

گیلانو

● آشنایی با SSH

● آشنایی با حلقه های هوشمند
قابلیت ها و توانایی ها

● انجام بیشتر با تشخیص
الگو مویره در عکس های دیجیتال

● نحوه ارتباطات مخابراتی بین
شهری و درون شهری در ایران

● و
●
●

گیلانہ

● ماہنامہ علمی دانشجویی - سال سوم - شماره سی و پنجم - ۲۸ تیر ۱۴۰۳
● صاحب امتیاز: انجمن علمی مهندسی کامپیوتر دانشگاه آزاد اسلامی واحد لاهیجان
● مدیر مسئول: سورنا کریمی
● سردبیر: ریحانه محمدپور
● ویراستار: فرهاد فخری، سعید نیکفر
● طراحی جلد و صفحه آرایی: نگین شهبازی
● هیات تحریریه:
حجت آزادروش، پارمیدا پروری، حنانه خانه زرین، نغمه ربیعی زاد، امیرحسین شبرنگ،
زهرا قنبرپور، آیدا ملکی چوکامی، مهیار نحوی

فهرست

آشنایی با SSH ۳ صفحه

تجزیه و تحلیل عمیق از معماری شبکه عصبی کانولوشن با یادگیری انتقالی برای تشخیص بیماری های پوستی ۹ صفحه

آشنایی با حلقه های هوشمند: قابلیت ها و توانایی ها ۱۱ صفحه

انجام بیشتر با تشخیص الگو مویره در عکس های دیجیتال ۱۳ صفحه

نحوه ارتباطات مخابراتی بین شهری و درون شهری در ایران ۱۵ صفحه

ردیابی و دسته بندی اشیاء با فریم ورک Hybrid Neuromorphic برای سیستم های بلادرنگ ۱۸ صفحه

پیش بینی بارندگی مناطق هند با شبکه RfGanNet ۲۰ صفحه

یادگیری ترکیبی چندوجهی از طریق محتوای بایوسگنال، صوتی و بصری برای تشخیص استرس روانی ۲۲ صفحه



قوی، به طور گسترده توسط مدیران شبکه برای مدیریت سیستم‌ها و برنامه‌های کاربردی از راه دور استفاده می‌شود. به این ترتیب، مدیران می‌توانند از طریق SSH وارد رایانه‌های دیگر شوند، دستورات را اجرا کنند و فایل‌ها را بین کامپیوترها منتقل کنند.

SSH نه تنها به عنوان یک پروتکل شبکه رمزنگاری، بلکه به عنوان مجموعه‌ای از ابزارها که این پروتکل را پیاده‌سازی می‌کنند نیز شناخته می‌شود. پیاده‌سازی SSH معمولاً شامل پشتیبانی از پروتکل‌های کاربردی مورد استفاده برای شبیه‌سازی ترمینال یا انتقال فایل است. علاوه بر این، SSH می‌تواند برای ایجاد تونل‌های امن برای سایر پروتکل‌های برنامه نیز مورد استفاده قرار گیرد.



تاریخچه SSH

SSH در اواسط دهه ۱۹۹۰ توسط Tatu Ylönen، محقق دانشگاه فناوری هلسینکی به وجود آمد. انگیزه اصلی برای ایجاد این پروتکل، نیاز به یک روش ایمن‌تر برای انتقال اطلاعات در شبکه‌های کامپیوتری بود. در آن زمان، پروتکل‌هایی مانند Telnet و rlogin که برای ارتباطات راه دور استفاده می‌شدند، اطلاعات را به صورت متنی ساده و بدون رمزنگاری ارسال می‌کردند. این موضوع باعث می‌شد که این پروتکل‌ها در برابر حملات امنیتی نظیر استراق‌سمع (sniffing) و حملات میانجی (man-in-the-middle)، بسیار آسیب‌پذیر باشند.

در سال ۱۹۹۵، Ylönen اولین نسخه SSH را منتشر کرد که به سرعت به عنوان جایگزینی ایمن برای پروتکل‌های

در دنیای امروز، امنیت اطلاعات و ارتباطات از اهمیت ویژه‌ای برخوردار است. با گسترش روزافزون شبکه‌های کامپیوتری و اینترنت، نیاز به پروتکل‌های امن برای انتقال داده‌ها و مدیریت سیستم‌های راه دور بیشتر از همیشه احساس می‌شود. یکی از مهم‌ترین و پرکاربردترین پروتکل‌ها در این زمینه، SSH (Secure Shell) است که نقش بسزایی در تأمین امنیت ارتباطات در شبکه‌های کامپیوتری ایفا می‌کند.

SSH به عنوان یک پروتکل امن، امکان دسترسی و مدیریت سیستم‌های راه دور را فراهم می‌کند و با استفاده از تکنیک‌های رمزنگاری قوی، امنیت ارتباطات را تضمین می‌نماید. این پروتکل به مدیران شبکه اجازه می‌دهد تا به صورت امن به سرورهای خود متصل شوند، دستورات را اجرا کنند، فایل‌ها را انتقال دهند و سیستم‌ها را از هر مکانی مدیریت کنند.

در این مقاله، به بررسی جامع پروتکل SSH خواهیم پرداخت. تاریخچه، نحوه کارکرد، مزایا و معایب استفاده از SSH و تکنیک‌های رمزگذاری مورد استفاده در آن را مورد بحث قرار خواهیم داد. همچنین، این پروتکل را با Telnet مقایسه کرده و به OpenSSH به عنوان یکی از پرکاربردترین پیاده‌سازی‌های SSH اشاره خواهیم کرد. با مطالعه این مقاله، درک بهتری از اهمیت و عملکرد SSH به دست خواهید آورد که به شما کمک می‌کند تا بتوانید در تأمین امنیت ارتباطات شبکه و مدیریت سیستم‌ها، انتخاب‌های آگاهانه‌تری داشته باشید.

SSH چیست؟

SSH مخفف Secure Shell یا Secure Socket Shell یک پروتکل استاندارد برای ارتباط ایمن میان دو کامپیوتر در شبکه اینترنت است. این پروتکل با رمزنگاری تمامی اطلاعات مبادله شده، یکی از امن‌ترین سیستم‌های ارتباطی در شبکه‌های اینترنتی محسوب می‌شود.

SSH امکان احراز هویت با استفاده از رمز عبور قوی و کلید عمومی را فراهم می‌کند و ارتباطات داده‌ای رمزگذاری شده را بین دو کامپیوتری که از طریق شبکه‌های باز مانند اینترنت به هم متصل می‌شوند، تأمین می‌کند. این پروتکل علاوه بر ارائه رمزگذاری

قدیمی‌تر مورد استقبال قرار گرفت. این نسخه اولیه، SSH-1 نامیده شد و با استفاده از رمزنگاری قوی، ارتباطات ایمن بین دو سیستم را فراهم می‌کرد. با گسترش استفاده از SSH و افزایش نیاز به امنیت بیشتر، نسخه دوم این پروتکل به نام SSH-2 در سال ۲۰۰۶ معرفی شد. SSH-2 بهبودهای قابل توجهی در زمینه امنیت و عملکرد داشت و بسیاری از نواقص نسخه اولیه را برطرف کرد. به‌طور خاص، SSH-2 از الگوریتم‌های رمزنگاری قوی‌تر و مکانیزم‌های احراز هویت پیشرفته‌تر استفاده می‌کند.

امروزه، SSH به‌عنوان یکی از مهم‌ترین و پرکاربردترین پروتکل‌های ارتباطی در شبکه‌های کامپیوتری شناخته می‌شود و توسط بسیاری از سیستم‌عامل‌ها و ابزارهای مدیریت شبکه پشتیبانی می‌شود. این پروتکل نه تنها برای مدیریت از راه دور سیستم‌ها، بلکه برای انتقال امن فایل‌ها و ایجاد تونل‌های امن برای سایر پروتکل‌های کاربردی نیز به کار می‌رود.

نحوه عملکرد SSH

پروتکل SSH در پنج مرحله اصلی اجرا می‌شود:

۱- احراز هویت: ابتدا کلاینت با استفاده از پروتکل SSH اتصال به سرور را آغاز می‌کند. در این مرحله سرور کلید عمومی خود را به کلاینت ارائه می‌دهد تا فرآیند تبادل کلید SSH شروع شود.

۲- تبادل کلید: کلاینت، یک کلیدجلسه تصادفی تولید کرده و آن را با کلید عمومی سرور رمزگذاری می‌کند. سپس سرور این کلیدجلسه را با استفاده از کلید خصوصی خود رمزگشایی می‌کند. این کلیدجلسه به‌عنوان پایه‌ای برای ایجاد یک ارتباط امن و رمزنگاری شده بین کلاینت و سرور استفاده می‌شود.

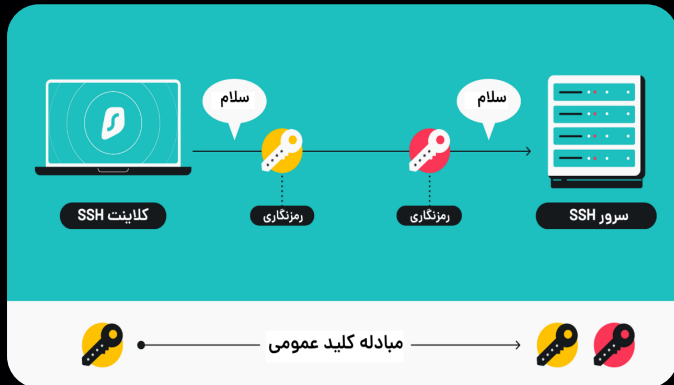
۳- ایجاد کانال رمزگذاری شده: پس از تبادل موفقیت‌آمیز کلید، کلاینت و سرور از این کلید برای رمزگذاری ارتباطات خود استفاده می‌کنند. این کار باعث می‌شود یک کانال امن برای انتقال داده‌ها برقرار شود و از اطلاعات مبادله شده در برابر استراق‌سمع و دستکاری محافظت شود.

۴- تأیید هویت کاربر: بعد از برقراری کانال امن، کلاینت باید هویت خود را به سرور احراز کند. این احراز هویت می‌تواند از طریق روش‌های مختلفی مانند استفاده از رمز عبور، کلید عمومی یا احراز هویت چندعاملی انجام شود. این مرحله، تضمین می‌کند که تنها کاربران مجاز

می‌توانند به سرور دسترسی پیدا کنند.

۵- دسترسی از راه دور: پس از احراز هویت موفق، کلاینت به سیستم از راه دور دسترسی پیدا می‌کند. این دسترسی کاملاً امن بوده و به کلاینت اجازه می‌دهد تا وظایف مختلفی مانند اجرای دستورات، انتقال فایل‌ها و مدیریت سرور را از راه دور انجام دهد.

این پنج مرحله نشان می‌دهند که SSH چگونه با ایجاد یک ارتباط امن و رمزنگاری شده، ارتباطات بین دو سیستم را ایمن می‌سازد و امکان مدیریت و انتقال داده‌ها را به‌صورت ایمن فراهم می‌کند.



مزایای استفاده از SSH

استفاده از SSH دارای مزایای متعددی است که این پروتکل را به یکی از پرکاربردترین و قابل‌اعتمادترین روش‌ها برای ارتباطات امن در شبکه‌های کامپیوتری تبدیل کرده است. در ادامه به برخی از این مزایا اشاره شده است:

۱- امنیت بالا: SSH با استفاده از الگوریتم‌های رمزنگاری قوی، اطلاعات مبادله شده بین کلاینت و سرور را رمزگذاری می‌کند. این امر از دستکاری و حملات میانجی جلوگیری می‌کند و امنیت اطلاعات را تضمین می‌کند.

۲- احراز هویت قوی: SSH امکان احراز هویت با استفاده از رمز عبور قوی و کلیدهای عمومی را فراهم می‌کند. این روش‌های احراز هویت تضمین می‌کنند که فقط کاربران مجاز به سیستم دسترسی پیدا کنند و امنیت سیستم افزایش یابد.

۳- مدیریت از راه دور: یکی از مهم‌ترین مزایای SSH امکان مدیریت سیستم‌ها و سرورها از راه دور است. مدیران شبکه می‌توانند با استفاده از SSH به سرورهای خود متصل شده، دستورات را اجرا کنند، فایل‌ها را انتقال دهند و سیستم‌ها را از هر مکانی مدیریت کنند.

۴- انتقال امن فایل‌ها: SSH از پروتکل‌های SFTP

SCP (Secure Copy Protocol) SSH File Transfer Protocol پشتیبانی می‌کند که امکان انتقال فایل‌ها به صورت امن بین سیستم‌ها را فراهم می‌کند. این امر به کاربران اجازه می‌دهد فایل‌ها را بدون نگرانی از افشای اطلاعات منتقل کنند.

۵- پشتیبانی از تونل‌سازی (Tunneling): SSH می‌تواند تونل‌های رمزنگاری شده ایجاد کند که از آن‌ها برای انتقال امن سایر پروتکل‌های شبکه استفاده می‌شود. این قابلیت به کاربران اجازه می‌دهد که پروتکل‌های غیرامن را در یک تونل امن قرار دهند و ارتباطات خود را ایمن کنند.

۶- انعطاف‌پذیری و قابلیت سفارشی‌سازی: SSH یک پروتکل بسیار انعطاف‌پذیر است که می‌تواند برای نیازهای مختلف سفارشی‌سازی شود. از آنجا که SSH به صورت متن‌باز است، می‌توان آن را مطابق با نیازهای خاص شبکه و امنیت تنظیم کرد.

۷- پشتیبانی گسترده: SSH توسط اکثر سیستم‌عامل‌های مدرن و ابزارهای مدیریت شبکه پشتیبانی می‌شود. این پشتیبانی گسترده، استفاده از SSH را برای مدیریت و ارتباطات شبکه آسان و فراگیر کرده است.

۸- کاهش خطرات: با استفاده از SSH، خطرات مرتبط با پروتکل‌های قدیمی‌تر و ناامن مانند Telnet و FTP که اطلاعات را به صورت متنی ساده منتقل می‌کردند، کاهش می‌یابد. SSH با ارائه رمزنگاری قوی و احراز هویت پیشرفته، سطح امنیتی بسیار بالاتری را فراهم می‌کند.

معایب استفاده از SSH

با وجود مزایای فراوان، استفاده از SSH نیز دارای برخی معایب و محدودیت‌ها می‌باشد که در ادامه به برخی از آن‌ها اشاره می‌شود:

۱- پیچیدگی در تنظیمات: راه‌اندازی و پیکربندی SSH ممکن است پیچیده و زمان‌بر باشد، به ویژه برای کسانی که تازه با این پروتکل آشنا شده‌اند. تنظیمات نادرست، می‌تواند به مشکلات امنیتی منجر شود.

۲- مشکلات عملکردی در شبکه‌های بزرگ: در شبکه‌های بزرگ و پیچیده، مدیریت و نظارت بر اتصالات SSH می‌تواند چالش‌برانگیز باشد. تعداد زیاد اتصالات، همزمان می‌تواند منابع سرور را به طور قابل توجهی مصرف کند و عملکرد سیستم را تحت تأثیر قرار دهد.

۳- نیاز به کلیدهای خصوصی و عمومی: مدیریت

کلیدهای خصوصی و عمومی، می‌تواند پیچیده باشد و نیاز به نگهداری و پشتیبانی دقیق دارد. اگر کلیدهای خصوصی به درستی مدیریت نشوند یا در معرض خطر قرار گیرند، امنیت سیستم به شدت تهدید می‌شود.

۴- حملات بروت فورس (Brute Force): اگر احراز هویت SSH به درستی پیکربندی نشده باشد، ممکن است در معرض حملات بروت فورس قرار گیرد. مهاجمان می‌توانند با استفاده از این روش‌ها تلاش کنند تا رمز عبور یا کلیدهای احراز هویت را حدس بزنند و به سیستم دسترسی پیدا کنند.

۵- نقاط ضعف در نسخه‌های قدیمی: نسخه‌های قدیمی‌تر SSH، مانند SSH-1 دارای نقاط ضعف امنیتی هستند که ممکن است مهاجمان بتوانند از آن‌ها سوءاستفاده کنند. استفاده از نسخه‌های به روز و پیکربندی صحیح برای کاهش این خطرات، ضروری است.

۶- مصرف منابع: اتصالات SSH ممکن است منابع قابل توجهی از سیستم از جمله CPU و حافظه را مصرف کنند. این موضوع، به ویژه در سرورهایی که تعداد زیادی اتصال همزمان دارند، می‌تواند مشکلات عملکردی ایجاد کند.

۷- اعتماد به کلیدهای احراز هویت: اگر یک کلید خصوصی به سرقت برود یا به درستی محافظت نشود، می‌تواند به مهاجمان اجازه دسترسی به سیستم‌ها و داده‌های حساس را بدهد. بنابراین، حفاظت از کلیدهای خصوصی از اهمیت بالایی برخوردار است.

۸- محدودیت‌های پهنای باند اینترنت: استفاده از رمزنگاری قوی می‌تواند مصرف پهنای باند را افزایش دهد، که ممکن است در شبکه‌هایی با پهنای باند محدود، مشکل‌ساز شود.

۹- پیکربندی‌های اشتباه و ناآگاهی کاربران: ناآگاهی کاربران و پیکربندی‌های اشتباه، می‌تواند منجر به نقض امنیتی شود. آموزش مناسب کاربران و اطمینان از پیکربندی صحیح SSH برای جلوگیری از این مشکلات ضروری است.

تکنیک‌های رمزگذاری SSH

پروتکل SSH از چندین تکنیک رمزگذاری برای اطمینان از امنیت ارتباطات استفاده می‌کند. این تکنیک‌ها شامل رمزگذاری متقارن، رمزگذاری نامتقارن، توابع هش و

امضاهای دیجیتالی برای احراز هویت و یکپارچگی داده‌ها هستند. در ادامه به توضیح این تکنیک‌ها خواهیم پرداخت:

۱- رمزگذاری متقارن (Symmetric Encryption): در رمزگذاری متقارن، از یک کلید مشترک برای رمزگذاری و رمزگشایی داده‌ها استفاده می‌شود. این کلید در طول مرحله تبادل کلید (Key Exchange) تولید و بین کلاینت و سرور به اشتراک گذاشته می‌شود. الگوریتم‌های متقارن معمولاً برای رمزگذاری داده‌های انتقالی در طول جلسه SSH به کار می‌روند. برخی از الگوریتم‌های متقارن مورد استفاده در SSH شامل موارد زیر هستند:

۱-AES(Advanced Encryption Standard): یکی از پرکاربردترین الگوریتم‌های رمزگذاری با کلیدهای ۱۲۸، ۱۹۲، و ۲۵۶ بیتی.

2- ChaCha20:

یک الگوریتم جریان قوی و سریع که برای دستگاه‌های با منابع محدود مناسب است.

۲- رمزگذاری نامتقارن (Asymmetric Encryption): رمزگذاری نامتقارن از دو کلید متفاوت، کلید عمومی و کلید خصوصی استفاده می‌کند. کلید عمومی برای رمزگذاری و کلید خصوصی برای رمزگشایی به کار می‌رود. این تکنیک در SSH برای تبادل کلید اولیه و احراز هویت استفاده می‌شود. برخی از الگوریتم‌های نامتقارن مورد استفاده در SSH عبارت‌اند از:

1-RSA(Rivest-Shamir-Adleman):

یک الگوریتم رمزگذاری نامتقارن که برای تبادل کلید و احراز هویت به کار می‌رود.

2- ECDSA (Elliptic Curve Digital Signature Algorithm):

یک الگوریتم مبتنی بر منحنی‌های بیضوی که برای امضاهای دیجیتالی و احراز هویت استفاده می‌شود.

3-Ed25519:

یک الگوریتم جدید و بسیار امن که برای کلیدهای عمومی SSH استفاده می‌شود.

۳- تبادل کلید (Key Exchange): فرآیند تبادل کلید به منظور ایجاد یک کلید جلسه مشترک بین کلاینت و سرور انجام می‌شود. این کلید جلسه برای رمزگذاری متقارن استفاده می‌شود. الگوریتم‌های تبادل کلید

مورد استفاده در SSH عبارت‌اند از:

1-Diffie-Hellman:

یک روش رایج برای تبادل کلید به صورت امن.

2-ECDH(Elliptic Curve Diffie-Hellman):

یک نسخه کارآمدتر و امن‌تر از Diffie-Hellman که از منحنی‌های بیضوی استفاده می‌کند.

۴- توابع هش (Hash Functions): توابع هش برای ایجاد کدهای تأیید صحت پیام استفاده می‌شوند که یکپارچگی و اصالت داده‌ها را تضمین می‌کنند. این توابع هش به هر پیام، یک مقدار هش منحصر به فرد با طول ثابت اختصاص می‌دهند.

الگوریتم‌های هش مورد استفاده در SSH عبارت‌اند از:

1-SHA-2(Secure Hash Algorithm):

یک مجموعه از توابع هش که امنیت بالا و عملکرد خوبی دارند.

2-SHA-3:

یک تابع هش جدیدتر که برای افزایش امنیت طراحی شده است.

۵- امضاهای دیجیتالی (Digital Signatures): امضاهای دیجیتالی برای احراز هویت و تأیید اصالت داده‌ها به کار می‌روند. این امضاها با استفاده از کلید خصوصی فرستنده ایجاد و با کلید عمومی گیرنده بررسی می‌شوند. الگوریتم‌های مورد استفاده برای امضاهای دیجیتالی در HSS عبارت‌اند از:

1-RSA:

برای امضا و احراز هویت.

2-ECDSA:

برای امضاهای دیجیتالی امن‌تر و کارآمدتر.

3-Ed25519:

برای امضاهای دیجیتالی سریع و بسیار امن.

این تکنیک‌های رمزگذاری باعث می‌شوند SSH یک پروتکل امن و قابل اعتماد برای ارتباطات شبکه‌ای باشد. با استفاده از ترکیبی از رمزگذاری متقارن و نامتقارن، توابع هش و امضاهای دیجیتالی، SSH تضمین می‌کند که اطلاعات مبادله شده بین کلاینت و سرور، امن و

7-SSH-Add:

ابزار اضافه کردن کلیدهای خصوصی به SSH-Agent.

OpenSSH با ارائه این ویژگی‌ها و ابزارها، به یکی از استانداردهای اصلی برای ارتباطات امن و مدیریت سیستم‌ها در شبکه‌های کامپیوتری تبدیل شده است. این مجموعه نرم‌افزاری به دلیل متن‌باز بودن، قابلیت اطمینان بالا و پشتیبانی گسترده از پروتکل‌ها و روش‌های احراز هویت، به‌طور گسترده در محیط‌های مختلف از جمله سازمان‌های تجاری، دولتی و آموزشی استفاده می‌شود.



تفاوت SSH با Telnet

Telnet و SSH دو پروتکل ارتباطی هستند که برای دسترسی و مدیریت سیستم‌های راه دور استفاده می‌شوند. هر چند که هدف اصلی هر دو پروتکل یکسان است اما تفاوت‌های مهمی در زمینه امنیت و عملکرد دارند. در ادامه به بررسی تفاوت‌های کلیدی بین Telnet و SSH اشاره می‌شود:

۱- امنیت: از نظر امنیتی، پروتکل Telnet بسیار ضعیف است، زیرا تمامی داده‌ها را به‌صورت متن ساده (Plain Text) منتقل می‌کند، اما SSH از رمزنگاری قوی برای تمامی داده‌های منتقل شده استفاده می‌کند که امنیت ارتباط را تضمین می‌کند.

۲- احراز هویت: از نظر احراز هویت، Telnet تنها از نام کاربری و رمز عبور استفاده می‌کند که به‌صورت متن ساده ارسال می‌شوند، اما SSH از روش‌های مختلفی مانند کلیدهای عمومی و احراز هویت چندعاملی استفاده می‌کند که امنیت بیشتری را فراهم می‌کند.

۳- قابلیت‌ها: از نظر قابلیت‌ها، Telnet تنها برای ارسال دستورات ساده به سیستم‌های راه دور مناسب است، اما SSH امکانات بیشتری مانند انتقال امن فایل‌ها (SFTP و SCP) و تونل‌سازی (Tunneling) را فراهم می‌کند.

۴- کاربردها: Telnet به دلیل ناامن بودن، بیشتر در شبکه‌های داخلی و کاربردهای غیرحساس استفاده می‌شود، اما SSH به‌طور گسترده در مدیریت سیستم‌های راه دور و انتقال امن داده‌ها در شبکه‌های مختلف استفاده می‌شود.



OpenSSH یک مجموعه نرم‌افزاری متن‌باز است که از پروتکل SSH برای برقراری ارتباطات امن و رمزنگاری شده بین دو سیستم کامپیوتری استفاده می‌کند. OpenSSH توسط پروژه OpenBSD توسعه داده شده و به‌عنوان یکی از پرکاربردترین و مطمئن‌ترین ابزارهای SSH شناخته می‌شود. این مجموعه شامل ابزارهای مختلفی برای مدیریت ارتباطات راه دور و انتقال امن داده‌ها است. این نرم‌افزار ابزارهای مختلفی دارد که از مهم‌ترین آنها عبارت‌اند از:

1-SSHD:

سرویس‌دهنده SSH که درخواست‌های اتصال SSH را می‌پذیرد و پردازش می‌کند.

2-SSH:

کلاینت SSH که برای برقراری ارتباط با سرویس‌دهنده‌های SSH استفاده می‌شود.

3-SCP:

ابزار انتقال امن فایل که از پروتکل SCP استفاده می‌کند.

4-SFTP:

کلاینت SFTP که برای انتقال امن فایل‌ها استفاده می‌شود.

5-SSH-Keygen:

ابزار تولید و مدیریت کلیدهای SSH.

6-SSH-Agent:

کند. در نتیجه، آشنایی و استفاده مناسب از SSH برای مدیران شبکه و افرادی که به امنیت اطلاعات و ارتباطات خود اهمیت می‌دهند، ضروری است. این پروتکل نه تنها امنیت و اعتماد بیشتری را به همراه دارد، بلکه با امکانات گسترده‌ای که ارائه می‌دهد، کارایی و مدیریت سیستم‌ها را نیز بهبود می‌بخشد. با انتخاب آگاهانه و پیاده‌سازی صحیح SSH می‌توانید از مزایای بی‌شمار آن بهره‌مند شوید و امنیت شبکه خود را به سطح بالاتری ارتقا دهید.

منابع:

<https://www.ssh.com/academy/ssh>

<https://www.cloudflare.com/learning/access-management/what-is-ssh>

<https://medium.com/@aqeelabbas3972/introduction-to-ssh-secure-shell-0d07e18d3149>



۵- پشتیبانی از سیستم‌عامل‌ها: هر دو پروتکل به‌طور گسترده پشتیبانی می‌شوند؛ اما SSH به‌عنوان ابزار استاندارد برای ارتباطات امن ترجیح داده می‌شود، در حالی که Telnet اغلب به‌دلیل ناامن بودن غیرفعال است.

جمع‌بندی

SSH به‌عنوان یک پروتکل ارتباطی امن، نقش حیاتی در برقراری ارتباط بین سیستم‌های کامپیوتری ایفا می‌کند. SSH از کلیدهای عمومی و خصوصی بهره می‌برد تا ارتباطی رمزنگاری شده و امن را فراهم کند. کاربران با استفاده از کلیدهای عمومی، اطلاعات خود را هنگام ارسال رمزگذاری کرده و سپس این اطلاعات در مقصد با استفاده از کلیدهای خصوصی رمزگشایی می‌شوند. به این ترتیب، کلیدهای SSH جایگزینی مطمئن و امن برای نام‌های کاربری و رمزهای عبور قدیمی محسوب می‌شوند.

در این مقاله به بررسی جامع پروتکل SSH پرداختیم و جوانب مختلف آن را مورد بحث قرار دادیم. از تاریخچه ایجاد و توسعه این پروتکل توسط Tatu Ylönen در اواسط دهه ۱۹۹۰، تا نحوه کارکرد آن در پنج مرحله اصلی و تکنیک‌های رمزگذاری مورد استفاده در SSH را مرور کردیم. همچنین، مزایا و معایب این پروتکل را بررسی کرده و نشان دادیم که چگونه SSH به‌عنوان یکی از امن‌ترین و قابل‌اعتمادترین روش‌ها برای دسترسی و مدیریت سیستم‌های راه دور شناخته می‌شود.

مقایسه بین SSH و Telnet نشان داد که SSH با استفاده از رمزنگاری قوی و احراز هویت پیشرفته، امنیت بسیار بیشتری نسبت به Telnet ارائه می‌دهد و به‌همین دلیل به‌عنوان جایگزینی امن برای Telnet در اکثر کاربردها مورد استفاده قرار می‌گیرد. علاوه بر این، با معرفی OpenSSH به‌عنوان یکی از پیاده‌سازی‌های متن‌باز و پرکاربرد SSH، امکانات و ابزارهای بیشتری برای مدیریت امن سیستم‌ها و انتقال داده‌ها فراهم شده است.

با مطالعه این مقاله، درک بهتری از اهمیت و عملکرد پروتکل SSH به دست خواهید آورد. این پروتکل با فراهم کردن ارتباطات امن و مدیریت سیستم‌های راه دور، نقش حیاتی در تأمین امنیت شبکه‌های کامپیوتری ایفا می‌کند. استفاده صحیح و به‌روز از SSH می‌تواند به‌طور قابل‌توجهی، امنیت ارتباطات شبکه‌ای را افزایش داده و از دسترسی‌های غیرمجاز جلوگیری



استفاده می‌شوند. در مرحله بعد که آماده‌سازی داده‌ها می‌باشد، چون تعداد تصاویر کافی نبود، از تکنیک‌های افزایش داده‌ها استفاده شد. این تکنیک‌ها شامل تغییر اندازه، چرخش و تغییر روشنایی تصاویر است تا مدل بتواند با تصاویر متنوع‌تری آموزش ببیند.

سپس مدل‌های شبکه عصبی پیچشی MobileNet و Xception که قبلاً روی یک مجموعه داده بزرگ -

(ImageNet) آموزش دیده‌اند، به کار گرفته شدند. این مدل‌ها می‌توانند ویژگی‌های کلی تصاویر را بشناسند. در مرحله یادگیری انتقالی، وزن‌های این مدل‌های پیش‌آموزش دیده به مدل‌های جدید منتقل شدند. این کار باعث می‌شود مدل‌ها سریع‌تر و با دقت بیشتری یاد بگیرند، چون از دانش قبلی استفاده می‌کنند. سپس با استفاده از داده‌های آماده‌شده و مدل‌های پیش‌آموزش دیده، مدل نهایی آموزش داده شد و در محیط Google Colab انجام شد. مدل‌ها با اضافه کردن لایه‌های اضافی بهبود داده شدند و تنظیمات بهینه‌سازی نیز اعمال شد.

در گام بعدی برای ارزیابی عملکرد مدل‌ها در شناسایی بیماری‌های پوستی، از معیارهایی مانند دقت، ماتریس سردرگمی و نمودارهای ROC استفاده شدند و نتایج نشان داد که مدل‌ها با دقت و کارایی بالا قادر به تشخیص بیماری‌های پوستی هستند.

در نهایت نیز، مدل‌های آموزش‌دیده برای پیش‌بینی بیماری‌های پوستی روی تصاویر جدید استفاده شدند؛ به این صورت که از چارچوب وب Flask برای استقرار مدل آموزش‌دیده استفاده شده و یک برنامه وب با استفاده از مدل Xception ایجاد شد که با تجزیه و تحلیل عکس پوست ارائه شده توسط کاربر، شرایط پوست را تشخیص می‌دهد؛ به این صورت که کاربر تصویر یک منطقه مشکوک به بیماری را با استفاده از هر دستگاه هوشمند آپلود می‌کند و آن را از طریق رابط به سیستم متخصص توسعه‌یافته یا برنامه وب ارسال می‌کند. سپس بازخورد بر اساس مدل آموزش‌دیده با طبقه‌بندی تصویر بر اساس شرایط مختلف پوست ایجاد می‌شود و در نهایت مدل توانست به درستی کلاس‌های

پوست حساس‌ترین و مهم‌ترین اندام بدن انسان است که از گرما، آسیب و عفونت محافظت می‌کند. متأسفانه گاهی اوقات شرایط پوست به دلیل عوامل باکتریایی، ویروسی، قارچی، سیستم ایمنی ضعیف و اختلالات ژنتیکی مختل می‌شود و بیماری‌های پوستی را ایجاد می‌کند. بسیاری از این بیماری‌ها واگیردار هستند و نه تنها برای فرد، بلکه برای دیگران نیز خطرناک هستند. تشخیص زودهنگام بیماری‌های پوستی می‌تواند خطرات آنها را تا حد زیادی کاهش دهد.

هوش مصنوعی می‌تواند راه حل بسیار خوبی برای توسعه سیستم‌های تشخیص بیماری‌های پوستی بر اساس تصاویر باشد. همچنین استفاده از مدل‌های یادگیری عمیق به دلیل دقت بالا در شناسایی الگوها و ویژگی‌های تصاویر، در این حوزه محبوبیت زیادی پیدا کرده‌اند.

Rifat Sadik و همکارانش، با هدف توسعه و ارزیابی یک سیستم خودکار برای تشخیص بیماری‌های پوستی با استفاده از مدل‌های یادگیری عمیق و بررسی کارایی آن‌ها در مقایسه با مدل‌های دیگر، توانستند راهحلی کارآمد برای تشخیص بیماری‌های پوستی با پیاده‌سازی معماری شبکه عصبی کانولوشنال ارائه کنند.

در این مطالعه، یک سیستم خودکار مبتنی بر تکنیک‌های بینایی کامپیوتر پیاده‌سازی شده که در آن دو معماری شبکه عصبی کانولوشنال ساختاریافته MobileNet و Xception به شناخت انواع مختلف بیماری‌های پوستی مانند درماتیت آتوپیک، اگزما، هرپس، خال و ملانوما کمک می‌کند. همچنین به منظور ساخت یک مدل دقیق، این دو معماری با یادگیری انتقالی و فرآیند تقویت تصویر در زمان واقعی، ترکیب شده است.

در واقع، این رویکرد پیشنهادی می‌تواند با شناخت موثرتر بیماری‌های پوستی مختلف، به پزشکان کمک کند و فرآیند تشخیص بیماری را بهبود ببخشد.

روش پژوهش

برای استفاده از سیستم پیشنهادی، در ابتدا تصاویر مختلفی از پنج نوع بیماری پوستی جمع‌آوری شده است. این تصاویر به‌عنوان داده‌های آموزشی برای مدل

از جهت‌گیری‌های تحقیقاتی آینده هم می‌تواند توسعه یک مدل تشخیص تصویر مبتنی بر ترانسفورماتور برای تشخیص بیماری‌های پوستی باشد.

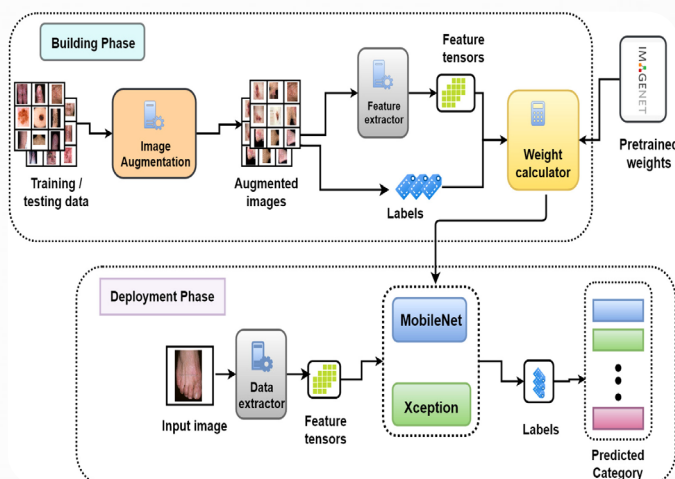


بیماری را پیش‌بینی کند.



Predict Clear

Predicted disease:
Herpes



1-<https://www.sciencedirect.com/science/article/pii/S2772442523000102>

2-<https://doi.org/10.1016/j.health.2023.100143>

3-Sadik, R., Majumder, A., Biswas, A. A., Ahammad, B., & Rahman, M. M. (2023). An in-depth analysis of Convolutional Neural Network architectures with transfer learning for skin disease diagnosis. *Healthcare Analytics*, 3, 100143

منابع:

معماری سیستم پیشنهادی «نمایشی سیستماتیک از رویکرد پیشنهادی که عبارت‌اند از: جمع‌آوری داده‌ها، پیش‌پردازش با استفاده از تقویت، یادگیری انتقالی، آموزش، آزمایش و پیش‌بینی‌های انجام شده در مراحل ساخت و استقرار»

نتیجه‌گیری:

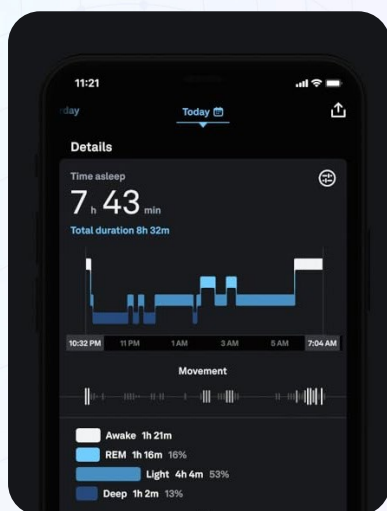
در مجموع، سیستم پیشنهادی نشان داد که با استفاده از مدل‌های MobileNet و Xception با تکنیک‌های یادگیری انتقالی و افزایش داده‌ها، می‌تواند به‌طور موثری در تشخیص بیماری‌های پوستی کمک کند. علاوه بر این، یک برنامه وب مبتنی بر فریم‌ورک Flask توسعه داده شده است که امکان تشخیص بیماری‌های پوستی را به‌صورت آنلاین فراهم می‌کند. این سیستم می‌تواند به پزشکان و متخصصین حوزه سلامت کمک کند تا تشخیص دقیق‌تری داشته باشند و همچنین فرآیند تشخیص را برای بیماران آسان‌تر کند. برای تحقیقات آینده نیز، برنامه‌ریزی شده است که از مجموعه داده‌های متنوع‌تری استفاده شود و کلاس‌های بیشتری از بیماری‌های پوستی مورد مطالعه قرار گیرد. یکی دیگر



آشنایی با حلقه‌های هوشمند: قابلیت‌ها و توانایی‌ها

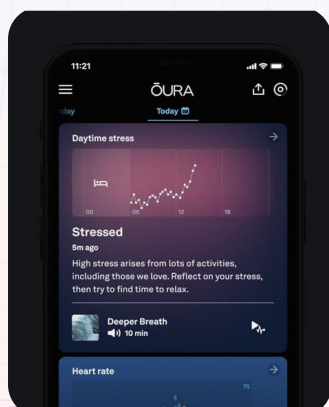
خانه‌زیرین دانشجوی کارشناسی مهندسی کامپیوتر

مانیتور کرده و اطلاعاتی درباره کیفیت، مدت‌زمان و الگوهای خواب ارائه می‌دهند. به‌عنوان مثال، Oura از Ring از حسگرهای نور «فوتوپلیتیسموگرام» (PPG) برای اندازه‌گیری حجم خون و تشخیص مراحل خواب استفاده می‌کند. همچنین استفاده از حلقه‌های هوشمند در خواب به دلیل کوچک بودن و سبکی نصب به ساعت‌ها و مچ‌بند‌های هوشمند بهتر است.



۳- ردیابی فعالیت: حلقه‌ها فعالیت‌های روزانه مانند تعداد قدم‌ها، مسافت طی شده و کالری سوزانده شده را ردیابی می‌کنند. این ویژگی کاربران را تشویق می‌کند تا فعال بمانند و به اهداف تناسب‌اندام خود برسند.

به‌طورکلی، حلقه‌های هوشمند با توجه به مدل‌های مختلف، قابلیت‌های مختلفی در زمینه سلامت دارند. برخی حلقه‌ها می‌توانند دمای بدن را مانیتور کنند که به تشخیص تب یا ردیابی چرخه‌های قاعدگی کمک می‌کند؛ برخی فشارخون و سطح گلوکز را ردیابی می‌کنند و بعضی از مدل‌ها، قابلیت اندازه‌گیری سطح استرس را از طریق فناوری الکترودرمال (EDA) دارند.



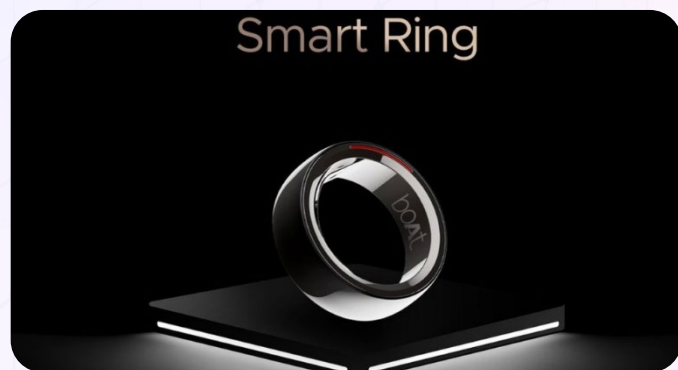
اعلان‌های هوشمند

حلقه‌های هوشمند می‌توانند اعلان‌هایی از تلفن همراه شما دریافت کنند و نیاز به بررسی مداوم گوشی را کاهش دهند. این اعلان‌ها می‌توانند شامل موارد زیر باشند:

۱- تماس‌ها و پیام‌ها:

اعلان‌های تماس‌های ورودی، پیامک‌ها و اعلان‌های اپلیکیشن‌ها به صورت لرزش یا نمایشگر LED به کاربر اطلاع داده می‌شود.

حلقه‌های هوشمند، به‌عنوان یکی از فناوری‌های پوشیدنی نوظهور، طیف وسیعی از قابلیت‌ها را در قالبی کوچک و شیک ارائه می‌دهند. این حلقه‌ها، با ترکیب راحتی و فناوری پیشرفته، امکانات مختلفی از مانیتورینگ سلامت تا راه‌حل‌های پرداخت هوشمند را برای کاربران فراهم می‌کنند. در این مقاله، به بررسی ویژگی‌ها و توانایی‌های اصلی حلقه‌های هوشمند می‌پردازیم و مزایا و کاربردهای آن‌ها را بیان می‌کنیم.



مانیتورینگ سلامت و تناسب‌اندام

یکی از ویژگی‌های برجسته حلقه‌های هوشمند، مانیتورینگ سلامت و تناسب‌اندام است. این حلقه‌ها مجهز به حسگرهایی هستند که پارامترهای مختلف فیزیولوژیکی را اندازه‌گیری می‌کنند:



۱- مانیتورینگ ضربان قلب: حلقه‌های هوشمندی مانند Oura Ring و Motiv Ring به‌طور پیوسته سطح ضربان قلب و اکسیژن خون را در طول روز و شب اندازه‌گیری می‌کنند. این امر به درک بهتر سلامت قلبی و شناسایی زودهنگام ناهنجاری‌ها کمک می‌کند.

۲- ردیابی خواب: ردیابی دقیق خواب یکی از ویژگی‌های برجسته است. حلقه‌های هوشمند، مراحل خواب را

۲- ایمیل‌ها و شبکه‌های اجتماعی: ایمیل‌های مهم و به‌روزرسانی‌های شبکه‌های اجتماعی می‌توانند به‌گونه‌ای تنظیم شوند که به کاربر اطلاع داده شوند و اطمینان حاصل شود که اطلاعات حیاتی از دست نمی‌رود.

پرداخت‌های بدون تماس

مشابه کارت‌های پرداخت بدون تماس، حلقه‌های هوشمند با فناوری NFC «ارتباطات میدان نزدیک» به کاربران امکان می‌دهند تا پرداخت‌های امن را تنها با لمس حلقه به پایانه پرداخت انجام دهند. حلقه McLearn نمونه‌ای برجسته است که به کاربران امکان می‌دهد تا بدون نیاز به حمل پول نقد یا کارت، تراکنش‌ها را انجام دهند.



کنترل دسترسی

حلقه‌های هوشمند می‌توانند به‌عنوان کلیدهای دیجیتال برای اهداف مختلف عمل کنند:

۱- دسترسی به خانه و محل کار: حلقه‌های مجهز به NFC یا بلوتوث می‌توانند درها را باز کنند و جایگزین کلیدهای سنتی یا کارت‌های دسترسی شوند.

۲- کنترل دستگاه‌ها: این حلقه‌ها می‌توانند دستگاه‌های هوشمند خانگی مانند چراغ‌ها، ترموستات‌ها و سیستم‌های امنیتی را کنترل کنند و راحتی و امنیت بیشتری را فراهم کنند.



ویژگی‌های امنیتی

حلقه‌های هوشمند می‌توانند با ارائه احراز هویت دومرحله‌ای (FA۲) برای حساب‌های آنلاین، امنیت

شخصی را افزایش دهند. این ویژگی اطمینان می‌دهد که حتی اگر رمز عبور به خطر بیفتد، از دسترسی غیرمجاز جلوگیری می‌شود. یکی از دیگر قابلیت‌های امنیتی، احراز هویت بیومتریک است که روشی پیشرفته و امن برای تأیید هویت افراد است که بر اساس ویژگی‌های فیزیکی یا شناختی منحصربه‌فرد انجام می‌شود. این ویژگی، لایه‌ای اضافی از امنیت را به اطلاعات حساس و تراکنش‌های مالی اضافه می‌کند که حلقه‌های هوشمند مانند Motiv در حال توسعه این قابلیت بر روی حلقه خود هستند.

طول عمر باتری

حلقه‌های هوشمند به دلیل اندازه کوچکشان به‌طورکلی، در صورت استفاده مداوم تا ۷ روز قابلیت شارژدهی دارد.

حلقه‌های هوشمند موجود در بازار

۱- حلقه هوشمند Oura نسل سوم

۲- اسمارت رینگ Motiv

۳- حلقه هوشمند McLEAR

۴- انگشتر هوشمند Noise Luna

۵- حلقه هوشمند boAt



حلقه هوشمند boAt Gen 1 S7

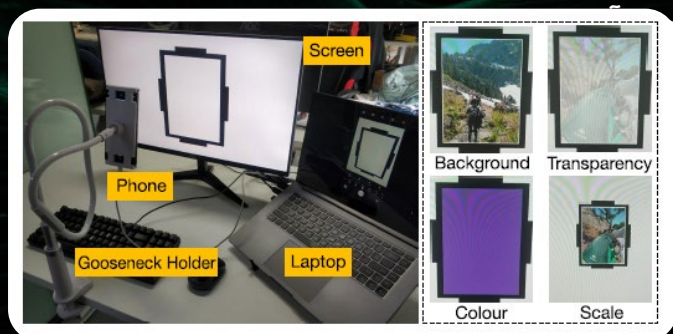
حلقه‌های هوشمند به‌عنوان یکی از نوآوری‌های مهم در حوزه فناوری‌های پوشیدنی، امکانات و قابلیت‌های فراوانی را در اختیار کاربران قرار می‌دهند. با وجود چالش‌ها و محدودیت‌های موجود، این دستگاه‌ها پتانسیل زیادی برای بهبود کیفیت زندگی و افزایش کارایی در زمینه‌های مختلف دارند. با پیشرفت تکنولوژی، انتظار می‌رود حلقه‌های هوشمند در زندگی روزمره ما قدرتمندتر و ضروری‌تر شوند.



انجام بیشتر با تشخیص الگو مویره در عکس های دیجیتال

نغمه ربیعی زاد | دانشجوی کارشناسی ارشد مهندسی کامپیوتر - گرایش هوش مصنوعی

از مجموعه داده های موجود COCO، ImageNet، PAS، CAL VOC و Retail50K به صورت تصادفی انتخاب شد. تصاویر مجموعه Retail50K به دلیل صحنه های متراکم، پیچیده ترین پس زمینه را دارند. در مجموع، ۱۸۱۴۷ لایه مویره مختلف و ۴۰۰۰ تصویر طبیعی



الگوهای مویره یک پدیده ناخواسته در تصویر دیجیتال هستند که در اثر تداخل الگوهای متناوب ایجاد می شوند. این الگوها بیشتر در تصاویر گرفته شده از صفحه نمایش های دیجیتال «گوشی، مانیتور و...» مشاهده می شوند و می توانند کیفیت تصاویر را کاهش دهند.

تشخیص الگوهای مویره در عکس های دیجیتال به عنوان یک موضوع مهم در ارزیابی کیفیت تصویر و وظایف دمویره سازی مطرح می شود. کنگ یانگ و همکارانش، چارچوبی ساده و کارآمد برای استخراج نقشه های لبه مویره از تصاویر دارای الگوهای مویره ارائه دادند. این چارچوب شامل یک استراتژی برای تولید تربل های آموزشی «تصویر طبیعی، لایه مویره، و ترکیب مصنوعی آنها» و شبکه عصبی شناسایی الگوی مویره (MoireDet) برای برآورد نقشه لبه مویره است. طراحی سه رمزگذار در MoireDet به بهره برداری از ویژگی های زمینه ای سطح بالا و ساختاری سطح پایین از الگوهای مختلف مویره می پردازد. از طریق آزمایشات جامع، مزایای MoireDet در دقت شناسایی تصاویر مویره و بهبود چشمگیر نسبت به روش های پیشرفته دمویره سازی نشان داده شده است.

۲- تولید نقشه لبه مویره:

برای نمایش شکل و شدت الگوهای مویره، از نقشه لبه مویره D استفاده می شود. این نقشه ویژگی های هندسی سطح بالای الگوهای مویره را با جزئیات دقیق مانند نوارها، امواج و منحنی ها که به شکل، مکان و شدت اثرات مویره مربوط هستند، حفظ می کند.

۳- استخراج و استفاده از لایه های مویره:

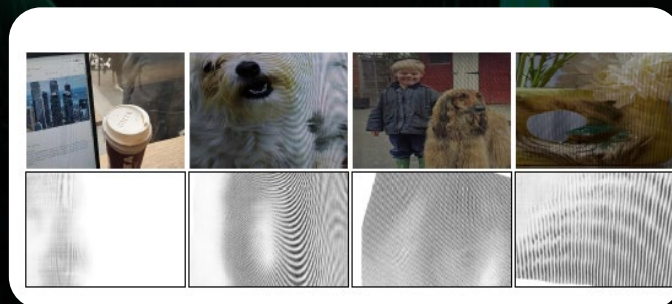
جمع آوری لایه های مویره در دو مرحله انجام می شود:

۱- جمع آوری اختلالات فرکانس بالا با استفاده از صفحه نمایش سفید خالص که کمترین تأثیر را بر تحریف نوارهای دقیق، امواج و منحنی های مؤثر در اثرات مویره دارد.

۲- معرفی اختلالات فرکانس پایین از طریق ضرب پیکسلی پس زمینه و لایه مویره جمع آوری شده.

نتایج

تشخیص الگوهای مویره در عکاسی دیجیتال به دلیل اهمیت آن در عکاسی محاسباتی و بازیابی تصاویر کمتر مورد توجه قرار گرفته است و نیاز به توجه بیشتری دارد. چارچوب پیشنهادی توانسته است با استفاده از تربل های آموزشی با کیفیت بالا و شبکه عصبی MoireDet، دقت و کارایی بالایی در شناسایی و بازیابی



روش پیشنهادی

۱- جمع آوری داده ها و تولید تربل های آموزشی:

برای ارزیابی وظیفه تشخیص الگوی مویره، یک مجموعه داده به نام MoireScape ایجاد شد که شامل تربل های تصویری مصنوعی و جفت های تصویر واقعی است. از سه مدل مختلف گوشی و نمایشگر «در مجموع $3 \times 3 = 9$ ترکیب» برای جمع آوری انواع لایه های مویره استفاده می شود. همچنین ۱۰۰۰ تصویر طبیعی

¼ z K İ ç Ò Z Ô E Ð x - ¾ - Ò Y ç a - ¾ • , Ÿ a
¾ X Ô J x ç š ç - X À i „ ” İ X İ Ð . é z x a š } -
Ö Ô Z İ - Ò Ö ç š a Z ç , Y e - z ú O È ç R , Ÿ Ū f Ö
- Ô J İ Ð J

½ - Ô Y • é z x -

¾ - } z Y - š X İ Ð . š ç z x a š } - z X İ Ö } z J Ó Ç Ū
- Ô J İ Ð J ½ š Y Ú İ š ç ¾ Ū İ f ç š - k İ Ð . a Ú
o X } z Y - z } ¾ | Z Ö ħ • š İ ç ç - ç z x ~ Ò Z Ô E Ð
- x ç Ú “ a z Ø Ô ç Z @ ½ š Y Ú İ š Y ¾ z ” f X }
- £

منابع:

. * * * 9 W F S X F H Y N T S X T S . R F L J 5 W
32, 2023





نحوه ارتباطات مخابراتی بین شهری و درون شهری در ایران

امیرحسین شبرنگ | دانشجوی کارشناسی ارشد مهندسی کامپیوتر - گرایش شبکه‌های کامپیوتری

سمت سیاهکل و یک رشته به سمت لاهیجان هدایت می‌شود؛ از لاهیجان به سمت لنگرود و سپس به رودسر می‌رسد. این کابل‌های نوری پهنای باند بسیار زیاد و زیادی دارند و کابل‌های قطوری هستند که می‌توانند یک شهر چندین هزار نفری یا چندین میلیون نفری را پوشش دهند. پس از اینکه این کابل‌های نوری به شهر می‌رسد، مستقیماً وارد مراکز مخابراتی می‌شود (معمولاً در شهرهای استان گیلان باتوجه به جمعیت و وسعت کم شهرها یک مرکز مخابراتی داریم). کابل فیبر نوری از مراکز مخابراتی به دو دسته تقسیم می‌شود:



۱- ارتباط بین‌شهری بر بستر سیم (برای تلفن‌های ثابت و اینترنت: - FTTH - VDSL - ADSL)

۲- ارتباط رادیویی برای کارهای خاص و تلفن‌های همراه
ارتباط بر بستر سیم

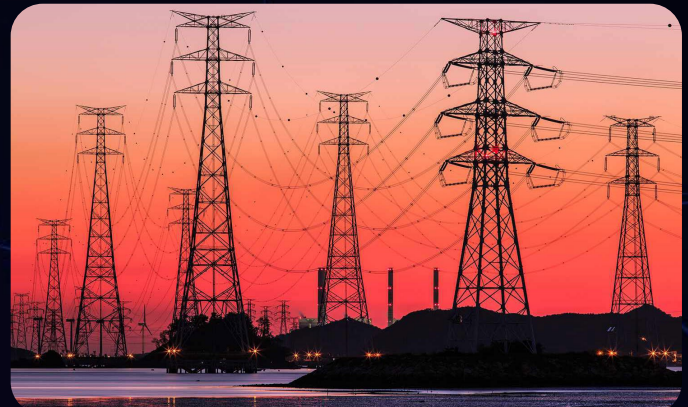
همان‌طور که همه شما می‌دانید، ارتباط بر بستر سیم از مراکز مخابراتی در سرتاسر شهر به مناطق اصلی شهر می‌رسد و تبدیل به یک ایستگاه می‌شود که به آن کافو می‌گویند؛ سپس از آن‌جا مجموعه‌ای از سیم‌ها به سمت ساختمان یا یک مجموعه‌ای هدایت می‌شوند و در ایستگاه خانگی که به آن پُست می‌گویند قرار می‌گیرند و سپس از آن‌جا مستقیماً به سمت واحد مسکونی مورد نظر هدایت می‌شود.

ارتباط رادیویی

اما در مورد ارتباطات رادیویی و تلفنی کمی قضیه متفاوت‌تر است. اپراتورها «همراه اول، ایرانسل، رایتل و...» ابتدا در نقاط شهری دکل‌های BTS خود را نصب

شاید برای شما هم سؤال باشد که ارتباطات مخابراتی در ایران به چه صورت است؟ یا زیرساخت مخابراتی کشور چگونه کار می‌کند؟ ما این بار در گیلانو، می‌خواهیم این مورد را تا حد ممکن بررسی کنیم.

ارتباطات مخابراتی مثل تلفن و اینترنت و...، به این حالت به صورت ترکیبی سیمی و بی‌سیم است؛ اما استفاده از هر تکنولوژی، استاندارد و قوانین خاص خودش را دارد. همان‌طور که می‌دانید، ارتباطات رادیویی در حالت نرمال، هزینه نصب و نگهداری بالاتری به مراتب نسبت به ارتباط بر بستر کابل «فیبر نوری» دارد و ناپایدارتر است. همچنین از نظر پهنای باند، ظرفیت کمتری دارد.



در سرتاسر شهرها و روستاها، دکل‌های موبایلی BTS زیادی نصب شده‌است که شاید ما به آن توجه نمی‌کنیم؛ اما دروازه ارتباطات ما آن‌ها هستند. در نقاط شهری، ما یک یا چند نقطه مخابراتی داریم که باتوجه به ظرفیت‌ها، این تعداد متغیر است. زیرساخت ارتباطی کشور در دست شرکت ارتباطات زیرساخت کشور است، یعنی تمامی اپراتورها باید از زیرساخت شرکت مخابرات استفاده کنند «اجاره‌ای» یا اینکه خودشان تجهیزات خودشان را داشته باشند که این مورد برای آن‌ها بسیار بسیار هزینه‌بر است.

ارتباطات بین‌شهری به این صورت است

ارتباطات بین‌شهری، به‌عنوان مثال شهر رشت تا شهر رودسر بر بستر کابل «فیبر نوری» است که در ابتدا از رشت به سمت آستانه اشرفیه، سپس به سمت لاهیجان این کابل کشیده می‌شود، در مسیر لاهیجان در قسمت بازکیاگوراب تقسیم شده و یک رشته به

بعضی دکل‌ها از طریق فیبر نوری به شبکه متصل می‌شوند و بعضی‌ها از طریق امواج رادیویی، چون:

۱- آلودگی فرکانسی کمتر می‌شود.

۲- شبکه پایدارتر می‌شود.

۳- عمر تجهیزات دکل افزایش پیدا می‌کند.

حتی‌الامکان بهتر است، دکل‌ها از طریق فیبر نوری به شبکه متصل شوند.

گاهی برق قطع می‌شود، مخصوصاً در فصل زمستان و در بعضی مناطق اینترنت قطع می‌شود و در بعضی مناطق خیر و یا اصلاً اینترنت‌های خانگی ممکن است قطع نشود. این مورد یکی از موضوعات بحث‌برانگیز است. این روزها از ما می‌پرسند که دلیلش چیست؟



من از مرکز مخابراتی شروع می‌کنم. باتوجه به اینکه مرکز مخابراتی قلب تپنده ارتباطات شهرستان است، دکل و تجهیزات آن «کافوهای نوری و مسی» به باتری‌های قوی و برق اضطراری مجهز هستند. این باعث می‌شود آن دکل و کافوهای نوری و مسی همیشه روشن بمانند. این یعنی اگر مودم ADSL یا VDSL خودتان را در صورت قطعی برق بتوانید با منبع باتری یا پاوربانک روشن کنید می‌توانید از اینترنت خانگی استفاده کنید.

حالا دکل‌های توزیع‌شده درون شهر هم به برق عادی وصل هستند و هم باتری‌های قوی‌ای را دارا می‌باشند. حتی بعضی از این دکل‌ها هم برق اضطراری دارند. حالا شاید بپرسید که چرا آنتن موبایل قطع می‌شود؟ این‌طور می‌توانم پاسخ دهم که باتری‌های بعضی از دکل‌ها ممکن است آسیب‌دیده باشد یا توسط برخی به سرقت رفته باشد یا حتی سوخته باشد که در این صورت، تمام کلاینت‌هایی که تحت پوشش آن دکل هستند بعد از قطعی برق کم‌کم ارتباطشان با شبکه قطع می‌شود.

در نظر داشته باشید که در راستای منزل شما با فاصله ۴۰۰ متری «فاصله هر دکل با دکل بعدی ۴۰۰ متر است» سه عدد دکل وجود دارد. در حالت عادی، شما

می‌کنند. سپس اگر در آن منطقه‌ای که دکل BTS نصب شده است ایستگاه فیبر نوری قرار داشته باشد، دکل از طریق آن به مرکز مخابراتی وصل می‌شود و سپس به شبکه وصل می‌شود. اگر فیبر نباشد، به صورت رادیویی به مرکز مخابراتی وصل می‌شود؛ تا بتواند به شبکه وصل شود.



پس دکل‌ها از طریق امواج رادیویی با موبایل ما ارتباط برقرار می‌کنند و در صورت وجود فیبر نوری، از طریق فیبر نوری و در صورت عدم وجود فیبر (مثل اطراف و حومه شهر، مناطق جنگلی و... که وجود فیبر نوری در آن مناطق غیرمنطقی است)، از طریق امواج رادیویی به مرکز مخابراتی وصل می‌شود. برای روستاها هم به همین صورت است، در روستاها یا مراکز دهستان‌ها، یک دکل مادر یا همان دکل اصلی که در شهر به آن مرکز مخابراتی گفته می‌شود نصب می‌شود. حال اگر روستا در مسیر فیبر نوری قرار گرفته باشد، دکل اصلی از طریق آن به شبکه متصل می‌شود؛ اگر نه، از طریق امواج رادیویی به نزدیک‌ترین دکل در مرکز مخابراتی شهری که آن روستا یا دهستان زیرمجموعه آن قرار دارد، متصل می‌شود تا از آن طریق به شبکه وصل شود. حالا وقتی دکل اصلی یا از طریق فیبر یا امواج رادیویی به شبکه وصل شد، دکل‌هایی که در روستاهای دوردست‌تر یا اطراف و جنگل و... قرار دارند، باتوجه به اینکه در روستاها و مناطق جنگلی و دوردست فیبر نوری نداریم، این دکل‌ها به دکل اصلی یا مادر آن روستا از طریق امواج رادیویی متصل می‌شوند.

تا اینجا مشکل ارتباطات تلفن همراه حل شد. حالا از همان مرکز مخابراتی روستا که دکل در آن قرار دارد و منشأ و سرچشمه ارتباط است، کابل‌های مسی به سمت منازل مسکونی و تجاری روستانشینان عزیز کشیده می‌شود و این‌گونه روستاها به تکنولوژی اینترنت ADSL مجهز می‌شوند و می‌توانند کیفیت اینترنتی همانند شهرنشینان داشته باشند.

روشن باشد. به جای آن یک دکل نصب شد و چند آنتن که باعث شد کاربرها با هر سیم‌کارتی به آن دکل‌ها متصل شوند. یعنی ۱۰۰ عدد کاربر با سیم‌کارت‌های مختلف به یک دکل وصل می‌شدند به جای آن که ۳ دکل نصب است. از این ۱۰۰ کاربر، ۴۰ کاربر ایرانسل، ۵۰ کاربر همراه اول و ۱۰ کاربر رایتل، که دکل‌های ایرانسل و همراه اول تعداد مشترکین بیشتری در آن منطقه داشت و رایتل ۱۰ مشترک که آن دکل معطل آن ۱۰ کاربر می‌شد و حداکثر استفاده را نداشت. این کار باعث شد دکل و آنتن اضافی روشن نباشد و همه با هر مدل سیم‌کارتی به شبکه متصل شوند و فقط محدودیت اتصال وجود دارد که هر دکل توانایی سرویس‌دهی به ۱۵۰ الی ۲۰۰ مشترک را داراست.

امیدوارم که در این مقاله به درک درستی از ارتباطات رسیده باشید. هر سوالی اگر در این زمینه داشتید می‌توانید از طریق راه‌های ارتباطی نشریه، به مسئولین و سپس به بنده دسترسی پیدا کنید.



به دکل اول متصل هستید و در فاصله کمتر از ۴۰۰ متر از اینترنت 4G استفاده می‌کنید. حال ناگهان برق قطع می‌شود. دکل اول برقی قطع می‌شود. همراه شما به دکل دوم متصل می‌شود که فاصله شما بیشتر از ۴۰۰ متر با آن است مثلاً ۵۰۰ متر. در این صورت، شما از طریق تکنولوژی 3G آنتن‌های آن دکل به اینترنت متصل می‌شوید. پس از مدتی، برق دکل دوم هم می‌رود و شما به دکل سوم که بر فرض ۷۰۰ متر با شما فاصله دارد متصل می‌شوید، اما این بار از طریق تکنولوژی 2G یا E آنتن‌های آن دکل به شبکه یا اینترنت متصل می‌شود که معمولاً در این مرحله آخر فقط قابلیت تماس و پیام کوتاه را خواهید داشت. اما اگر در محدوده شما همان یک عدد دکل باشد کلاً ارتباط شما با شبکه قطع می‌شود.

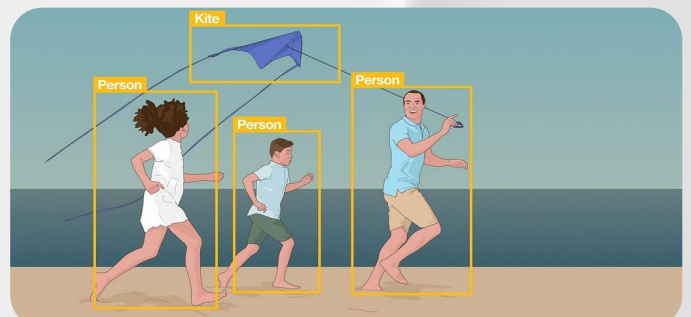
رومینگ

چند سال قبل، ما قابلیتی به نام رومینگ داخلی داشتیم. زمانی که اپراتورها شروع به کار کرده بودند، هر اپراتور باید برای خود دکل خاص خودش را می‌زد. مثلاً در نقطه شیطان‌کوه لاهیجان اگر سه اپراتور ایرانسل و رایتل و همراه اول می‌خواستند به مشترکین‌شان پوشش‌دهی مناسبی ارائه دهند، باید در این نقطه با فاصله اندکی ۳ عدد دکل نصب می‌کردند که این مورد هم برای کشور هزینه‌بر بود و هم آلودگی فرکانسی و بیماری‌های عصبی و مربوطه را به همراه داشت و هم برای اپراتورها هزینه‌بر بود که در اینجا بعضی از اپراتورها دکل را نصب می‌کردند و بعضی‌ها برای جلوگیری از هزینه‌های اضافی و آلودگی فرکانسی دست به استفاده از رومینگ داخلی زدند. یعنی اگر در آن منطقه مثلاً اپراتور رایتل تجهیزات و دکل نداشت، از طریق سرویس رومینگ، از تجهیزات اپراتورهای همکار استفاده می‌کرد که در این مورد هزینه‌های اعتباری آن مشترک کمی نسبت به حالت عادی افزایش می‌یافت. مدتی که گذشت، اپراتورها تصمیم گرفتند حتی‌الامکان از رومینگ داخلی به جهت حفظ ارزش‌های شرکت استفاده نکنند و باز دست به احداث دکل‌های جدید زدند که در اینجا سازمان تنظیم مقررات ورود کرد و از سالی به بعد، تصمیم گرفت پوشش‌دهی و نصب دکل‌ها را بر عهده بگیرد. یعنی به طوری یک واسط شود و اپراتورها تجهیزات خود را روی آن دکل نصب کنند. یعنی مثلاً در نقطه شیطان‌کوه لاهیجان که مثلاً ۱۰۰ مشترک با سیم‌کارت‌های مختلف وجود داشت و باید ۳ عدد دکل با چندین نوع آنتن



مسئله مورد بررسی در مقاله

روش های موجود ردیابی مبتنی بر یادگیری عمیق، نیاز به محاسبات پیچیده و حجم حافظه بالایی دارند و همچنین دوربین های سنتی مورد استفاده، انرژی زیادی مصرف می کنند که این برای اجرا روی دستگاه هایی با توان پایین مانند تلفن همراه و دوربین های نظارتی، غیرکاربردی می باشد. به همین علت Andres Ussa و همکارانش، تحقیقات خود را روی بهبود عملکرد ردیابی اشیاء و دسته بندی آن ها معطوف نمودند.



راهکار پیشنهاد شده

برای حل چالش فوق، محققان یک عملکرد جدید برای ردیابی اشیاء و دسته بندی آن ها به صورت real-time معرفی می کنند که به طور ویژه برای دستگاه های کوچک کم توان که منابع محدودی دارند، طراحی شده است. این فریم ورک جدید، hybrid neuromorphic نام دارد و از دوربین های رویدادمحور یعنی مبتنی بر تغییرات پیکسل های تصویر استفاده می کند که می توانند جزئیات را حتی در محیط های خیلی تاریک یا خیلی روشن نیز ضبط کنند.

در رویکرد پیشنهادی، به جای پردازش تغییرات تصویر به صورت پیکسل به پیکسل، تغییرات در سطح هر پیکسل با فریم هایی ترکیب گشته و با کمک چگالی و سرعت پیکسل های متحرک در هر فریم، تا هشت شیء مختلف به طور همزمان ردیابی می گردد.

اطلاعات اشیاء ردیابی شده، به پالس های الکتریکی به نام Spike تبدیل شده و به عنوان ورودی به تراشه TrueNorth Neuromorphic که ساخت کمپانی IBM می باشد، داده می شوند تا با استفاده از مدل های Spik-ing neural network مانند الگوریتم Energy efficient

deep network پردازش و دسته بندی شوند.

در نهایت متد پیشنهادی، روی یک پردازنده FPGA پیاده سازی می گردد و با جدیدترین تکنیک های ردیابی و دسته بندی اشیاء مبتنی بر فریم و مبتنی بر Event «تغییرات پیکسل ها» مقایسه می شود.

بلوک دیاگرام سیستم بلادرنگ hybrid neuromorphic

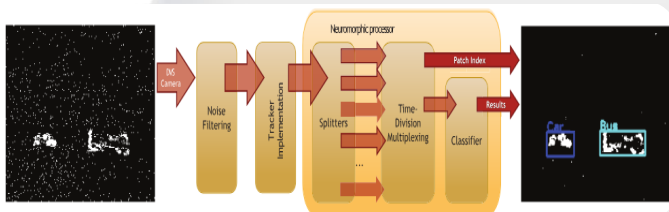
۱- تشخیص حرکات در ویدیو

۲- ردیابی اجسام متحرک بر اساس همپوشانی آن ها با فریم های قبلی

۳- تبدیل اشیاء ردیابی شده به پالس های الکتریکی Spike با استفاده از مدل پواسون

۴- پردازش Spike ها

۵- طبقه بندی اشیاء



ردیابی اشیاء (EOT)

متد ردیابی EOT اطلاعات دریافتی جدید از طریق دوربین های مبتنی بر تغییرات در شدت یا نور پیکسل ها را به یک سری باکس های مستطیلی به نام track اختصاص می دهد که این کار به ردیاب اجازه می دهد تا چندین شیء متمایز را به طور همزمان دنبال کند.

ردیابی از طریق این متد ۳ مرحله دارد:

۱- در مرحله اول، ردیاب داده های ورودی از تغییرات پیکسل ها را دریافت کرده و تصمیم می گیرد که این داده ها را به track هایی که از قبل برای اشیاء وجود داشتند ارجاع دهد یا یک track جدید با ID منحصر به فرد برای آن ها تولید کند. شیوه عملکرد آن به این صورت است که وقتی یک شیء متحرک جدید ظاهر شود، ردیاب چک می کند که داده های ورودی تا چه حدی با track های ثبت شده از اشیایی که قبلاً

آزمایش و مقایسه

نمونه‌ها پس از پیش‌پردازش اولیه، برای train شدن به تراشه TrueNorth منتقل می‌شوند.

۷۵ درصد داده‌ها به‌عنوان داده‌های آموزشی و ۲۵ درصد داده‌ها به‌عنوان داده‌های تست انتخاب می‌شوند.

مقایسه عملکرد جدیدترین روش‌های موجود ردیابی اشیاء با متد EOT روی مجموعه داده‌های جمع‌آوری شده، نشان داد این متد رویکرد بهتر و دقت و صحت بالاتری نسبت به سایر روش‌ها دارد.

نتایج کلیدی

- ۱- نیازمندی رویکرد EOT به ۷ برابر حافظه کمتر برای ذخیره‌سازی اطلاعات و کاهش حجم محاسبات تا ۳ برابر نسبت به متدهای دیگر.
- ۲- دسته‌بندی درست داده‌ها با استفاده از تراشه EEDN.
- ۳- عملکرد بهتر در ردیابی همزمان اشیاء نسبت به الگوریتم استاندارد طبقه‌بندی.

تشخیص داده شده بودند، همپوشانی دارند. اگر میزان همپوشانی زیاد بود، یعنی هر دو مربوط به یک شیء واحد می‌باشند و پیکسل‌ها به آن track اختصاص داده می‌شوند؛ ولی اگر میزان همپوشانی آن‌ها کم باشد، یعنی ورودی ما نمایانگر یک شیء جدید است و در این حالت یک track جدید برای آن ساخته می‌شود که اطلاعاتی مثل موقعیت، اندازه و سرعت آن دسته از پیکسل‌ها را به‌عنوان مقدار اولیه می‌گیرد.

۲- در مرحله دوم، داده‌های ورودی ادغام یا جدا می‌شوند. به‌طورمثال وقتی داده‌های مختلف ورودی به یک track واحد اشاره کنند، یعنی نماینده یک شیء خاص هستند و این مکانیزم، آن‌ها را با هم ادغام می‌کند؛ یا اگر داده ورودی نمایانگر چند track متفاوت باشد، به اشیاء متفاوتی اشاره دارد که از طریق متد EOT از هم جدا می‌شوند.

در این مرحله نیز، Track هایی که دیگر با هیچ یک از داده‌های ورودی مطابقت ندارند حذف می‌گردند.

Continuous-Time EOT یک رویکرد جایگزین برای Regular EOT است که به‌طور Real-time ورودی‌های جدید را تک‌به‌تک پردازش می‌کند که این کار باعث افزایش بهره‌وری و بهبود دقت دوربین‌های رویدادمحور در ردیابی اشیاء با سرعت بالا و حرکات سریع می‌شود.

فواید

۱- با سنجش مداوم داده‌ها، ردیاب می‌تواند سریع‌تر به تغییرات واکنش نشان دهد و اطلاعات دقیق‌تری در مورد مکان و اندازه اشیاء ارائه کند.

۲- با پردازش داده‌ها به‌محض ورود، می‌توان تأخیر بین زمانی که تغییری در صحنه اتفاق افتاده است و زمانی که ردیاب آن تغییر را منعکس می‌کند، را کاهش داد.

چالش‌ها

افزایش پیچیدگی محاسباتی، افزایش هزینه و نیاز به الگوریتم‌های پیچیده‌تر برای تشخیص درست اشیاء، از جمله چالش‌های این رویکرد هستند.

جمع‌آوری داده

محقق‌ها برای جمع‌آوری داده‌های مورد نیاز، سه مکان مختلف در محوطه دانشگاه خود را انتخاب کردند.

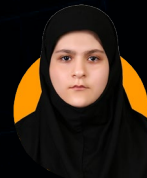
برای تولید یک فریم، داده‌ها را هر ۶۶ میلی‌ثانیه از محیط جمع‌آوری نمودند.

منابع:

Ussa, A., Rajen, C. S., Pulluri, T., Singla, D., 1- Ramesh, B. & ... Acharya, J., Chuanrong, G. F (2023). A hybrid neuromorphic object tracking and classification framework for real-time systems. IEEE Transactions on Neural Networks and Learning Systems

<https://doi.org/10.1109/tnn-2-ls.2023.3243679>





پیش بینی بارندگی مناطق هند با شبکه RfGanNet

آیدا ملکی چوکامی | دانشجوی کارشناسی ارشد مهندسی کامپیوتر - گرایش هوش مصنوعی

مدل‌های پیشنهادی RfNet و RfGAN

مدل پیشنهادی در دو بخش ارائه شده است:

۱- RfGAN یک شبکه مولد متخاصم جدید برای افزایش داده‌ها معرفی شده است که می‌تواند داده‌های مصنوعی را زیاد کند.

۲- RfNet: یک روش جدید مبتنی بر یادگیری عمیق برای پیش‌بینی بارش در هند معرفی شده است.

مدل RfNet ترکیبی از LSTM دوطرفه، LSTM و CNN برای پیش‌بینی بارندگی است. LSTM برای حفظ بهتر اطلاعات استفاده می‌شود و LSTM دوطرفه برای درک بهتر دنباله‌های سری زمانی استفاده می‌شود. CNN روابط بین ورودی‌ها و خروجی‌ها را تحلیل می‌کند. همچنین از لایه و تکنیک Dropout برای جلوگیری از بیش‌برازش (Overfitting) استفاده شده است.

مدل RfGanNet و عملکرد آن

از ترکیب دو مدل ارائه شده، به مدل RfGanNet رسیدند که نتایج تجربی نشان می‌دهد، مدل پیشنهادی RfNet، هنگامی که با داده‌های تولیدشده توسط RfGAN آموزش دیده‌است، به دقت ۹۷/۲۲ درصد دست یافته و از سایر روش‌ها عملکرد بهتری ارائه داده‌است. همان‌طور که در شکل زیر مشاهده می‌کنید، RfGAN برای افزایش اندازه داده‌های آموزشی و بهبود کارایی آموزش مدل پیشنهادی ما یعنی مدل RfGanNet استفاده می‌شود. خطوط آبی که داده‌های واقعی را نشان می‌دهند بسیار نزدیک به خطوط نارنجی که داده‌های مصنوعی را نشان می‌دهند، هستند. این بدین معناست که مدل به‌درستی آموزش دیده‌است.

یکی از چالش‌های اصلی پیش‌بینی بارندگی، کمبود داده‌های واقعی و معتبر است که برای آموزش مدل‌های پیش‌بینی ضروری هستند. برای رفع این مشکل، می‌توان از شبکه‌های مولد متخاصمی (GAN) استفاده کرد که قادر به تولید داده‌های مصنوعی مشابه داده‌های واقعی هستند. شبکه‌های مولد متخاصمی یا GAN، به عنوان یک مدل یادگیری عمیق در دسته‌بندی یادگیری بدون ناظر (Unsupervised Learning) قرار می‌گیرند. ورودی داده‌ها به صورت برچسب‌خورده نیستند و مولد تنها از داده‌های واقعی استفاده می‌کند تا داده‌های مصنوعی مشابهی تولید کند. در واقع، یادگیری در این شبکه‌ها توسط مولد و متمایزکننده به وقوع می‌پیوندد؛ به این صورت که مولد سعی در تولید داده‌های جدید شبیه به داده‌های واقعی می‌کند و متمایزکننده تلاش می‌کند تا هر نمونه تولید شده توسط مولد را به‌درستی شناسایی و تمییز نماید. این کار تا زمانی که داده‌های تولید شده به تدریج واقعی‌تر شوند و به یک حالت پایدار همگرا شوند ادامه خواهد داشت. این شبکه برای داده‌های سری زمانی مانند بارش باران مناسب خواهد بود.

پیش‌پردازش داده‌ها

بنسال و همکاران، داده‌های ۳۶ منطقه از هند را جمع‌آوری کردند. برای پیش‌پردازش، جایگزینی داده‌های نامعتبر و تبدیل متغیرها به فرمت دسته انجام شد. همچنین داده‌های ساعتی به ماهانه تبدیل شدند و با روش آرنج (Elbow) مناطق هند را به پنج خوشه تقسیم کردند که در شکل زیر مشاهده می‌کنید:

Table 2
Cluster wise regional classification.

Cluster	Regions
1	West Uttar Pradesh, Haryana, Delhi, Chandigarh, Punjab, Jammu and Kashmir, West Rajasthan, Saurashtra and Kutchh, Rayalseema region, North Interior Karnataka, Tamil Nadu
2	Bihar, East Uttar Pradesh, Gujarat, East Rajasthan, Himachal Pradesh, Central Maharashtra, Marathwada, Coastal Andhra Pradesh, Telangana, South Interior Karnataka
3	Lakshadweep, Nagaland, Manipur, Mizoram, Tripura, Gangetic West Bengal, Orissa, Jharkhand, Uttarakhnad, Madhya Pradesh, Vidarbha, Chhatisgarh
4	Assam, Meghalya, Sub Himalayan West Bengal and Sikkim, Andaman and Nicobar Islands, Arunachal Pradesh, Kerala
5	Konkan and Goa, Coastal Karnataka

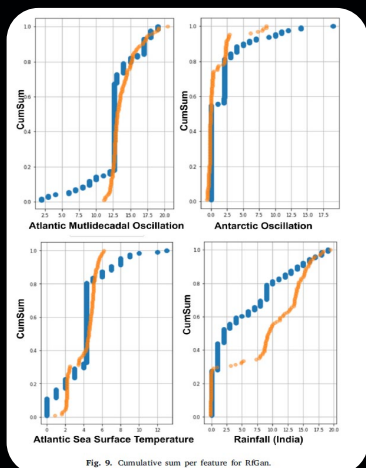
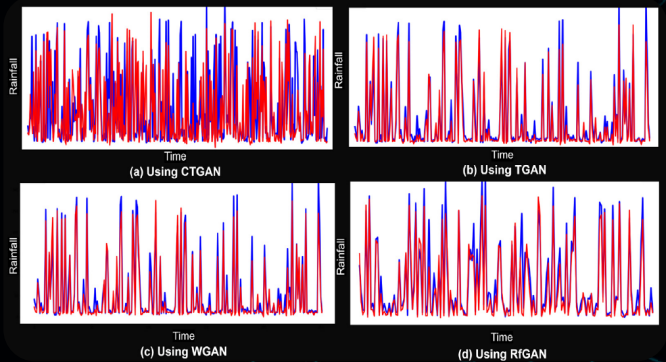


Fig. 9. Cumulative sum per feature for RfGan.

همچنین مدل پیشنهادی RfGAN، که از ویژگی‌های باقی‌مانده برای بهبود کیفیت داده‌های تولیدشده و تمرکز بر داده‌های سری زمانی استفاده می‌کند، در مقایسه با سه مدل دیگر (CTGAN که برای داده‌های جدولی شرطی طراحی شده، TGAN که داده‌های جدولی پیچیده بهینه‌سازی شده، و WGAN که از فاصله Wasserstein برای پایداری بیشتر استفاده می‌کند) عملکرد بهتری از خود نشان داده است. نتایج تجربی نشان می‌دهد که RfGAN توانسته است داده‌های مصنوعی با کیفیت بالاتری تولید کند و دقت مدل RfNet را بهبود بخشد.



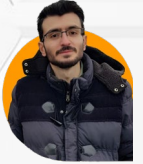
منابع:

1-Kamakhya Bansal, Ashish Kumar Tripathi, Avinash Chandra Pandey, Vivek Sharma

2-RfGanNet: An efficient rainfall prediction method for India and its clustered regions using RfGan and deep convolutional neural networks

3-<https://doi.org/10.1016/j.eswa.2023.121191>





استرس چیست؟

استرس یک حالت روانی است که هر فردی در زندگی روزمره خود آن را تجربه می‌کند. این یک مکانیسم نجات بدن در دوره‌های بحرانی است. با این حال، پس از فراتر رفتن از یک سطح خاص، استرس دیگر سالم نیست. برعکس، شروع به آسیب رساندن به سلامت، وضعیت عاطفی، بهره‌وری و کیفیت زندگی فرد می‌کند. اگر فرد به شدت استرس داشته باشد، این می‌تواند باعث مشکلات جدی سلامتی شود.



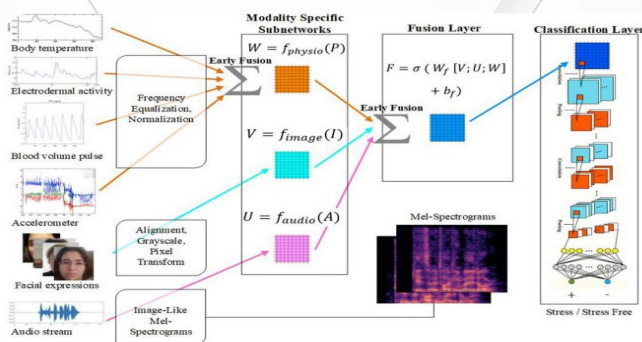
مسئله‌ی مورد بحث در مقاله

استرس روانی، یک عامل خطر مهم برای چندین بیماری است و می‌تواند بر کیفیت زندگی افراد از جمله کار و روابط شخصی آن‌ها تأثیر منفی بگذارد. روش‌های سنتی تشخیص استرس روانی از طریق مصاحبه و پرسشنامه ممکن است پاسخ‌های هیجانی آنی افراد را دریافت نکنند. در این مطالعه، از روش نمونه‌گیری تجربه برای تحلیل پاسخ‌های عاطفی شرکت‌کنندگان استفاده شد که درک جامع‌تر و پویاتری از تجربیات شرکت‌کنندگان ارائه می‌دهد. مجموعه داده Work-Stress3D با استفاده از اطلاعات جمع‌آوری شده از ۲۰ شرکت‌کننده برای سه روش مجزا گردآوری شد. به طور متوسط در طول یک هفته، ۱۷۵ ساعت داده‌های حاوی سیگنال‌های فیزیولوژیکی مانند BVP، EDA و دمای بدن و همچنین حالات چهره و داده‌های شنوایی از یک فرد جمع‌آوری شد. ما یک مدل همجوشی جدید ارائه می‌کنیم که از روش‌های همجوشی دوگانه اولیه برای ترکیب داده‌ها، از روش‌های متعدد استفاده می‌کند. امتیاز F1 مدل ۰/۹۴ با از دست دادن ۰/۱۸ بسیار دلگرم‌کننده است و نشان می‌دهد که می‌تواند به طور دقیق درجات مختلف استرس را شناسایی و طبقه‌بندی کند. علاوه بر این، ما استفاده از تکنیک‌های یادگیری انتقال را برای بهبود کارایی سیستم تشخیص استرس خود بررسی می‌کنیم. علی‌رغم تلاش‌هایمان، نتوانستیم به نتایج بهتری نسبت به مدل فیوژن دست یابیم. یادگیری انتقالی منجر به دقت ۰/۹۳ و از دست دادن ۰/۱۷ شد که دشواری انطباق مدل‌های از پیش

آموزش‌دیده را با کار تحلیل استرس نشان می‌دهد. نتایج به دست آمده بر اهمیت همجوشی چندوجهی در تشخیص تنش و اهمیت انتخاب مناسب‌ترین معماری مدل برای کار داده‌شده تأکید می‌کند. مدل همجوشی پیشنهادی، پتانسیل خود را برای دستیابی به طبقه‌بندی دقیق و قوی تنش نشان می‌دهد. این تحقیق به زمینه تحلیل استرس کمک می‌کند و به توسعه مدل‌های موثر برای تشخیص استرس کمک می‌کند.

راهکار پیشنهاد شده

در این تحقیق، ما یک استراتژی جامع برای تشخیص استرس با ادغام چند روش با استفاده از معماری‌های یادگیری عمیق پیشنهاد می‌کنیم. در رویکرد ما، فعالیت الکترودرمال، فشار حجم خون، دمای پوست، شتاب‌سنج، گفتار و حالات چهره به عنوان مدالیته در نظر گرفته می‌شوند. هر مدالیته تحت یک روش پیش‌پردازش دقیق قرار می‌گیرد تا کیفیت و قابلیت اطمینان داده‌ها را تضمین کند. همجوشی اولیه در دو مرحله در طول فرآیند همجوشی رخ می‌دهد. اول، روش‌های بیوسگنال (TEMP، BVP، EDA) و ACC ترکیب می‌شوند تا دینامیک زمانی سیگنال‌های فیزیولوژیکی پاسخ‌دهنده به استرس را به تصویر بکشند. سپس روش بیوسگنال ترکیبی با حالات چهره و امواج صوتی ترکیب می‌شود تا تصویری جامع از سطوح استرس ایجاد شود. این ساختارهای همجوشی تشخیص دقیق و قابل‌اعتماد تنش را با گرفتن و تفسیر اطلاعات مربوط از روش‌های مختلف تسهیل می‌کنند. شکل زیر معماری و رویه سیستم تشخیص تنش چندوجهی ما را نشان می‌دهد و تکنیک‌های مورد استفاده در این تحقیق را نشان می‌دهد.



مراحل تشخیص استرس

بخش نتایج تجربی این مطالعه پاسخ‌های احساسی را با تجزیه و تحلیل سیگنال‌های زیستی جمع‌آوری شده از حسگرهای متعدد و همچنین تصاویر و سیگنال‌های صوتی به دست آمده از طریق برنامه تلفن همراه بررسی می‌کند. با استفاده از فهرست جامعی از هفت برچسب احساسی، داده‌های ویدیویی و صوتی به صورت روشی تجزیه و تحلیل شدند تا طیف وسیعی از حالات احساسی را به تصویر بکشند. احساسات مثبت برای نماد موقعیت‌های بدون استرس، در حالی که احساسات منفی برای نشان دادن موقعیت‌های استرس‌زا استفاده می‌شوند. به منظور ایجاد یک مجموعه داده برچسب‌دار برای پیش‌بینی استرس، پاسخ‌های نظرسنجی آزمایشی هفت‌روزه شرکت‌کنندگان در نظر گرفته شد. پاسخ‌های نظرسنجی به عنوان منبع ارزشمندی برای تشخیص تظاهرات احساسی مرتبط با استرس از سیگنال‌های فیزیولوژیکی عمل کردند. به طور خاص، عبارات عاطفی مثبت به عنوان «بدون استرس»، به معنای بهزیستی عاطفی، برچسب‌گذاری شدند، در حالی که عبارات هیجانی منفی به عنوان «استرس‌زا» برچسب‌گذاری شدند، که مواردی از استرس بالا را نشان می‌دهد. این مطالعه به دنبال ایجاد درک جامعی از رابطه بین پاسخ‌های هیجانی و سطوح استرس با برچسب‌گذاری دقیق و طبقه‌بندی عبارات احساسی گرفته شده از داده‌های جمع‌آوری شده است. در تمام آزمایش‌ها، مجموعه داده‌ها به ترتیب به مجموعه‌های آموزشی و آزمایشی ۸۰ درصد و ۲۰ درصد تقسیم شدند. این تحلیل، مبنایی را برای ارزیابی بعدی و ارزیابی عملکرد مدل همجوشی چندوجهی عمیق پیشنهادی فراهم می‌کند.

آزمایشات:

مجموعه داده WorkStress3D با ترکیب داده‌ها از منابع متعدد برای استفاده از مزایای روش‌های متعدد و افزایش درک حالات احساسی شرکت‌کنندگان ایجاد شد. با ادغام و استخراج اطلاعات مناسب، هدف مجموعه داده تلفیقی، بهبود عملکرد داده‌ها و دقت طبقه‌بندی بود. برای تولید مجموعه داده ادغام نهایی، تکرارهای چندگانه ادغام، کاهش و ادغام داده‌ها مورد نیاز بود.

۱- پیش‌پردازش داده‌های بصری: (2048x1152) پیکسل اصلی و رنگ‌های RGB در پیش‌پردازش تصاویر جمع‌آوری شده حالات صورت، از بین رفتند. لازم بود

حالت واقعی صورت از پس‌زمینه جدا شود تا استخراج ویژگی و پردازش تصویر بعدی تسهیل شود. این کار از طریق تراز کردن چهره، نرمال‌سازی و تقویت صورت انجام شد. علاوه بر این، همه عکس‌ها به پایین‌ترین وضوح ممکن برای مطالعه کوچک شدند.

۲- پیش‌پردازش سیگنال صوتی: ویژگی‌های طیف سیگنال‌های صوتی جمع‌آوری شده مورد بررسی قرار گرفت. با استفاده از یک مقیاس دودویی، طیف‌های توان را استخراج کردیم و کشف کردیم که طیف‌های mel مهم‌ترین جزئیات شنوایی را ضبط می‌کنند. پس از این مراحل، داده‌های صوتی با دقت بیشتری نشان داده شدند که تجزیه و تحلیل و ادغام بیشتر را تسهیل کرد.

۳- پیش‌پردازش سیگنال فیزیولوژیکی: سیگنال‌های فیزیولوژیکی شرکت‌کنندگان در فرکانس‌های مختلف با استفاده از دستگاه حسگر Empatica E4 که مچ‌پوشیده شده بود نمونه‌برداری شد. برای حل این مشکل، از تکنیک نمونه‌برداری پایین برای یکنواخت‌تر کردن فرکانس سیگنال‌ها استفاده شد. نمونه‌برداری پایین برای دستیابی به تعادل بین راندمان محاسباتی و دقت انتخاب شد. با نمونه‌برداری از تمام ورودی‌های فیزیولوژیکی به ۴ هرتز، سازگاری و همجوشی مؤثر به دست آمد.

۴- تبدیل ویژگی: ویژگی‌های درجه دوم، تحت تبدیل ویژگی‌های چندجمله‌ای قرار گرفتند تا همبستگی‌های مرتبه بالاتر را به دست آورند و نمایش سیگنال‌های فیزیولوژیکی را افزایش دهند. با ادغام داده‌های خام سیگنال‌های فیزیولوژیکی، ویژگی‌های اضافی تولید شد. هدف این بود که پاسخ‌های فیزیولوژیکی شرکت‌کنندگان و تعاملات غیرخطی را با دقت بیشتری به تصویر بکشیم.

نتایج کلیدی

هدف این تحقیق بررسی امکان‌سنجی مدل‌سازی استرس فردی با ادغام اطلاعات از منابع متعدد «حالت‌های چهره، گفتار و سیگنال‌های زیستی» در یک مدل واحد با استفاده از همجوشی اولیه بود. این تحقیق منجر به اکتشافات و اضافات مهمی در رشته تحلیل استرس شده است. در وهله اول، ما ساختار همجوشی چندمدلی را ارزیابی کردیم و متوجه شدیم که ادغام حالات چهره، گفتار و سیگنال‌های زیستی با هم،

منابع:

1-Dogan, G., & Akbulut, F. P. (2023). Multi-modal fusion learning through biosignal, audio, and visual content for detection of mental stress. *Neural Computing and Applications*, 35(34), 24435–24454

2-<https://doi.org/10.1007/s00521-023-09036-4>



عملکرد طبقه‌بندی استرس را در استفاده از هر روش به‌تنهایی افزایش می‌دهد. مدل همجوشی پیشنهادی، دقت قابل‌توجه خود را در تشخیص و طبقه‌بندی سطوح تنش، با امتیاز $F1 = 0.94$ و تلفات کم 0.18 نشان می‌دهد که از نتایج روش‌های منفرد فراتر می‌رود. طبقه‌بندی تنش‌ها به‌طور دقیق همچنین مستلزم انتخاب بازه زمانی مناسب در داده‌های متوالی است. ما متوجه شدیم که یک پنجره زمانی 30 ثانیه‌ای موثرترین بوده و پس از آن پنجره‌های 15 و 60 ثانیه‌ای قرار دارند. با توجه به این نتایج، به نظر می‌رسد مدت‌زمان پنجره زمانی متوسط، نقطه شیرینی برای ثبت الگوهای فیزیولوژیکی و رفتاری ضروری است و درعین‌حال از فقدان اطلاعات زمانی حیاتی جلوگیری می‌کند. تحقیق پیشنهادی بر ارتباط در نظر گرفتن منابع داده‌های متعدد و اندازه فریم ایده‌آل، و همچنین اثربخشی یک استراتژی همجوشی چند مدل و غیره تأکید می‌کند. علاوه بر مدل همجوشی، ما یک آزمایش پیش‌بینی استرس را با استفاده از یادگیری انتقال انجام دادیم، اما با وجود استفاده از تکنیک‌های یادگیری انتقال، نتوانستیم از عملکرد مدل همجوشی در تشخیص استرس پیشی بگیریم. با این وجود ما امتیاز باخت را 0.01 امتیاز کاهش داده‌ایم. یادگیری انتقالی دقت 0.93 و از دست دادن 0.17 را به‌همراه داشت که نسبت به نتایج قابل‌توجه مدل تلفیقی پایین‌تر بود. اگرچه نشان داده شده‌است که یادگیری انتقال در حوزه‌های متعددی مؤثر است، به نظر می‌رسد که تحلیل استرس نیاز به رویکرد تخصصی‌تری دارد. با وجود این، نتایج به‌دست‌آمده سطح بالایی از دقت را نشان می‌دهد و بر اهمیت انتخاب مناسب‌ترین معماری مدل برای یک کار معین تأکید می‌کند. برای کشف استراتژی‌های جایگزین و به‌طور بالقوه بر اساس این یافته‌ها، تحقیقات و اصلاحات اضافی لازم است. این نتایج به دانش روبه‌رشد در مورد تجزیه و تحلیل استرس اضافه می‌کند و سرنخ‌هایی را برای بهبود برنامه‌های تشخیص استرس موجود ارائه می‌دهد (Dogan & Akbulut, 2023).

گیلانو

📍 SCC_LIAU

✉ scc.liau@gmail.com

گیلانو نشریه‌ای دانشجویی در زمینه علمی تخصصی با صاحب امتیازی انجمن علمی مهندسی کامپیوتر دانشگاه آزاد اسلامی واحد لاهیجان است که با ترتیب انتشار ماهنامه منتشر می‌گردد.

گیلانو از اردیبهشت ۱۴۰۰ شروع به فعالیت کرد و در آن به موضوعات مرتبط با تمام گرایش‌های مهندسی کامپیوتر نظیر هوش مصنوعی، رباتیک، نرم افزار، سخت افزار، شبکه و موضوعات بین رشته‌ای پرداخته می‌شود.