



دانشگاه صنعتی شریف

دانشکده مهندسی برق

پایان نامه کارشناسی ارشد

گرایش مخابرات

مدلسازی نهان نگاری تصویر بر اساس تئوری اطلاعات

نگارنده

ابوالفضل یاریان

استاد راهنما

دکتر مسعود بابائی زاده

شهریورماه ۱۳۸۴

این پروژه تحت قرارداد پژوهشی شماره مورخ از پشتیبانی مادی و معنوی مرکز تحقیقات مخابرات ایران بهره‌مند شده

است.

توجه

این پروژه بر اساس قرارداد شماره (.....) از حمایت مالی
مرکز تحقیقات مخابرات ایران برخوردار شده است.

بسمه تعالی

دانشگاه صنعتی شریف
دانشکده مهندسی برق

پایان نامه کارشناسی ارشد

عنوان: مدلسازی نهان نگاری تصویر بر اساس تئوری اطلاعات

نگارش: «نام و نام خانوادگی دانشجو»

اعضا هیات داوران:

.....امضاء:	دکتر ...
.....امضاء:	دکتر ...
.....امضاء:	دکتر ...
.....امضاء:	دکتر ...
.....امضاء:	دکتر ...

تاریخ: ۶ شهریور ۱۳۸۴.

تقدیم و قدردانی

در این صفحه از کسانی که مایلید تشکر می‌کنید.

چکیده:

در دنیای دیجیتال امروزه، نهان نگاری مقاوم تصویر که در آن یک سیگنال حامل داده به صورت نامرئی و مقاوم در برابر حملات در تصویر تعبیه می‌شود، به عنوان یک راهکار برای حل مساله حفاظت از حق تالیف محصولات تصویری معرفی شده است. برای این منظور تاکنون جهت نهان نگاری روشهای متعددی به کار گرفته شده است که از آن جمله می‌توان به استفاده از مدل‌های بینایی جهت یافتن میزان بیشینه انرژی نهان نگاره برای تعبیه در تصویر و استفاده از حوزه های مقاوم در برابر حملات، اشاره نمود. در همین راستا در این پایان نامه به استفاده از مفاهیم حوزه تئوری اطلاعات به عنوان یک راهنما در توسعه الگوریتم‌های موجود، جهت قرار دادن بهینه نهان نگاره پرداخته شده است. همچنین در ساختار پیشنهادی که برای افزایش مقاومت در حوزه تبدیل تصویر پیاده می‌شود، از تبدیلات چنددقتی مانند تبدیل موجک گسسته و تبدیل MR-SVD که به سیستم بینایی انسان نزدیک‌ترند، استفاده می‌شود. به طوریکه در حوزه تبدیل موجک، با استفاده از آنتروپی و تاثیر پدیده پوشش آنتروپی به اصلاح مدل‌های بینایی مرتبط با این حوزه پرداخته و بدین ترتیب نهان نگاره با قدرت و مقاومت بالاتر در تصویر تعبیه نموده و همچنین کیفیت بهتر برای تصویر نهان نگاری شده بدست آمد. همچنین در حوزه تبدیل MR-SVD ابتدا این تبدیل که تاکنون برای نهان نگاری استفاده نشده بود، جهت نهان نگاری بکار گرفته شد و سپس مشابه ساختار پیشنهادی مبتنی بر آنتروپی در حوزه تبدیل موجک، در حوزه این تبدیل نیز بکار رفت و نتایج شبیه‌سازیها مقاوم‌تر بودن ساختار پیشنهادی و کیفیت بالاتر تصویر نهان نگاری شده در این حوزه را نتیجه داد.

کلمات کلیدی:

- | | |
|-----------------------|------------------------------------|
| ۱- نهان نگاری تصویر | Image Watermarking |
| ۲- تبدیل چنددقتی | Multi-Resolution Transform |
| ۳- سیستم بینایی انسان | Human Visual System (HVS) |
| ۴- تبدیل موجک | Wavelet Transform |
| ۵- تجزیه مقادیر تکین | Singular Value Decomposition (SVD) |
| ۶- آنتروپی | Entropy |
| ۷- پوشش آنتروپی | Entropy Masking |

فهرست مطالب

۱	مقدمه	۱
۲	مرور مفاهیم پایه	۲
۲	۱-۲ DevOps	۲
۲	۱-۱-۲ تعریف	۲
۳	۲-۱-۲ چرخه کاری DevOps	۳
۴	۳-۱-۲ خط لوله CI/CD	۴
۷	۴-۱-۲ مزایای متدولوژی DevOps	۷
۹	۲-۲ مجازی سازی و کانتینر سازی	۹
۹	۱-۲-۲ مجازی سازی	۹
۱۱	۲-۲-۲ کانتینر سازی	۱۱
۱۴	۳ مدل بینایی انسان و کاربرد آن در نهان نگاری	۱۴
۱۴	۱-۳ مقدمه	۱۴
۱۵	۴ آنتروپی و استفاده از آن در نهان نگاری	۱۵
۱۵	۱-۴ مقدمه	۱۵
۱۵	۲-۴ آنتروپی	۱۵
۱۶	۵ نتیجه گیری و پیشنهادات	۱۶

فهرست جداول

۱-۲	نمونه هایی از ابزار برای مراحل خاص اتوماسیون خط لوله CI/CD	۵
-----	--	---

فهرست تصاویر

۴ مراحل DevOps	۱-۲
۱۰ انواع هایپروایزر [۳]	۲-۲
۱۱ تفاوت ماشین مجازی و کانتینر	۳-۲
۱۳ معماری لایه ای تصویر داکر	۴-۲

فهرست کلمات اختصاری

2D-DWT	2-Dimensional Discrete Wavelet Transform
CPD	Cycle Per Degree
CSF	Contrast Sensitivity Function
⋮	⋮

فصل ۱

مقدمه

گسترش روز افزون شبکه جهانی اینترنت و توسعه فناوری اطلاعات، نیاز فزاینده‌ای را به استفاده از سرویسهای چندرسانه‌ای دیجیتال، در پی داشته به طوریکه کاربردهای دیجیتال شاهد رشد شگرفی در طول دهه گذشته بوده است که نتیجه آن ایجاد سیستمهای کارآمد در ذخیره، انتقال و بازیابی اطلاعات است. مزایای فراوان فناوری دیجیتال، باعث محبوبیت و کاربرد هر چه بیشتر آن توسط اشخاص شده تا جاییکه حتی وسایل ضبط و پخش صدا و تصویر آنالوگ خانگی هم به سرعت با نمونه‌های دیجیتال جایگزین شده‌اند. اما این موضوع مسائل حاشیه‌ای دیگری برای بشر ایجاد نموده است. به طوریکه امکان تهیه کپی‌های متعدد از روی نسخه اصلی بدون کاهش کیفیت آن و یا سادگی جعل و تغییر محتوای اطلاعاتی نسخه اصلی، باعث شده که مالکیت معنوی^۱ صاحبان اثر به خطر افتاده و در نتیجه بسیاری از ارائه دهندگان سرویسهای چندرسانه‌ای (از جمله شرکتهای فیلم‌سازی) از ارائه نمونه دیجیتال محصولاتشان خودداری نمایند. لذا برطرف نمودن این مشکلات، یکی از زمینه‌های پژوهشی مهم در عرصه مخابرات و بخصوص پردازش سیگنال است.

فصل ۲

مرور مفاهیم پایه

۱-۲ DevOps

۱-۱-۲ تعریف

دِوایس که از اتحاد واژگان Development و Operation به وجود آمده است؛ ترکیبی از ابزارها، کنش‌ها و فرهنگ کاری است که تیم‌های توسعه^۱ و عملیات^۲ را به همکاری موثرتر نزدیک می‌کند و کسب و کارها با استفاده از می‌توانند اپلیکیشن‌ها و سرویس‌هایشان را با سرعت بالاتری نسبت به روش‌های سنتی تحویل دهند. همین سریع‌تر شدن سرعت توسعه و انتشار نرم‌افزار، سازمان‌ها را قادر می‌سازد تا در مقایسه با کسب‌وکارهایی که هنوز از روش‌های سنتی توسعه نرم‌افزار استفاده می‌کنند خدمات بهتری به مشتریان ارائه دهند. در واقع دِوایس سعی دارد تا مشکل جدایی تیم‌های مختلف را رفع کرده و یک فرهنگ سازمانی یکپارچه را میان تیم‌های مختلفی که در حال توسعه یک نرم‌افزار هستند ایجاد کند. از این جهت بسیاری از کارها می‌تواند به صورت خودکار پیش رفته و در نهایت همه چیز با سرعت بیشتری صورت بگیرد [۱، ۱۲]. این خودکار سازی با استفاده از خط لوله CI/CD از منبع کد شروع می‌شود و تا مانیتورینگ محصول ادامه میابد [۱۴].

تا قبل از تشکیل دِوایس، تیم‌های توسعه نرم‌افزار یا تیم عملیاتی در محیط‌های جداگانه کار می‌کردند. هدف تیم توسعه تولید محصول جدید و با افزودن ویژگی‌های جدیدی روی محصولات قبلی بود. هدف تیم عملیاتی نیز ثابت نگه داشتن وضعیت موجود سرویس‌ها برای پایداری بیشتر بود. به مرور زمان در فرآیند توسعه نرم‌افزار، روش‌های چابک^۳ ایجاد شد تا با مشتری تعامل بهتری برقرار شود و نیازهایی که دارد به محصول اضافه شود [۸]. جدایی دو تیم توسعه و عملیات از هم باعث

Development^۱
Operation^۲
Agile^۳

می‌شد که در فرآیند تولید محصول و استقرار^۴ آن، اتلاف وقت ایجاد شود و محصول دیرتر به دست مشتری برسد [۶].

۲-۱-۲ چرخه کاری DevOps

همانطور که در شکل ۲-۱ مشاهده می‌کنید، DevOps قصد دارد از ابزار و جریان‌های کاری^۵ برای خودکارسازی یک یا چند مورد از موارد زیر استفاده کند:

۱. کدنویسی: شامل توسعه، بازبینی کد و ابزارهای کنترل نسخه است. مثلاً، یک تیم تصمیم می‌گیرد از گیت^۶ به عنوان ابزار کنترل نسخه و از گیت هاب^۷ نیز به عنوان یک مخزن راه دور استفاده کند. این تیم مجموعه‌ای از دستورالعمل‌های سبک کدنویسی را با استفاده از ابزاری نظیر Linter به همراه حداقل درصد پوشش تست تعریف کرده و با تعیین استراتژی انشعاب مبتنی بر تنه^۸ تغییرات خود را به منظور بازبینی برای ادغام با انشعاب اصلی^۹ برای توسعه دهنده ارشد ارسال می‌کند [۱۱].

۲. ساخت: شامل ایجاد و ذخیره خودکار مولفه^{۱۰} ها می‌باشد. به طور مثال یک تیم تصمیم می‌گیرد یک Container image قابل اجرا از محصول خود ایجاد کند.

۳. تست: شامل ابزارهایی برای تست محصول می‌باشد. تیم محیطی را به منظور تست هر تغییر جدید راه اندازی می‌کند که در آن مجموعه‌ای از آزمایش‌ها مانند آزمون واحد^{۱۱}، آزمون یکپارچگی^{۱۲} و ... به طور خودکار در برابر هر ویرایش کد اجرا می‌شود. ادغام و تست کد به طور مکرر، به تیم‌های توسعه کمک می‌کند تا از کیفیت کدشان اطمینان حاصل کرده و جلوی خطاهای احتمالی را بگیرند.

۴. پیکربندی: شامل پیکربندی و مدیریت خودکار زیرساخت می‌باشد. این مورد شامل مجموعه‌ای از اسکریپت‌هایی برای بازتولید محیط در حال اجرا و زیرساخت نرم افزاری شامل سیستم عامل تا پایگاه داده و سرویس‌های خاص و پیکربندی شبکه آنها می‌باشد [۷، ۹].

۵. استقرار: این مرحله شامل استراتژی استقرار است. به طور مثال تیم می‌تواند تصمیم بگیرد که یک محصول به طور

^۴ Deploy

^۵ Workflow

^۶ Git

^۷ Github

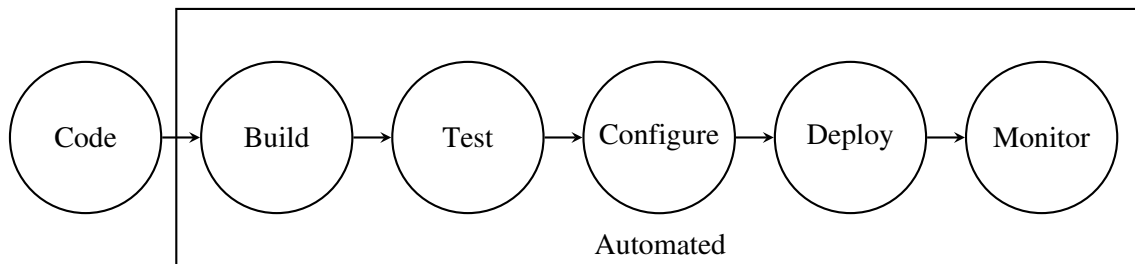
^۸ Trunk-Based

^۹ Merge request

^{۱۰} Artifact

^{۱۱} Unit test

^{۱۲} Integration test



شکل ۲-۱: مراحل DevOps

مستقیم منتشر شود یا ابتدا در یک محیط آزمایشی مورد ارزیابی قرار گیرد. هم چنین در مواقعی که مشکلی در استقرار وجود دارد چه کاری انجام دهند و استراتژی بازگشت^{۱۳} خود را پیاده سازی کنند.

۶. نظارت: از عملکرد محصول تا نظارت بر تجربه کاربر نهایی را شامل می شود. به عنوان مثال، می تواند مدت زمان درخواست های پایگاه داده یا بارگذاری وبسایت یا تعداد کاربرانی که از ویژگی های خاص محصول استفاده می کنند یا تعداد بازدیدکنندگان از یک وبسایت که به ثبت نام ختم می شود یا تعداد کاربران جدید در یک مجموعه زمانی خاص را پوشش دهد. مرحله نظارت هم چنین شامل هشدار خودکار خرابی ها نیز می باشد (به عنوان مثال، آستانه استفاده از CPU [۱۰]). در نهایت نظارت بر محیط تولید به منظور اطمینان از صحت کارکرد صحیح محصول ضروری است.

۳-۱-۲ خط لوله CI/CD

در دنیای توسعه نرم افزار دستیابی به بهره وری بالا، کیفیت مطلوب محصول و رضایت مشتری از اهداف اصلی هر سازمانی است. در متدولوژی DevOps و رویکردهای مرتبط با آن مانند ادغام مداوم^{۱۴}، تحویل مداوم^{۱۵} و استقرار مداوم^{۱۶} به طور فزاینده ای محبوب شده اند زیرا به سازمان ها کمک می کنند تا با سرعت و کارآمدی بیشتری به این اهداف دست یابند [۶].

ادغام مداوم به فرآیندی اطلاق می شود که در آن توسعه دهندگان برنامه های خود را به طور مداوم (معمولاً چندین بار در روز) در یک مخزن مشترک ادغام می کنند. به محض ادغام کد، یک سری از تست های خودکار اجرا می شود تا اطمینان حاصل شود که این تغییرات جدید باعث بروز مشکل در نرم افزار نشده اند [۱۳]. این تست ها شامل تست های واحد، تست های یکپارچگی و تست های کارکردی می باشند. از آنجایی که برنامه های کاربردی پیشرفته کنونی در چندین پلتفرم و ابزار های مختلف اقدام به توسعه می کنند، لذا نیاز به مکانیزمی برای ادغام و تایید تغییرات مختلف، اهمیت بالاتری پیدا می کند.

^{۱۳}Rollback

^{۱۴}Continuous Integration (CI)

^{۱۵}Continuos Delivery (CD)

^{۱۶}Continuous Deployment (CD)

جدول ۱-۲: نمونه هایی از ابزار برای مراحل خاص اتوماسیون خط لوله CI/CD

Tools	Phase
Bazel Gradle،	Build
pytest Selenium،	Test
Terraform Ansible،	Configure
Jenkins ArgoCD،	Deploy
Sentry Prometheus،	Monitor

تحويل مداوم ادامه ای بر ادغام مداوم است و به تیم‌ها این امکان را می‌دهد تا نرم‌افزار را پس هر تغییر مهم در کد به مرحله تولید برسانند. در این مدل، هر خروجی که از فرایند CI عبور کرده و تست‌های لازم را با موفقیت پشت سر گذاشته باشد، به صورت خودکار آماده انتشار می‌شود [۱۳]. به عبارتی دیگر، هدف از تحويل مداوم، داشتن پایگاه کدی است که همیشه آماده استقرار در محیط تولید باشد. این فرایند ممکن است شامل تست‌های اضافی برای ارزیابی عملکرد، امنیت و سازگاری با محیط‌های تولید نیز باشد.

استقرار مداوم که گاهی با تحويل مداوم اشتباه گرفته می‌شود، به فرآیندی اطلاق می‌شود که در آن هر تغییر در کد که تمام مراحل تست و تأیید را با موفقیت پشت سر می‌گذارد، به صورت خودکار در محیط تولید قرار می‌گیرد [۱۳]. این به معنای آن است که نسخه‌های جدید نرم‌افزار می‌توانند به طور مداوم و بدون دخالت دستی به کاربران نهایی تحويل داده شوند. این رویکرد به تیم‌ها کمک می‌کند تا سریعتر به بازخوردها پاسخ دهند و بهبودهای مستمری را در محصول خود اعمال کنند، اما نیازمند یک فرآیند آزمایشی بسیار قوی و اطمینان از کیفیت کد است.

فرآیند کامل CI/CD که در شکل ۱-۲ هم به عنوان بخشی از چرخه کاری توضیح داده شد [۶]، با یک فرآیند ساخت شروع می‌شود. در این مرحله کد توسط ابزارهای مرتبط که در جدول ۱-۲ ذکر شده است، تبدیل به نرم‌افزار قابل اجرا می‌شوند. پس از این مرحله، تست‌های خودکار که شامل تست‌های واحد، تست‌های یکپارچه‌سازی و تست‌های رابط کاربری هستند، اجرا می‌شوند تا اطمینان حاصل شود که تغییرات جدید باعث بروز خطا در نرم‌افزار نمی‌شوند. در صورت موفقیت‌آمیز بودن تست‌ها، یک نسخه قابل اجرا از کد نسخه گذاری شده و در مخازنی همانند Nexus نگه داری می‌شوند. در مرحله پیکربندی تنظیم محیط لازم برای نصب و استفاده از نرم‌افزار انجام می‌شود. دو رویکرد اصلی برای این کار وجود دارد: مرحله به مرحله^{۱۷} و اعلامی^{۱۸}. در رویکرد اول، پیش‌نیازها به ترتیب آماده‌سازی می‌شوند و شکست در هر مرحله می‌تواند به عدم انجام دادن مراحل بعدی منجر شود. این رویکرد، که اغلب با استفاده از ابزارهایی مانند Ansible پیاده‌سازی می‌شود، زمانی مفید است که نیاز به اعمال تغییرات جزئی بر محیط باشد. در مقابل، رویکرد اعلامی به طور همزمان کل محیط را بر اساس یک حالت نهایی

Procedural^{۱۷}Declarative^{۱۸}

تعریف شده آماده می‌کند. این رویکرد باعث می‌شود که در صورت بروز خطا در یک بخش، سایر بخش‌ها تحت تأثیر قرار نگیرند. برای اجرای این رویکرد، می‌توان از ابزارهایی مثل Terraform استفاده کرد [۴]. پس از این، مرحله‌ی استقرار آغاز می‌شود که در آن نرم‌افزار به محیط‌های تست، توسعه یا تولید منتقل می‌شود. این فرایند اغلب شامل مکانیزم‌هایی برای پشتیبانی و بازگرداندن نسخه‌های قبلی در صورت بروز مشکل است. یکی از قسمت‌های فرآیند کامل این خط لوله نیز با استفاده از ابزاری مانند Gitlab CI، CircleCI و Jenkins می‌تواند انجام گردد. در آخر نیز مرحله نظارت انجام می‌شود. ابزارهای نظارتی نظیر Prometheus و Grafana معمولاً شامل نمودارها، گزارش‌ها، و آمارهایی هستند که به شما اطلاعاتی در مورد وضعیت فعلی خط لوله و عملکرد برنامه‌های آزمایشی و انتشارات را ارائه می‌دهند. هم چنین اطلاعاتی مانند زمان طول کشیده برای هر مرحله، تعداد خطاها و متوسط زمان بین خرابی‌ها^{۱۹} از جمله آمارهایی هستند که ممکن است در این مرحله نمایش داده شوند. لازم به ذکر است که می‌توان به منظور بررسی سبک کدنویسی و اعمال استاندارد های تیم توسعه در ابتدا خط لوله بخشی را قرار داد تا از استاندارد بودن کد اطمینان یابد. در این بخش می‌توان از Linter ها یا pre-commit hooks استفاده کرد. معروف ترین ابزار برای هر مرحله را در جدول ۲-۱ نیز مشاهده می‌کنید.

به هنگام طراحی و پیاده سازی یک خط لوله CI/CD باید به نکات زیر توجه کرد [۶، ۴، ۱۳]:

- قابلیت بازگشت به حالت قبل^{۲۰}

- قابلیت مشاهده^{۲۱} و هشدار دادن^{۲۲}

- امنیت

- مدت زمان اجرای خط لوله

برای هر نسخه از کد باید یک استراتژی بازگشت وجود داشته باشد تا اگر مشکلی پیش آمد، به نسخه قبلی بازگردانده شود. یک راه حل آسان برای بازگشت می‌تواند اجرای نسخه قدیمی تر از طریق همان خط لوله CI/CD باشد. بازگشت به ورژن قبلی همیشه ساده نیست، چراکه اگر سرویس در حال اجرا قابل بازگشت باشد، باید به بازگرداندن داده‌ها قبلی و زمان توقف هنگام استقرار نسخه جدید نیز توجه کرد.

هر انتشار باید شفاف باشد که چه تغییراتی اعمال شده و چه کسی تغییرات را تأیید کرده است. هم چنین تیم توسعه باید بداند که استقرار موفقیت‌آمیز بوده و چه زمانی انجام شده است. در نهایت باید هشدارهای واضحی از کد خراب در خط لوله و

^{۱۹} Mean time between failures (MTBF)

^{۲۰} Rollback

^{۲۱} Observability

^{۲۲} Alerting

خطای احتمالی در انتشار وجود داشته باشد. اگر مشکلی در استقرار پیش آید و هیچ سابقه واضحی از تغییرات وجود نداشته باشد، بازگشت به حالت قبل دشوار خواهد بود. علاوه بر این دلیل بروز این مشکل در استقرار نیز برای تیم نامعلوم است. تصور کنید که یک توسعه‌دهنده به صورت دستی به یک ماشین محیط تولید دسترسی پیدا کرده و به طور تصادفی یک فایل کلیدی را حذف می‌کند که پس از چند روز باعث خرابی‌های سیستم می‌شود. هیچ ردی از این تغییرات وجود ندارد، هیچکس نمی‌داند کجا را باید به حالت قبلی برگرداند و حتی بازگشت به کد قبلی ممکن است کمی نکند زیرا فایل گمشده ممکن است در ورژن قبلی بازتولید نشود.

توجه به امنیت در فرآیندهای CI/CD بسیار حیاتی است تا سلامت و امنیت فرآیندهای توسعه و ارسال نرم‌افزار حفظ شود. اجرای کنترل دسترسی بر اساس نقش^{۲۳} ضروری است تا فقط افراد مجاز بتوانند تغییراتی در فرآیند CI/CD اعمال کرده و کد را ارسال کنند. این شامل کنترل دسترسی به ابزارهای CI/CD نظیر Jenkins و همچنین به هر سیستم متمرکز مانند مخازن کد منبع است. هم چنین مدیریت اسرار^{۲۴} جنبه اساسی امنیت خط لوله است. اسراری مانند کلیدهای API، رمزعبورها و گواهی‌نامه‌ها باید به طور امن ذخیره و دسترسی‌پذیر باشند. استفاده از ابزارهایی مانند HashiCorp Vault می‌تواند به مدیریت امنیت اسرار کمک کند.

مدت زمان اجرای کامل یک خط لوله از ساخت تا استقرار برای حفظ چابکی بسیار مهم است. تست‌ها و ساخت‌های طولانی مدت می‌توانند منجر به تداخل با خط لوله‌های دیگر باشد. بهبود و بهینه‌سازی این فرآیند از طریق اجرای موازی تست‌ها، بهبود قابلیت مقیاس‌پذیری زیرساخت و بهینه‌سازی کد می‌تواند به کاهش زمان مورد نیاز برای تست و ساخت و بهبود جریان کار توسعه کمک کند.

در محصولاتی که از یادگیری ماشین استفاده می‌کنند نیز مراحل خط لوله برای رسیدگی به چرخه عمر مدل و داده‌ها افزایش می‌یابد، اما عناصر، مزایا و اهداف یکسان هستند.

۲-۱-۴ مزایای متدولوژی DevOps

این متدولوژی یک رویکرد نوآورانه در توسعه نرم‌افزار و عملیات است که مزایای بسیاری برای بهبود عملکرد سازمانی^{۲۵} ارائه می‌دهد [۵]. ادغام این روش‌ها می‌تواند نحوه مواجهه تیم‌ها با چالش‌های پروژه و تعامل با فناوری را تغییر داده و منجر به افزایش کارایی، قابلیت اطمینان و رضایت شود [۷].

۱. افزایش سرعت و کارایی: با خودکارسازی فرایند انتشار نرم‌افزار از طریق CI/CD، تیم‌ها می‌توانند فرکانس و سرعت

^{۲۳} Role-Based Access Control (RBAC)

^{۲۴} Secrets

^{۲۵} Organization performance

انتشارها را افزایش داده که منجر افزایش سرعت پاسخ دهی به مشتری شده و مزیت رقابتی ایجاد می کند [۱۴].

۲. ایجاد محیط‌های عملیاتی پایدارتر: تضمین قابلیت اطمینان به‌روزرسانی‌های برنامه و تغییرات زیرساخت یکی از مزایای مهم این متدلوژی می باشد. از طریق خط لوله CI/CD، هر تغییری برای اطمینان از کارایی و ایمنی ادغام با محیط تولید آزمایش می‌شود تا از انتشار نسخه‌های معیوب جلوگیری کند. یکی از شاخص‌های اصلی پایداری، انتشارهای متناوب و مکرر است. با استفاده از این متدلوژی توسعه‌دهندگان می‌توانند خطاها را سریع‌تر شناسایی و رفع کنند. این موضوع باعث کاهش شاخص $MTTR^{26}$ می‌شود. این شاخص مدت زمان برگشت به وضعیت پایدار بعد از وقوع خطا یا اشکال را نشان می‌دهد و هرچه مقدار آن کمتر باشد، پایداری سیستم بیشتر است [۶]. علاوه بر انتشار پیوسته و مستمر، نرم‌افزارهای مانیتورینگ هم با پایش مداوم نرم‌افزار و سرورها و ایجاد دسترسی به اطلاعات حیاتی نرم‌افزار و محیط عملیاتی برای مهندسان، نقش مهمی در شناسایی و رفع خطاها و در نتیجه حفظ پایداری دارند.

۳. مقیاس پذیری: تسهیل‌کننده مدیریت مقیاس‌پذیر زیرساخت‌ها و فرآیندهای توسعه است. تکنیک‌هایی مانند زیرساخت به عنوان کد^{۲۷} مدیریت محیط‌های توسعه، آزمایش و تولید را به شکلی تکرارپذیر و کارآمد ساده‌سازی می‌کنند [۱].

۴. صرفه‌جویی در هزینه‌ها و منابع: علاوه بر مدیریت بهتر عملکرد و ارتباطات، هزینه‌ها و منابع را هم به نسبت روش‌های قدیمی کاهش می‌دهد. با استفاده از این متدلوژی و خط لوله CI/CD طول چرخه‌ها کوتاه‌تر و نتایج کمی و کیفی بهتر می‌شوند و در نتیجه هزینه‌ها نیز کاهش پیدا می‌کنند. این فرآیند حتی نیاز به منابع سخت‌افزاری و منابع انسانی را هم کاهش می‌دهد. با استفاده از معماری ماژولار، اجزا و منابع به خوبی دسته‌بندی شده و سازمان‌ها می‌توانند به راحتی از فضا و رایانش ابری برای انجام کارها استفاده کنند. چابکی در این متدلوژی اهمیت زیادی دارد لذا فناوری ابری نیز این چابکی را به تیم‌ها ارائه و سرعت و هماهنگی بین تیم‌ها را افزایش می‌دهد. با کمک این فناوری، حتی اگر در فرایند توسعه و عملیات نیاز به منابع جدید و بیشتر بود، با ثبت یک درخواست ساده در عرض چند دقیقه منابع جدید در اختیار سازمان قرار می‌گیرد. از مزایای دیگر استفاده از رایانش ابری می‌توان به حداقل شدن هزینه‌های شروع و عملیاتی پروژه، بهبود امنیت، افزایش مشارکت و بهبود دسترسی و کاربری داده‌ها اشاره کرد.

۵. تجزیه ایزوله‌گرایی: در بسیاری از سازمان‌ها، به دلایل امنیتی و مدیریتی، اطلاعات در تیم‌ها به طور جداگانه نگهداری می‌شوند و این باعث ایجاد سیلوهای سازمانی شده که مانع از گردش منظم داده و اطلاعات در سازمان می‌شود. با این حال، با بهره‌گیری از این متدلوژی و وجود همکاری فعال در تیم‌ها، ارتباطات بهبود می‌یابد. این امر باعث می‌شود که

²⁶Mean Time To Recover
²⁷infrastructure as a code

اطلاعات به طور موثرتر جریان یابد، کارایی تیم‌ها افزایش یابد و در نتیجه، کارایی کلی سازمان بهبود پیدا کند.

۲-۲ مجازی سازی و کانتینر سازی

۱-۲-۲ مجازی سازی

تکنولوژی مجازی سازی^{۲۸} به روشی اشاره دارد که در آن منابع سخت افزاری یک سیستم فیزیکی به چندین محیط مجازی تقسیم می‌شوند. این تکنولوژی به سازمان‌ها این امکان را می‌دهد تا منابع خود را به شیوه‌ای کارآمدتر استفاده کنند، زیرا می‌توانند چندین سیستم عامل و برنامه را روی یک سرور فیزیکی اجرا کنند. مجازی سازی انواع مختلفی دارد، از جمله مجازی سازی سرور، دسکتاپ، نرم افزار و شبکه، که هر کدام کاربردهای خاص خود را دارند [۲، ۳].

مجازی سازی سرور یکی از تکنولوژی‌های کلیدی در مدیریت و بهره‌برداری از داده‌ها و منابع سخت افزاری در مراکز داده است. این فناوری امکان تقسیم یک سرور فیزیکی^{۲۹} به چندین سرور مجازی را می‌دهد، به طوری که هر سرور مجازی می‌تواند به صورت مستقل عمل کرده و سیستم عامل و برنامه‌های کاربردی خود را اجرا کند. مجازی سازی سرور معمولاً شامل سه جزء اصلی است [۳]:

- هایپروایزر^{۳۰}
- ماشین مجازی
- سیستم مدیریت مرکزی

هایپروایزر، که گاهی اوقات به عنوان مدیر ماشین مجازی^{۳۱} شناخته می‌شود، نقش محوری در مجازی سازی سرور دارد. این نرم افزار بر روی سخت افزار سرور نصب می‌شود و وظیفه آن تقسیم منابع سرور فیزیکی، مانند CPU، حافظه، فضای دیسک و شبکه به چندین ماشین مجازی است. هایپروایزرها به دو دسته تقسیم می‌شوند.

هایپروایزر نوع^{۳۲} مستقیماً بر روی سخت افزار نصب می‌شود و به طور مستقل از سیستم عامل فیزیکی عمل می‌کند. می‌توان از هایپروایزرهای نوع ۱ معروف به VMware ESXi، Microsoft Hyper-V و KVM اشاره کرد که برای بهینه سازی عملکرد و امنیت طراحی شده‌اند.

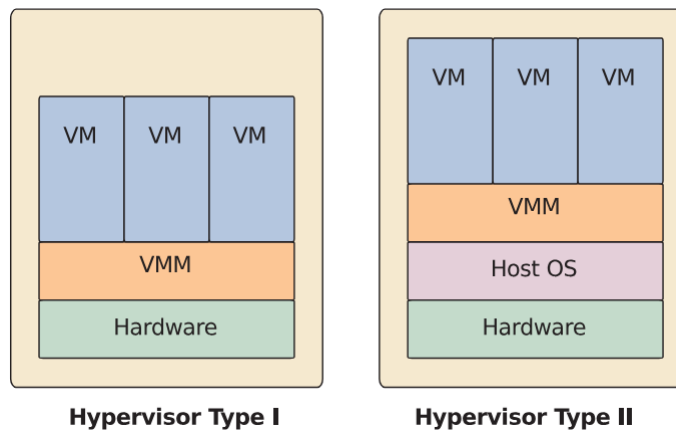
^{۲۸}Virtualization

^{۲۹}Bare-metal

^{۳۰}Hypervisor

^{۳۱}Virtual Machine Manager (VMM)

^{۳۲}Bare-metal



شکل ۲-۲: انواع هایپروایزر [۳]

هایپروایزر نوع ۳۲ روی یک سیستم عامل میزبان نصب می‌شود و به عنوان یک برنامه درون سیستم عامل عمل می‌کند. از هایپروایزر نوع ۲ نیز می‌توان به VMware Workstation و Oracle VirtualBox اشاره کرد. این هایپروایزرها اغلب برای تست و توسعه مورد استفاده قرار می‌گیرند. در شکل ۲-۲ ساختار آن را مشاهده می‌کنید.

هایپروایزرها به لحاظ انعطاف پذیری و امکان پیکربندی متنوع، قابلیت‌های قدرتمندی را برای مدیریت سرورهای مجازی فراهم می‌کنند. آنها می‌توانند به طور خودکار منابع را بین ماشین‌های مجازی تخصیص دهند و امکاناتی مانند تکثیر^{۳۴} و بازیابی فاجعه^{۳۵} را ارائه دهند.

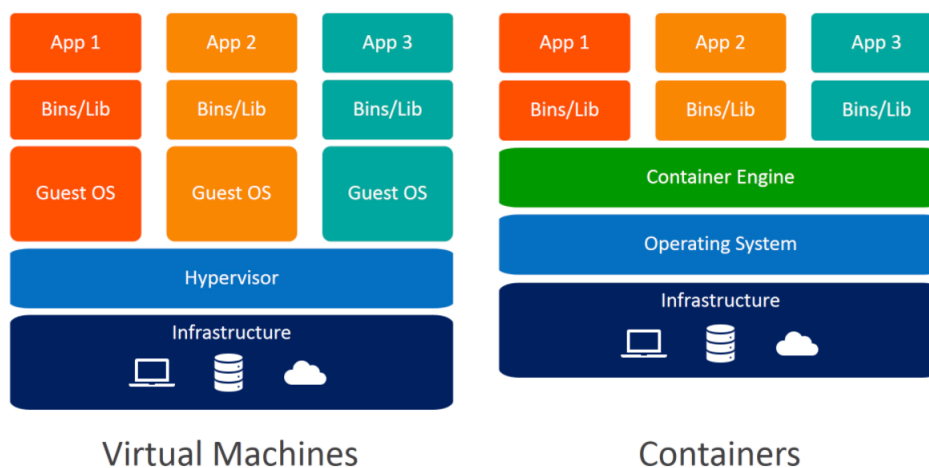
ماشین مجازی^{۳۶} واحدی از منابع مجازی است که شبیه‌سازی یک سرور فیزیکی را انجام می‌دهد. هر VM می‌تواند سیستم عامل خود را داشته باشد و مستقل از دیگر VMها عمل کند. این امر به کاربران اجازه می‌دهد که برنامه‌های متعدد را بدون تداخل با یکدیگر اجرا کنند. VMها از منابع سخت‌افزاری تخصیص داده شده توسط هایپروایزر استفاده می‌کنند و می‌توانند به راحتی از یک سرور فیزیکی به دیگری با استفاده از تکنیک‌هایی نظیر Snapshot منتقل شوند. استفاده از تکنولوژی مجازی‌سازی نقش بسیار مهمی در فرآیندهای DevOps دارد. با امکان ایجاد و حذف سریع ماشین‌های مجازی، مجازی‌سازی به تیم‌های توسعه این امکان را می‌دهد که به سرعت محیط‌های نرم‌افزاری مورد نیاز خود را راه‌اندازی و پس از اتمام کار، آنها را به راحتی حذف کنند، که این امر منجر به صرفه‌جویی در هزینه‌ها و منابع می‌شود. علاوه بر این، مجازی‌سازی ریسک‌های مرتبط با استقرار نهایی در محیط تولید را کاهش داده و با ایجاد محیط‌های شبیه‌سازی شده برای آزمایش‌های پیش از استقرار، اطمینان حاصل می‌کند که نرم‌افزار قبل از راه‌اندازی به درستی کار می‌کند.

^{۳۲} Hosted

^{۳۴} Replication

^{۳۵} Disaster Recovery

^{۳۶} Virtual Machine (VM)



شکل ۲-۳: تفاوت ماشین مجازی و کانتینر

۲-۲-۲ کانتینرسازی

کانتینرها محیط‌هایی هستند که به برنامه‌های نرم‌افزاری امکان می‌دهند تا با تمام وابستگی‌های خود در یک بسته واحد جمع‌آوری شوند. آن‌ها همانند برنامه‌های نرم‌افزاری سنتی که به شما اجازه می‌دهند مستقل از نرم‌افزارهای دیگر و خود سیستم عامل کار کنید، نصب نمی‌شوند. مهمترین دغدغه کانتینرها این است که چگونه محیطی فراهم کنند تا نرم‌افزارهایی که در یک محیط پردازشی اجرا می‌شوند با انتقال به محیط دیگر، بدون ایراد و مشکل اجرا شوند. این تکنولوژی از معماری میزبان بهره می‌برد تا از منابع سخت‌افزاری مشترک استفاده کند، اما اجرای برنامه‌ها را در فضاهایی منزوی و مستقل فراهم می‌کند. کانتینرها به مشتریان این قابلیت را می‌دهند، تا برنامه‌ها و وابستگی‌های آن‌ها را به صورت یک فرآیند ایزوله شده در سیستم اجرا کنند. تمام اجزای ضروری مورد نیاز یک برنامه به صورت یک image بسته‌بندی می‌شود. Image مربوطه در یک محیط ایزوله اجرا شده و فضای حافظه، CPU و فضای ذخیره سازی خود را با سیستم عامل به اشتراک نخواهد گذاشت. این عمل موجب می‌شود که فرآیندهای موجود در کانتینر، قادر به مشاهده سایر فرآیندها در خارج از آن نباشند.

کانتینرها و ماشین‌های مجازی هر دو ابزارهایی برای ایزوله‌سازی منابع نرم‌افزاری هستند، اما تفاوت‌های اساسی در معماری و کاربرد آن‌ها وجود دارد که در شکل ۲-۳ نشان داده شده است. ماشین‌های مجازی با ایجاد یک لایه انتزاعی کامل بر روی سخت‌افزار فیزیکی کار می‌کنند که به آن‌ها اجازه می‌دهد سیستم‌عامل‌های مستقل را بر روی هر VM اجرا کنند. این امر به هر ماشین مجازی امکان می‌دهد منابع سخت‌افزاری را به صورت مجزا استفاده کند، اما باعث می‌شود VM‌ها نسبت به کانتینرها سنگین‌تر و کم‌استفاده‌تر باشند. در مقابل، کانتینرها به جای سیستم‌عامل‌های کامل، تنها برنامه‌ها و وابستگی‌های

خود را ایزوله می‌کنند و همگی بر روی هسته سیستم عامل میزبان اشتراکی اجرا می‌شوند، که این امر باعث سبک‌تر، سریع‌تر و مقیاس‌پذیرتر شدن کانتینرها نسبت به ماشین‌های مجازی باشند. از این رو، کانتینرها برای محیط‌هایی که نیازمند راه‌اندازی سریع و مدیریت منابع کارا هستند، مانند میکروسرویس‌ها و برنامه‌های کاربردی مبتنی بر Cloud، ایده‌آل می‌باشند. این تکنولوژی ریشه در مفهوم چارچوب‌های Unix مانند chroot دارد که در دهه ۱۹۷۰ معرفی شد. اما، پیشرفت‌های اصلی در این زمینه با ظهور Docker در سال ۲۰۱۳ آغاز شد. داکر یک پلتفرم متن باز است که استانداردسازی ایجاد، اجرا و مدیریت کانتینرها را فراهم کرد و به سرعت به یکی از مهم‌ترین ابزارها در این حوزه تبدیل شد.

اجزای کلیدی مورد استفاده در پیاده‌سازی کانتینرها شامل موارد زیر است:

- موتورهای کانتینر^{۳۷}

- سازآرایی کانتینر^{۳۸}

موتورهای کانتینری مانند Docker Engine و Containerd ابزارهایی هستند که کانتینرها را ایجاد، اجرا و مدیریت می‌کنند. این موتورها از فناوری‌های موجود در هسته لینوکس مانند Namespaces و Control groups (cgroups) برای ایزوله‌سازی کانتینرها استفاده می‌کنند و به آن‌ها امکان می‌دهند که فرایندها و منابع سیستمی را به صورت مستقل از یکدیگر مدیریت کنند. Namespaces بخشی از هسته لینوکس که امکان جداسازی عناصری مثل شبکه، فرایندها و فضای فایل سیستم را فراهم می‌کند. هر کانتینر در یک namespace جداگانه اجرا می‌شود که استقلال آن را نسبت به دیگر برنامه‌ها تضمین می‌کند. cgroups نیز به مدیریت استفاده از منابع سخت‌افزاری مانند CPU و حافظه توسط فرایندها کمک می‌کند. این فناوری امکان اختصاص دقیق منابع به کانتینرها را می‌دهد و از مصرف بیش از حد منابع توسط یک کانتینر جلوگیری می‌کند.

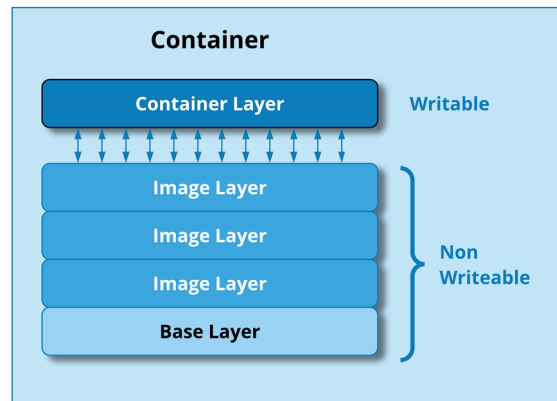
برای مدیریت و مقیاس‌بندی کانتینرها در محیط‌های تولید، ابزارهای سازآرایی مانند Kubernetes و Docker Swarm کاربرد دارند. این ابزارها به توسعه‌دهندگان این امکان را می‌دهند که خوشه^{۳۹} های بزرگ کانتینری را مدیریت کنند و برنامه‌ها را با انعطاف‌پذیری و دقت بالا مقیاس بندی نمایند.

Docker Image به عنوان اساسی‌ترین بخش در اکوسیستم داکر نقش کلیدی در پیاده‌سازی و توزیع برنامه‌های نرم‌افزاری دارد. تصاویر داکر از یک معماری لایه‌ای بهره می‌برند. معماری لایه این امکان را فراهم می‌کند که تغییرات نسبت به یک تصویر پایه به صورت دیفرانسیلی اعمال شود. هر لایه در تصویر داکر، تغییراتی را نسبت به لایه قبلی اضافه می‌کند. این رویکرد باعث می‌شود که بازسازی و به‌روزرسانی تصاویر کانتینری فقط بر روی لایه‌هایی که تغییر کرده‌اند انجام شود، که به نوبه

^{۳۷} Container Engine

^{۳۸} Container Orchestration

^{۳۹} Cluster



شکل ۲-۴: معماری لایه ای تصویر داکر

خود باعث کاهش حجم داده‌های مورد نیاز برای ذخیره‌سازی و انتقال می‌شود. زمانی که Dockerfile نوشته می‌شود، هر دستور (مانند RUN، COPY و FROM) یک لایه جدید در تصویر داکر ایجاد می‌کند. این لایه‌ها به ترتیبی که در داکر فایل آمده‌اند، روی هم اضافه می‌شوند. داکر از یک فایل سیستم Union استفاده می‌کند که به آن اجازه را می‌دهد تا لایه‌های مختلف را به گونه‌ای ترکیب کند که به نظر یک فایل سیستم یکپارچه است. ساختار لایه ای تصویر داکر را در شکل ۲-۴ مشاهده می‌کنید.

فصل ۳

مدل بینایی انسان و کاربرد آن در نهان نگاری

۱-۳ مقدمه

بیشتر تصاویر دیجیتال پس از گذر از پردازشهای مختلف، سرانجام توسط چشم انسان دیده و سنجیده می‌شوند، لذا ضروری است که بتوان کیفیت بصری تصویر را همچنان حفظ نمود. در کاربرد نهان نگاری، پنهان‌سازی کامل نهان نگاره و حفظ کیفیت بصری تصویر یکی از نیازهای ضروری است. لذا سیستم بینایی انسان را باید مورد بررسی قرار داده و از آن استفاده نمود. بررسیها نشان می‌دهد [۱] که در نهان نگاری با بهره‌گیری مناسب از مدل بینایی انسان، امکان بالا بردن بیشتر انرژی نهان نگاره با حفظ ویژگی نامرئی بودن، فراهم می‌گردد.

فصل ۴

آنتروپی و استفاده از آن در نهان نگاری

۴-۱ مقدمه

در فصل گذشته سیستم بینایی انسان و ویژگی‌های آن را مورد بررسی قرار دادیم. در حوزه تبدیل DCT و تبدیل موجک، دو مدل معروف و موجود برای سیستم بینایی معرفی کردیم. همچنین چارچوب کلی استفاده از مدل‌های بینایی را برای کاربرد نهان نگاری، مطرح نمودیم و دو طرح مرجع P&Z و K&R را نیز مورد بررسی قرار دادیم. در این فصل به بیان هدف اصلی این پایان نامه که بررسی اثر آنتروپی در نهان نگاری است، می‌پردازیم. لذا ابتدا در بخش ۴-۲ به بیان مفهوم آنتروپی پرداخته، سپس در بخش ...

۴-۲ آنتروپی

در این قسمت ابتدا توضیح مختصری در باره مفهوم آنتروپی داده خواهد شد.

فصل ۵

نتیجه‌گیری و پیشنهادات

با پیشرفت فن‌آوری دیجیتال و گسترش هرچه بیشتر کاربردهای سرویس‌های چندرسانه‌ای دیجیتال، نیازهای امنیتی جدیدی در سطح جهان مطرح گردیده است و لذا با نفوذ دنیای دیجیتال به زندگی مردم، طراحی سیستم‌های امنیتی مرتبط به آن اهمیت فراوانی در سالهای اخیر پیدا کرده‌اند. به دنبال این نیاز، نهان‌نگاری به عنوان روشی مؤثر جهت تأمین برخی از این نیازها مورد توجه قرار گرفته و پیشرفت سریعی داشته است.

در این پایان‌نامه جهت آشنایی و نیل به یک دیدگاه کلی از سیستم‌های نهان‌نگاری ابتدا به بیان کاربردهای نهان‌نگاری

پرداختیم. ...

مراجع

- [1] “What is devops?,” URL: <https://aws.amazon.com/devops/what-is-devops/> [Accessed: 2024-05-07].
- [2] “What is virtualization?,” URL: <https://aws.amazon.com/what-is/virtualization/> [Accessed: 2024-05-08].
- [3] L Navarro E Hernandez-sanchez F Rodriguez-Haro, F Freitag, “A summary of virtualization techniques,” in *Iberoamerican Conference on Electronics Engineering and Computer Science*, 2012.
- [4] Anja Kammer Florian Beetz and Dr. Simon Harrer, *GitOps Cloud-native Continuous Deployment*, 2021.
- [5] N. Forsgren and J. Humble, “The role of continuous delivery in it and organizational performance,” in *Western Decision Sciences Institute (WDSI)*, March 2016.
- [6] Jez Humble and David Farley, *Continuous Delivery: Reliable Software Releases through Build, Test, and Deployment Automation*, Addison-Wesley Professional, 2010.
- [7] M. Huttermann, *DevOps for Developers*, chapter Infrastructure as Code, 2012.
- [8] A. Van Bennekum A. Cockburn-W. Cunningham M. Fowler J. Grenning J. Highsmith A. Hunt R. Jeffries K. Beck, M. Beedle, “Manifesto for agile software development,” 2001, URL: <https://agilemanifesto.org/> [Accessed: 2024-02-17].
- [9] E. D. Nitto M. Guerriero M. Artac, T. Borovssak and D. A. Tamburri, “Devops: Introducing infrastructure-as-code,” in *International Conference on Software Engineering Companion (ICSE-C)*, May 2017.
- [10] A. Q. Gates N. Delgado and S. Roach, “A taxonomy and catalog of runtime software-fault monitoring tools,” *IEEE Transactions on Software Engineering*, vol. 30, pp. 859–872, December 2004.
- [11] paul hammant, “Trunk based development,” URL: <https://trunkbaseddevelopment.com/> [Accessed: 2023-11-01].
- [12] K. Petersen R. Jabbari, N. Ali and B. Tanveer, “What is devops?: A systematic mapping study on definitions and practices,” May 2016.
- [13] Indika Perera S.A.I.B.S. Arachchi, “Continuous integration and continuous delivery pipeline automation for agile software project management,” in *Moratuwa Engineering Research Conference (MERCOn)*, May 2018.
- [14] M. Virmani, “Understanding devops bridging the gap from continuous integration to continuous delivery,” in *Fifth International Conference on the Innovative Computing Technology (INTECH 2015)*, May 2015.

ABSTRACT

In the digital world today, invisible and robust image watermarking which embeds invisible signals in to the digital images has been proposed as a major solution to the problem of copyright protection of digital images. Several approaches such as exploiting Human Visual System (HVS) and invariant domain watermarking have been proposed to achieve this goal. In this thesis we use the information-theoretic concepts as tools to develop methods for embedding watermark in an optimized way. Also multi-resolution transforms such as wavelet transform and MR-SVD (Multi-Resolution form of the Singular Value Decomposition) are used in the proposed structure, because theses transforms resemble the HVS characteristics for an optimized watermarking structure. Entropy concept and entropy masking effects were proposed to use to develop a model in DWT domain to increase the strength and robustness of the watermark, while perceived quality of the electronic image is not altered. Then, the structure similar to the entropy-based proposed structure in DWT domain, is used for watermarking in the MR-SVD transform domain, which is found a new approach to robust image watermarking. Simulation results show that the proposed methods outperform conventional methods in terms of both invisibility and robustness.

KEYWORDS

1. Image Watermarking.
2. Multi-Resolution Transform.
3. Human Visual System (HVS).
4. Wavelet Transform.
5. Singular Value Decomposition (SVD).
6. Entropy.
7. Entropy Masking.



SHARIF UNIVERSITY OF TECHNOLOGY
ELECTRICAL ENGINEERING DEPARTMENT

M.Sc. THESIS

Title:

An Information-Theoretic Model for Image Watermarking

by:

AAAAA BBBBBB

Supervisor:

Dr. ...

August 2005