم مختلف استفاده می‌کنند در دسته بندی‌های فیلترینگ هرزنامه‌ها حایز اهمیت هستند که به الگوریتم‌های ترکیبی نیز شهرت دارند و در دو دسته بگینگ[۲۴] و بوستینگ[۲۵] قرار می‌گیرند[34]. به همه روش‌های فیلترینگ هرزنامه‌هایی که مبتنی بر یادگیری ماشین می‌باشند روش‌های آماری نیز می‌گویند(شکل ۳).

روش‌های یادگیری ماشین در ایمیل‌ها، از مدل فضای برداری (VSM[۲۶]) استفاده می‌کنند. VSM روشی جبری برای فیلتر اطلاعات (IF[۲۷])، بازیابی اطلاعات (IR[۲۸])، اندیس گذاری و رتبه‌بندی می‌باشد. این مدل اسناد به زبان طبیعی را به شیوه‌ای ریاضی از طریق بردارها که در یک فضای چند بعدی است ارائه می‌دهد. بااین‌حال، در VSM فرض بر این است که هر کلمه)Term(مستقل است. این دیدگاه حداقل ازنقطه نظر زبانی، کاملاً درست نیست. بنابراین، نمی‌تواند پدیده‌های زبانی موجود در زبان طبیعی را تحمل کند.

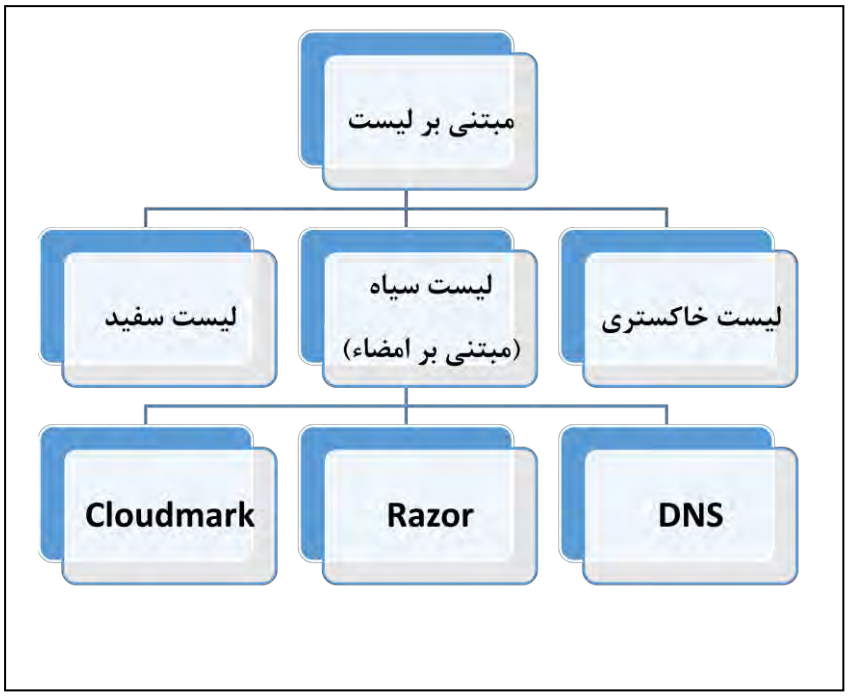
ضعف VSM باعث شد، در چند سال گذشته، مدل برداری مبتنی بر موضوع)TVSM(و مدل برداری مبتنی بر موضوع پیشرفته)eTVSM(مطرح شود[23]. eTVSM از هستی‌شناسی برای بیان روابط مختلف بین term ها استفاده می‌کند. و در این راه، یک مدل بازیابی غنی‌تر زبان طبیعی را فراهم می‌کند که قادر به تطبیق مترادف، همچنین homonyms (کلمه‌ای که تلفظ آن با کلمه دیگر یکسان ولی معنی آن دگرگون باشد) و دیگر پدیده‌های زبانی را پشتیبانی کند.

در شکل شماره ۳ یک دسته بندی کلی به عنوان نمونه‌ای از دسته بندی فیلترینگ متون مبتنی بر محتوا نشان داده شده است. گر چه این در این دسته بندی تمامی روش‌های موجود برای فیلتر کردن هرزنامه‌ها درج نشده ولی اکثر روش‌های محبوب مورد استفاده محققین ذکر گردیده است.

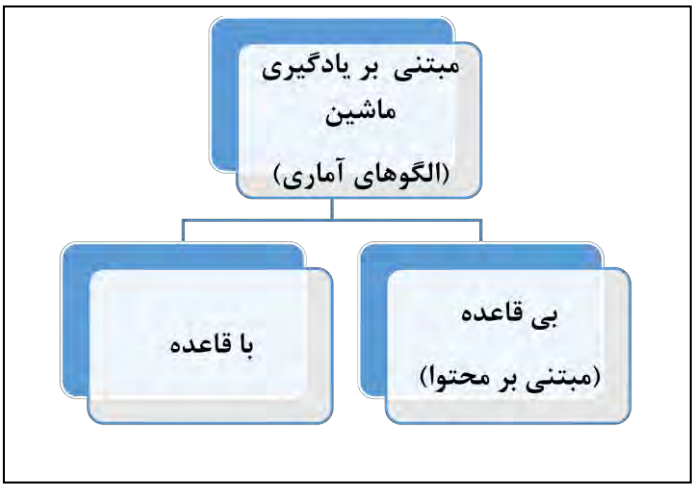
در مقابل الگوریتم‌های بی قاعده می‌توان به روش‌های با قاعده(شکل۲) اشاره کرد و بیان داشت که این فیلترها با استفاده از قوانین ثابت و از پیش تعیین شده‌ای طبق یک قاعده خاصی سعی در شناسایی هرزنامه‌ها می‌کنند و قادر به شناسایی هرزنامه‌هایی که خارج از قاعده می‌باشند نیستند و با توجه به ترفندهای هرزنامه‌نویسان منجر به افزایش عبور هرزنامه‌ها از فیلتر می‌شوند. بنابر این در موارد حساس، کارایی پایین تری نسبت به الگوریتم‌های مبتنی بر محتوا دارند.

در دسته بندی فیلترینگ هرزنامه‌های ایمیل نظرات مختلفی وجود دارد ولی دسته بندی نشان داده شده در این مقاله(شکل ۵) یک دسته بندی پیشنهادی با توجه به مرور مقالات مختلف صورت گرفته است ولی می‌توان دسته بندی کامل‌تر و اصولی تری نیز نشان داد که امید است در مقالات بعدی ارائه گردد.

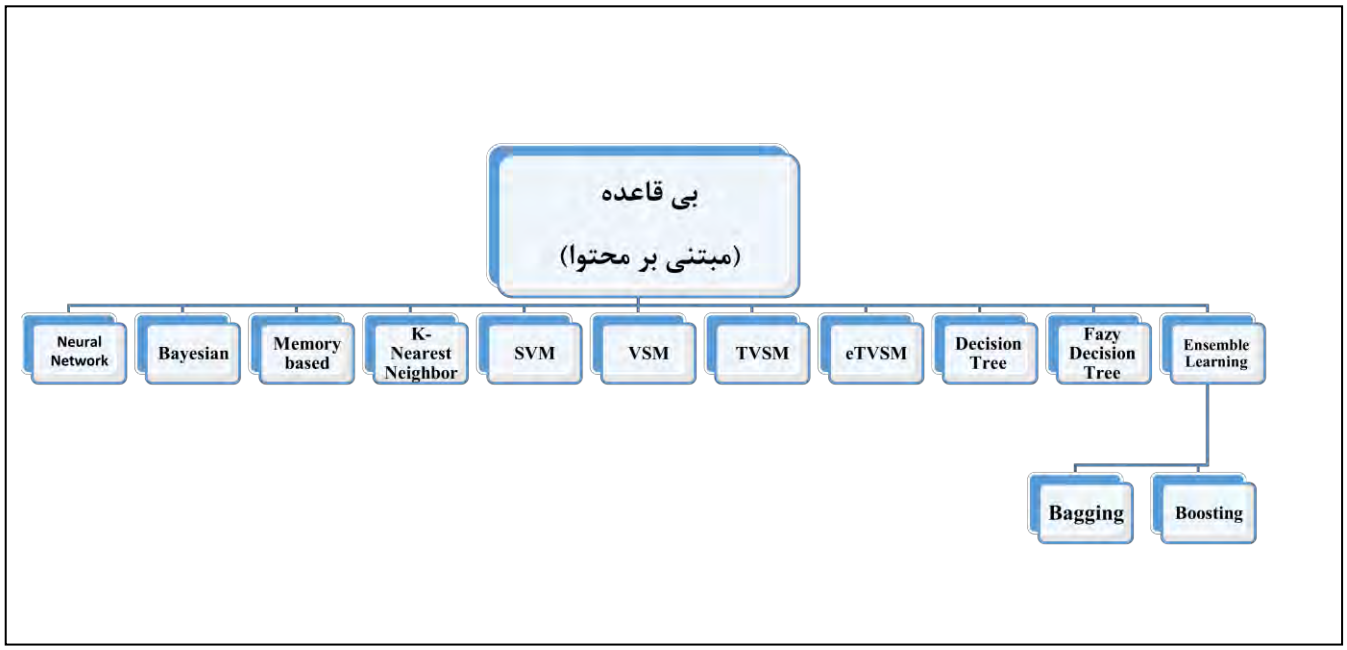
[23] Committee Machine
[24] Bagging
[25] Boosting
[26] Vector Space Model
[27] Information Filtering
[28] Information Recovery



شکل۱ – نمونه دسته بندی روش‌های فیلترینگ هرزنامه ایمیل مبتنی بر لیست.



شکل ۲- دسته بندی روش‌های فیلترینگ هرزنامه مبتی بر یادگیری ماشین(الگوهای آماری).



شکل ۳- نمونه دسته بندی روش‌های فیلترینگ هرزنامه‌های بی قاعده (مبتنی بر محتوا).

۶- مراحل اصلی فیلترینگ هرزنامه

مراحل اصلی فیلترینگ هرزنامه مبتنی بر محتوا در پنج مرحله می‌باشد که در زیر به آن اشاره شده است[26] و در شکل شماره ۴ نیز مراحل آن به ترتیب برای شناسایی اسپم از غیر اسپم نشان داده شده است.

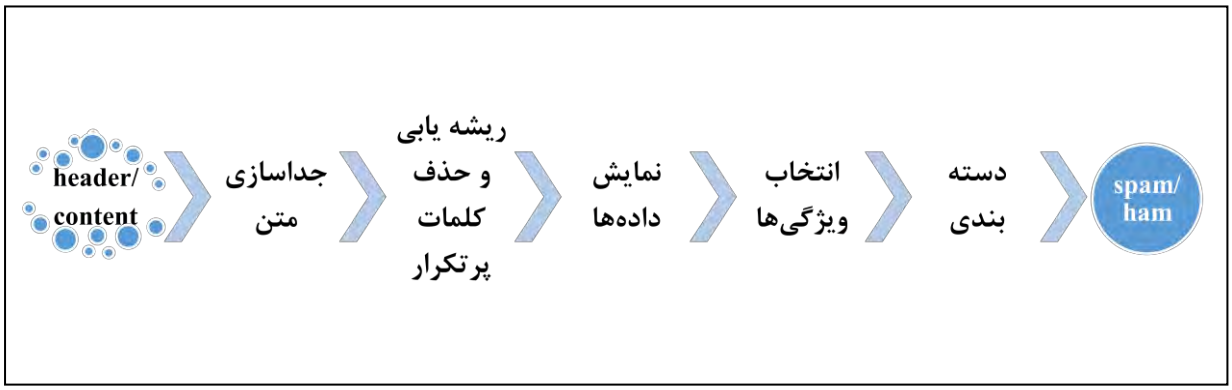
الف) جداسازی نشانه : استخراج کلمات از بدنه‌ی نامه که دارای ارزش محتوایی نیستند[22].

ج) ریشه‌یابی: باز گرداندن کلمات به ریشه‌ی اصلی خود.

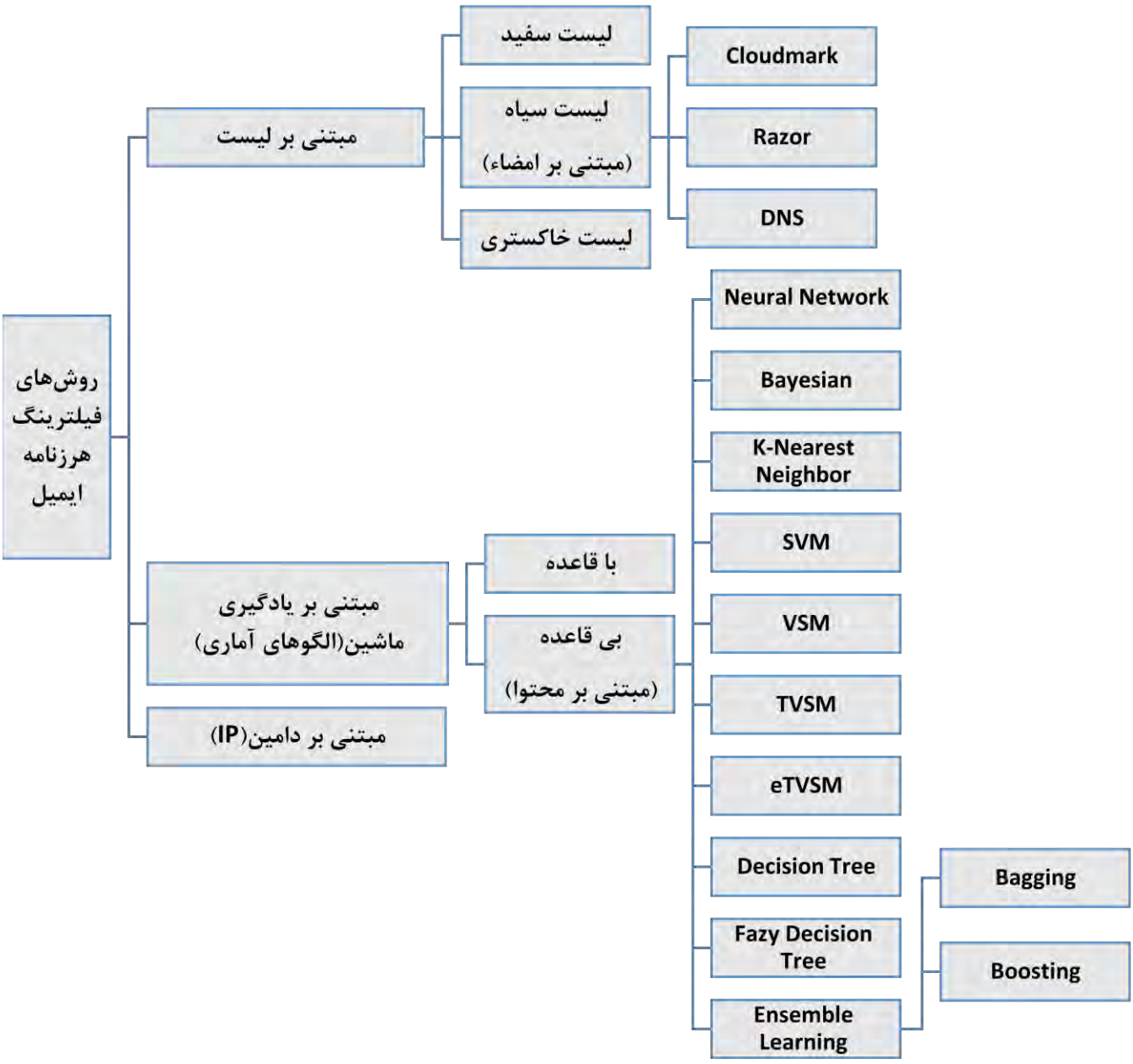
د) نمایش: تبدیل کردن مجموعه کلمات به فرم مشخص و مورد نیاز برای الگوریتم مورد نظر، مانند ساخت بردار ویژگی با استفاده از روش کیسه‌ای ازکلمات.

هـ) انتخاب ویژگی: انتخاب زیر مجموعه‌ای از کلمات نشان داده شده، که حاوی اطلاعات مفیدتری هستند. به عبارت دیگر حذف ویژگی‌های نامناسب از بردار ویژگی نشان داده شده در مرحله قبل.

و) دسته بندی: با توجه به چهار مرحله قبلی که ذکر گردید در این مرحله در واقع دسته بندی هرزنامه از نامه‌های عادی صورت گرفته و تشخیص نهایی برای شناسایی هرزنامه‌ها انجام شده است.



شکل۴- مراحل اصلی فیلترینگ هرزنامه مبتنی بر محتوا[31].



شکل ۵- دسته بندی پیشنهادی روش‌های فیلترینگ هرزنامه‌های ایمیل در یک نگاه.

۷- نتیجه گیری

شناسایی و دسته‌بندی فیلترینگ هرزنامه‌ها به محققین کمک می‌کند تا به میزان اهمیت مبارزه با آن‌ها پی ببرند. شاید بتوان دسته بندی موجود در این مقاله را یکی از خلاصه‌ترین و همچنین کامل‌ترین دسته‌بندی‌های ارائه شده در زمینه آشنایی با هرزنامه‌ها و فیلترینگ آن‌ها دانست ولی با این حال، تحقیق بیشتر در این زمینه ضروری است. با وجود هرزنامه‌های فراوانی که برای صندوق پست الکترونیکی کاربران و سازمان‌های مختلف در حال ارسال است به جرات می‌توان گفت که هنوز هیچ روشی نتوانسته است به طور کامل هرزنامه‌ها را از ایمیل‌های معتبر و عادی تشخیص دهد. هرزنامه‌ها شبیه ویروس‌های کامپیوتری همه روزه در حال افزایش و یا تغییر شکل هستند که برای مبارزه با آن‌ها باید به راه حل‌های جدیدتری نیز دست یافت. هر یک از روش‌های مبارزه با هرزنامه‌ها دارای محاسن و معایبی است که برای استفاده از آن‌ها باید توسط متخصصین فن تشخیص داده شود، ولی بهترین روش را می‌توان ترکیبی از الگوریتم‌های موجود دانست که آن نیز پیچیدگی و هزینه بیشتری بدنبال خواهد داشت. در نهایت، باید اذعان داشت که هزینه به اشتباه بلاک کردن یک نامه عادی بسیار بیشتر از هزینه آن است که یک نامه هرز، از فیلتر عبور نماید.

مراجع

۱- جلیلی، س و گرانی، ش، "جداسازی هرزنامه‌های متنی یک رویکرد مبتنی بر الگوریتم ژنتیک و روش دسته بندی SVM"، چهارمین کنفرانس انجمن رمز ایران، دانشگاه علم و صنعت ایران، ۲۴ – ۲۶ اسفند ۱۳۸۶.

۲- حلافی، ع و هارون‌آبادی، ع، "مروری بر تکنیک‌های فیلتر هرزنامه مبتنی بر محتوا"، دومین همایش ملی مهندسی کامپیوتر و فن‌آوری اطلاعات، باشگاه پژوهشگران جوان و نخبگان واحد شوشتر، اسفندماه ۱۳۹۳.

۳- کاظمی، ز، هارون‌آبادی، ع و میرعابدینی، س، "بازنگری رویکردهای پایه در تشخیص هرزنامه‌ها"، دومین همایش ملی مهندسی رایانه و مدیریت فناوری اطلاعات، دانشگاه شهید بهشتی، ۱۸ خرداد ۱۳۹۳.

4- رحیمی، ا، کاهانی، م، "شناسایی هرزنامه در نظرات"، سومین همایش رویکردهای آموزش های نوین در علوم کامپیوتر، دانشگاه فردوسی مشهد، شهریور ۱۳۹۳.

5- Izzat, A. Ikdam, A., " *Clustering and classification of email contents*" Journal of King Saud University – Computer and Information Sciences pp. 27, 46–57, 2003.

6- Aladdin Knowledge Systems, Anti-Spam white paper, http://www.ealaddin.com.

7- Santos, I. Laorden, C. Sanz, B. and Bringas, P.G., "*Enhanced topic-based vector space model for semantics-aware spam filtering* " Exp. Syst. Appl. 39, 2012.

8- Bratko, A. Filipic, B. Cormack, G. Lynam, T. and Zupan, B., *"Spam filtering using statistical data compression models"* The Journal of Machine Learning Research, pp. 2673–2698, 2006.

9- Kamini, B. and Josef, P., *"A Case Study of User-Level Spam Filtering"* Proceedings of the Twelfth Australasian Information Security Conference (AISC 2014), Auckland, New Zealand .

10- Yang, Y. and Pedersen, J.O., *"A comparative Study on Feature selection in Text Categorization*", In Proceedings of 14th International Conference on Machine Learningx, pp. ,412-420, 2008.

11- Chhabra, S., *"Fighting Spam, Phishing and Email Fraud"* Thesis.Computer Science 2005. Department, University of California Reverside.

12- Calton, P.u. and Webb, S., "*Observed trends in spam constraction techniques: A case study of spam evalution*" In Proceeding of Third Conference on Email and Anti-Spam,CEAS"pp. 104, 2006.

13- Goodman, J. and Rounthwaite, R., "*Stopping outgoing spam*" in Proceedings of the Fifth ACM Conference on Electronic Commerce, PP 30-39, 2004.

14- Cormack, G. and Lynam, T. " *Spam corpus creation for TREC*" In Proceedings of Second Conference on Email and Anti-Spam, pp. 28-3, 2005.

15- Wood, K. Kegelmeyer, W.p. and Bowyer, K., "*Combination of Multiple Classifiers using Local Accuracy Estimates"*, IEEE Transaction on Pattern Analysis and Machine, vol. 19x, pp. 115-111, 1888.
16- Santos, E.M.D. Sabourin, R, and Maupin, P., "*A Dynamic Overproduce-and-Choose Strategy for the Selection of Classifier Ensembles*", Pattern Recognition, vol. 41, pp.2993-3009, 2008.
17- Martin-Herran, G. Rubel, O. and Zaccour, G., "*Competing for consumer's Attention"* Automatica, 44(2), 361–37, 2008.
18- Guzella, T.S. and Walmir, M.C., "*A review of machine learning approaches to Spam filtering"* Expert Systems with Applications, 36(7), 2009. 10206e22.
19- Laorden, C. Pedrero, X. Santos, I. Sanz, B. Nieves, G. and Bringas, P.G., *"Study on the effectiveness of anomaly detection for spam Filtering"* Elsevier 0020-0255, 2014.
20- Sakkis, G. Androutsopoulos, I. Paliouras, G. Karkaletsis, V. Spyropoulos, C.D. and Stamatopoulos, P., "*Amemory-basedapproach to anti-spam filtering for mailing lists*" Inf.Retr.6(1), 49–73, 2003.
21- Kuropka, D., "*Modelle Reprsentation naturlichsprachlicher Dokumente-Information-Filtering und-Retrieval mit relationalen Datenbanken*" Advan Inform, Syst, Manage, Sci, 10, 2004.
22- Wilbur, W. Sirotkin, K., "*The automatic identification of stop words*" J, Inform, Sci, 18, pp. 45–55, 2003.
23- Santos, I. Laorden, C. Sanz, B. Bringas, P.G., "*Enhanced topic-based vector space model for semantics-aware spam filtering*" Exp, Syst, Appl, 39, 2012.
24- Bing, L., *"Sentiment Analysis and Opinion Mining*", Morgan & Claypool Publishers, May, 2012.
25- Castillo, Carlos., "*A reference collection for web spam*." ACM Sigir Forum. Vol. 40. No. 2. ACM, 2006.
26- Gyongyi, Z. and Garcia-Molina, H., *"Web Spam Taxonomy*" Technical Report, Stanford University, 2004.
27- Spirin, N. and Han, J., "*Survey on Web Spam Detection*": Principles and Algorithms Department of Computer Science University of Illinois at Urbana- Champaign Urbana, IL 61801, USA.
28- Cormack, G. and Lynam, T., "*Spam corpus creation for TREC.*" In Proceedings of Second Conference on Email and Anti-Spam,CEAS, 2005.
29- Nitin, J. and Liu, B., "*Opinion spam and analysis.*" Proceedings of the 2008 International Conference on Web Search and Data Mining. ACM, 2008.
30- Fung, G.P.C. Yu, J. X. Wang, H. CheungD.W. and Liu, H., "*A Balanced Ensemble Approach to Weighting Classifiers for Text Classification*", In Proceedings of the 6th International Conference on Data Mining (ICDM '06), pp. 869-873, 2006.
31- Khorsi. *"An overview of content-based spam filtering techniques"*, Informatics, 2007.
32- Sebastiani, F., "*Machine learning in automated text categorization*" *ACM Computing Surveys*, Vol. 34, No. 1, 2000.
33- Kołcz, A. and Alspector, J., *"SVM-based filtering of email spam with content-specific misclassification costs," Proc. of TextDM'01 Workshop on Text Mining*, 2001.
34- Schaffer, C., "*Selection a Classification Method by Cross-Validation* Machine Learning" vol. 13, pp.135-143, 1993.
35- Li, C.H. Huang, J.X., " *Spam filteringusingsemanticsimilarityapproachandadaptiveBPNN*" Neurocomputing pp. 88–97, 2012.
36- Commtouch Software Ltd.,[2010], Internet Threats Trend Report: http://www.commtouch.com/download/1679S [2010].