



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 مرور مفاهیم پایه                         | ۲  |
| ۲  | ۱-۱-۲ تعریف                                  | ۲  |
| ۳  | ۲-۱-۲ تاریخچه BSS                            | ۳  |
| ۵  | ۳-۱-۲ کاربردهای BSS                          | ۵  |
| ۶  | ۴-۱-۲ ICA به عنوان روشی برای حل مسأله BSS    | ۶  |
| ۸  | ۳ مدل بینایی انسان و کاربرد آن در نهان نگاری | ۸  |
| ۸  | ۱-۳ مقدمه                                    | ۸  |
| ۹  | ۴ آنتروپی و استفاده از آن در نهان نگاری      | ۹  |
| ۹  | ۱-۴ مقدمه                                    | ۹  |
| ۹  | ۲-۴ آنتروپی                                  | ۹  |
| ۱۰ | ۵ نتیجه گیری و پیشنهادات                     | ۱۰ |

# فهرست جداول



# فهرست تصاویر

|   |       |                        |     |
|---|-------|------------------------|-----|
| ۳ | ..... | مراحل دواپس            | ۱-۲ |
| ۴ | ..... | سیستم جداساز در روش HJ | ۲-۲ |

# 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<sup>۱</sup> 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.

---

<sup>۱</sup> Intellectual Property

## فصل ۲

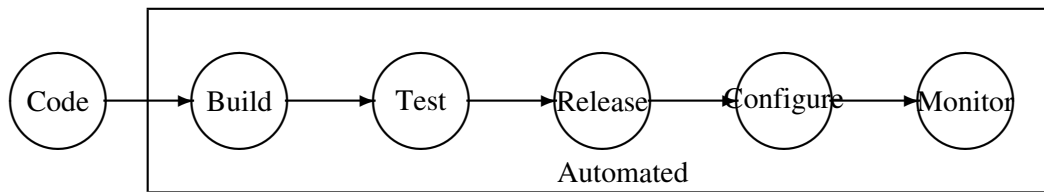
# مرور مفاهیم پایه

## ۱-۲ Devops چیست؟

### ۱-۱-۲ تعریف

دِوایس از اتحاد واژگان Development و Operation به معنای روش‌هایی است که تیم‌های توسعه و عملیات را به همکاری موثرتر نزدیک می‌کند. ارزشهای روش دِوایس به فرایند توسعه نرم‌افزار اضافه می‌شود که با استفاده از آن فرآیند تولید نرم‌افزار چابک و خودکار می‌گردد. این خودکارسازی از منبع کد شروع می‌شود با استفاده از خط لوله CI/CD تا مانیتورینگ محصول ادامه می‌یابد. در عمل، DevOps قصد دارد از ابزار و گردش کار برای خودکارسازی یک یا چند مورد استفاده کند مراحل : DevOps

- مرحله کدنویسی: شامل توسعه، بررسی کد و ابزارهای کنترل نسخه است. مثلاً، یک تیم تصمیم می‌گیرد از Git به عنوان ابزار کنترل نسخه و Github به عنوان یک مخزن راه دور استفاده کند. این تیم مجموعه‌ای از دستورالعمل‌های سبک کد اعمال‌شده خودکار و پوشش تست را تعریف می‌کند درصداً، در مورد استفاده از استراتژی انشعاب توسعه تصمیم می‌گیرد و تمام تغییرات در شعبه اصلی را اعمال می‌کند تا توسط یک توسعه دهنده ارشد بررسی و پذیرفته شود.
- مرحله استقرار: شامل ایجاد و ذخیره خودکار آثار است. مثلاً، یک تیم تصمیم می‌گیرد یک image قابل اجرا از محصول خود ایجاد کند.
- مرحله تست: شامل ابزارهای آزمایش مداوم است. تیم، محیطی را راه اندازی می‌کند که در آن یک مجموعه‌ای از آزمایش‌های مداوم به‌طور خودکار در برابر هر ویرایش کد اجرا می‌شود که بسیار مهم است. فرآیند تست برای هر مرحله



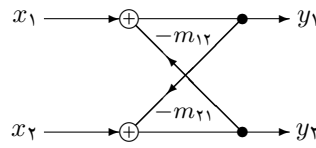
شکل ۲-۱: مراحل دواپس

از CI/CD می تواند متفاوت باشد.

- مرحله انتشار: این مرحله شامل استراتژی انتشار است به طور مثال تیم می تواند تصمیم بگیرد که یک محصول به طور مستقیم منتشر شود یا ابتدا در یک محیط آزمایشی مورد ارزیابی قرار گیرد.
- مرحله پیکربندی: شامل پیکربندی و مدیریت خودکار زیرساخت است. بهترین شیوه ها شامل اعلام زیرساخت تولید توسط کد است که به معنی مجموعه ای از اسکریپت ها برای بازتولید محیط در حال اجرا و زیرساخت نرم افزار شامل سیستم عامل تا پایگاه داده و سرویس های خاص و پیکربندی شبکه است.
- مرحله نظارت: از عملکرد محصول تا نظارت بر تجربه کاربر نهایی را شامل می شود. به عنوان مثال، می تواند مدت زمان پرس و جوهای پایگاه داده یا بارگذاری وب سایت یا تعداد آنها را پوشش دهد. همچنین می تواند عملکرد زیرساخت نرم افزار مانند سطح استفاده از CPU را مورد ارزیابی قرار دهد.

## ۲-۱-۲ تاریخچه BSS

با توجه به ظاهر ill posed مسأله BSS، مطرح شدن آن در پردازش سیگنال نسبتاً دیرنگام بوده است. امکان حل مسأله BSS نخستین بار در سال ۱۹۸۵ و توسط هرو (Hérault)، ژوتن (Jutten) و آنس (Ans) در یک کاربرد بیولوژیکی ارائه شد [۸] (اولین مقاله بین المللی روی این موضوع به زبان انگلیسی [۷] است). ایده اولیه حدود سال ۱۹۸۲ و هنگامی بوجود آمد که این تیم روی یک مسأله بیولوژیکی کار می کرد و مشاهده کردند که هنگام انتقال اطلاعات مربوط به سرعت و مکان زاویه ای یک مفصل به مغز، اطلاعات مربوط به سرعت و مکان توسط دو سیگنال عصبی مختلف به مغز ارسال می شوند، ولی در هر دوی این سیگنالها اطلاعات مکان و سرعت با هم مخلوط هستند و در نتیجه مغز حتماً باید روشی برای جداکردن این اطلاعات داشته باشد. به عبارتی مغز باید به طریقی بتواند سیستم معکوس را تنها از روی مشاهدات تخمین بزند. آنها در نهایت روشی برای تخمین پارامترهای سیستم معکوس یافتند که بعدها به الگوریتم HJ (Hérault-Jutten) معروف شد.



شکل ۲-۲: سیستم جداساز در روش HJ

هرو و ژوتن برای جداسازی دو سیگنال مخلوط ابتدا مدل فیدبک دار شکل ۲-۱-۲ را برای سیستم جداساز در نظر گرفتند. روشن است که این مدل با انتخاب مناسب ضرایب  $m_{12}$  و  $m_{21}$  قادر است سیگنالها را از هم جدا کند. در واقع داریم:

$$\begin{cases} y_1 = x_1 - m_{12}y_2 \\ y_2 = x_2 - m_{21}y_1 \end{cases} \quad (۱-۲)$$

و یا به فرم ماتریسی  $y = x - My$ ، که در آن:

$$M \triangleq \begin{bmatrix} 1 & m_{12} \\ m_{21} & 2 \end{bmatrix} \quad (۲-۲)$$

در نتیجه خواهیم داشت:

$$y = (I + M)^{-1}x \quad (۳-۲)$$

بنابراین اگر ضرایب  $m_{12}$  و  $m_{21}$  بگونه‌ای انتخاب شوند که  $I + M = A$  شود (که در آن  $A \triangleq [a_{ij}]$  ماتریس ضرایب مخلوط‌کننده است)، منابع از هم جدا خواهند شد. البته این معادلات تنها نشان می‌دهند که سیستم شکل ۲-۱-۲ قادر به جداسازی منابع است و هیچ راه عملی برای تعیین پارامترهای سیستم جداساز بدست نمی‌دهد، چراکه ماتریس مخلوط  $A$  مجهول است. سپس الگوریتم HJ (به عنوان اولین الگوریتم جداسازی منابع و اولین الگوریتمی که قابل حل بودن مساله BSS را نشان داد) بر مبنای این ایده استوار است که با توجه به اینکه منابع از هم مستقل آماری هستند، ضرایب  $m_{12}$  و  $m_{21}$  باید بگونه‌ای تعیین شوند که خروجی‌های  $y_1$  و  $y_2$  هم مستقل آماری باشند. از طرف دیگر دو تابع غیرخطی و فرد  $f$  و  $g$  را در نظر بگیرید. اگر  $E\{f(y_1)g(y_2)\}$  و  $E\{f(y_2)g(y_1)\}$  برابر صفر شوند (میانگین سیگنالها صفر فرض شده است)، از روی بسط تیلور این توابع می‌توان انتظار داشت که کلیه ممانهای متقابل (از مرتبه فرد  $y_1$  و  $y_2$ ) صفر باشند که به معنی استقلال آماری آنهاست. در نهایت هرو و ژوتن الگوریتم زیر را برای تعیین ضرایب  $m_{12}$  و  $m_{21}$  پیشنهاد کردند:

$$\begin{cases} m_{12} \leftarrow m_{12} - \mu f(y_1)g(y_2) \\ m_{21} \leftarrow m_{21} - \mu f(y_2)g(y_1) \end{cases} \quad (۴-۲)$$

که در آن عدد مثبت کوچکی است که learning rate را تعیین می‌کند. سپس هرو و ژوتن توابع فرد ساده‌ای مثل  $f(y) = y^3$  و  $g(y) = \arctan(y)$  را در نظر گرفتند و نشان دادند که این الگوریتم واقعاً قادر است سیگنالهای مخلوط را جدا کند، به عبارتی حل مساله BSS ممکن است.

زیبایی و سادگی آگوریتم HJ در حل یک مسئله ظاهراً پیچیده به تدریج توجه محققان دیگر را نیز به این مسئله جلب کرد. برخی از آنها (مثل Lacoume) در ابتدا تنها برای آنکه اشتباه بودن ادعای HJ را نشان دهند به کار روی این مسئله پرداختند، که این تلاشها در نهایت منجر به اثبات ریاضی قابل حل بودن BSS، و ارائه آگوریتم‌های بهتری برای آن شد [۲، ۱۲، ۶]. با این وجود تا میانه دهه ۱۹۹۰، این مسئله بیشتر در بین محققان فرانسوی باقی ماند و محدود مقالات بین‌المللی ارائه شده در کنفرانسهای شبکه‌های عصبی، در بین انبوه مقالات روی موضوعاتی چون back-propagation، شبکه‌های هاپفیلد و Kohonen's self organizing maps که در آن موقع مورد توجه زیاد محققان شبکه‌های عصبی بودند، مدفون شد. زمینه متفاوت دیگری که در آن موقع در حال گسترش بود، Higher Order Spectral Analysis (HOS) بود که نخستین کنفرانس آن در سال ۱۹۸۹ برگزار شد و کارهای Cardoso و Comon در این کنفرانس ارائه شدند [۲، ۶].

از حدود میانه دهه ۱۹۹۰ و بعد از آنکه Bell و Sejnowski روش خود را بر مبنای Infomax ارائه کردند [۱]، این مسئله مورد توجه بیشتر محققان قرار گرفت و آگوریتم‌های مختلفی برای حل مسئله در حالت‌های مختلف ارائه گردید. بخصوص باید به روش [۴] اشاره کرد که خانواده‌ای از روشهای equivariant برای جداسازی منابع معرفی می‌کند. در این روشها، کیفیت جداسازی به condition number ماتریس مخلوط‌کننده بستگی ندارد، یعنی هرچه هم که سیگنالها به شدت مخلوط شده باشند (خروجی سنسورها به هم شبیه باشند، یا دترمینان ماتریس مخلوط‌کننده به صفر نزدیک باشد)، تأثیری در کیفیت نهایی جواب ندارند (در عدم حضور نویز).

از حدود میانه دهه ۹۰ مقالات در این زمینه به سرعت افزایش یافت. اولین کنفرانس بین‌المللی روی این موضوع (ICA99) در سال ۹۹ در فرانسه برگزار شد که در آن بیش از یکصد محقق که روی این مساله کار می‌کردند، گرد هم آمدند. این کنفرانس از آن سال تا کنون هر ۱/۵ سال یکبار و در کشورهای مختلف برگزار می‌شود (ICA2009 قرار است در برزیل برگزار شود).

## ۳-۱-۲ کاربردهای BSS

با آنکه مساله ICA یا BSS نسبتاً مبحث جدیدی در پردازش سیگنال است، تا کنون استفاده از آن در کاربردهای مختلفی گزارش شده است. از جمله این کاربردها می‌توان موارد زیر را برشمرد:

- کاربرد در Feature extraction در پردازش تصویر.

- جداسازی تصاویر مخلوط.

- کاربرد در Denosing سیگنال تصویر.

- استفاده در جداسازی سیگنالهای پزشکی ECG، EEG و MEG.
- استفاده در حذف سروصدای ماشین از صدای ضبط شده در گوشی تلفن همراه.
- استفاده در حذف نویز و سروصدا به عنوان یک بلوک پیش پردازش در سیستمهای تشخیص صحبت (Speech recognition). با استفاده از چنین بلوکی می توان نرخ تشخیص صحبت را افزایش داد.
- حل cocktail party problem (جداسازی چند سیگنال صحبت مخلوط). این کاربرد یکی از مشکلترین کاربردهای BSS است که با آنکه برای مخلوطهای مصنوعی و سیگنالهایی که در یک اتاق آکوستیک ضبط شده اند، بخوبی کار می کند، برای جداسازی مخلوط ضبط شده در یک اتاق معمولی (وقتی از روی دیوارها اکو وجود دارد) هنوز کیفیت روشهای ارائه شده چندان بالا نیست.
- استفاده در تشخیص همزمان چند جسم در سیستمهای تشخیص شیء با استفاده از القای الکترومغناطیسی. در این سیستمها هر شخص یا شیء یک Label دارد که حضور آن در نزدیکی سنسور مربوطه باعث شناسایی شخص یا شیء می شود. با استفاده از ICA امکان identification همزمان چند label بوجود می آید (وقتی چند label در نزدیکی دستگاه تشخیص ظاهر می شوند). این کاربرد patent شده است.
- استفاده در مخابرات (CDMA).
- کاربرد در اقتصاد (استخراج عوامل پنهان در اطلاعات تجاری).
- کاربرد در شناسایی جو: یک سیگنال به طرف جو فرستاده می شود، انعکاسهای آن از روی لایه های مختلف جو با استفاده از ICA از هم جدا می شوند که هرکدام در برگیرنده اطلاعاتی در مورد لایه های مختلف جو است.
- کاربرد در زمین شناسی: مشابه روش قبل برای شناسایی لایه های مختلف زمین.
- کاربرد در ستاره شناسی: مؤلفه های مستقل تصاویر دریافتی از فضا با استفاده از ICA استخراج می شوند و از روی آنها اطلاعاتی در مورد منابع مستقلی که آنها را ارسال کرده اند بدست می آید.

## ۲-۱-۴ ICA به عنوان روشی برای حل مسأله BSS

دیدیم که ایده اصلی حل مسأله BSS استفاده از استقلال منابع و بیرون کشیدن مؤلفه های مستقل مشاهدات است. به همین دلیل، گرفتن یک بردار مشاهده و تجزیه آن به مؤلفه های مستقل را «تجزیه به مؤلفه های مستقل» یا ICA (Independent



Component Analysis) نام‌گذاری کردند. به عبارت دیگر، ICA به هر الگوریتم یا روشی اطلاق می‌شود که نمونه‌هایی از یک بردار تصادفی را به عنوان ورودی دریافت کرده، و در خروجی مؤلفه‌های مستقل آن را بدست می‌دهد، یعنی مؤلفه‌هایی می‌دهد که از یکدیگر بطور آماری مستقل هستند و بردار ورودی را می‌توان به صورت ترکیب این مؤلفه‌های مستقل بیان کرد.

این نام‌گذاری در مقایسه با تبدیل قدیمی‌تر «تجزیه به مؤلفه‌های اصلی (PCA)»<sup>۱</sup> انجام گرفته است: PCA نمونه‌های یک بردار تصادفی را دریافت کرده و تحت یک تبدیل ماتریسی دوران، خروجیهایی بدست می‌دهد که با یکدیگر ناهمبسته (decorrelated) هستند و ورودیها را می‌توان به صورت ترکیب خطی این مؤلفه‌های ناهمبسته بیان کرد.

بنابراین تفاوت PCA و ICA آن است که PCA به تبدیلی از نوع دوران محدود است ولی ICA نیست. در عوض، PCA خروجیهایی می‌دهد که از یکدیگر ناهمبسته هستند (استقلال درجه ۲)، ولی لزوماً مستقل آماری نیستند، اما ICA خروجیهایی می‌دهد که به مفهوم دقیق مستقل (و نه فقط ناهمبسته) هستند. به عنوان مثال به سادگی می‌توان نشان داد که در BSS بدست آوردن خروجی‌هایی که از هم ناهمبسته باشند برای بازیابی منابع کافی نیست و ناهمبستگی (به عنوان تقریبی از استقلال) نمی‌تواند مسأله BSS را حل کند، و برای حل این مسأله استقلال کامل نیاز است. به عبارتی نمی‌توان PCA را برای حل مسأله BSS به کار برد.

البته توجه داریم که ICA دو ابهام ذاتی نیز دارد: تغییر ترتیب مؤلفه‌های مستقل و نیز تغییر انرژی آنها تغییری در استقلال آنها نمی‌دهد. مثلاً در BSS که تنها اطلاعات ما از منابع استقلال آماری آنها است، منابع را می‌توان از روی مخلوطها به دست آورد ولی با ابهام در انرژی و ترتیب آنها؛ به عبارت دیگر، انرژی و ترتیب منابع را نمی‌توان تنها از روی فرض استقلال آماری آنها به دست آورد. البته بازیابی منابع با این دو ابهام در بسیاری از کاربردها قابل قبول است و اهمیت چندانی ندارد.

در حالتیکه تعداد سنسورها مساوی با تعداد منابع باشد، ICA متداول‌ترین روش برای BSS است. البته تعمیم ICA به حالتی که تعداد سنسورها از منابع بیشتر باشد نیز بسیار ساده است. برای مطالعه بیشتر در مورد ICA خواننده را به مقالات مروری [۱۴، ۱۳، ۱۱، ۹، ۳]، کتابهای [۵، ۱۰] و مراجع ذکر شده در آنها ارجاع می‌دهیم.

### 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، نهان نگاری به عنوان روشی مؤثر جهت تأمین برخی از این نیازها مورد توجه قرار گرفته و پیشرفت سریعی داشته است.

در این پایان نامه جهت آشنایی و نیل به یک دیدگاه کلی از سیستمهای نهان نگاری ابتدا به بیان کاربردهای نهان نگاری

پرداختیم. ...

# مراجع

- [1] T. Bell and T. Sejnowski, "An information-maximization approach to blind separation and blind deconvolution," *Neural Computation*, vol. 7, no. 6, pp. 1004–1034, 1995.
- [2] J.-F. Cardoso, "Blind identification of independent signals," in *Workshop on Higher-Order Spectral Analysis*, Vail (CO), USA, June 1989.
- [3] J.-F. Cardoso, "Blind signal separation: statistical principles," *Proceedings IEEE*, vol. 9, pp. 2009–2025, 1998.
- [4] J.-F. Cardoso and B. Laheld, "Equivariant adaptive source separation," *IEEE Trans. on SP*, vol. 44, no. 12, pp. 3017–3030, December 1996.
- [5] Andrzej Cichocki and Shun-ichi Amari, *Adaptive Blind Signal and Image Processing: Learning Algorithms and Applications*, John Wiley and sons, 2002.
- [6] P. Comon, "Separation of stochastic processes," in *Workshop on Higher-Order Spectral Analysis*, Vail (CO), USA, June 1989.
- [7] J. Héroult and C. Jutten, "Space or time adaptive signal processing by neural networks models," in *Intern. Conf. on Neural Networks for Computing*, Snowbird (Utah, USA), 1986, pp. 206–211.
- [8] J. Héroult, C. Jutten, and B. Ans, "Détection de grandeurs primitives dans un message composite par une architecture de calcul neuromimétique en apprentissage non supervisé," in *Actes du Xeme colloque GRETSI*, Nice, France, 20-24 Mai 1985, pp. 1017–1022, (in French).
- [9] A. Hyvarinen, "Survey on independent component analysis," *Neural Computing Surveys*, vol. 2, pp. 94–128, 1999.
- [10] A. Hyvarinen, J. Karhunen, and E. Oja, *Independent Component Analysis*, 2001.
- [11] A. Hyvarinen and E. Oja, "Independent component analysis: Algorithms and applications," *Neural Networks*, vol. 13, pp. 411–430, 2000.
- [12] J.-L. Lacoume and P. Ruiz, "Sources identification: a solution based on cumulants," in *IEEE ASSP Workshop*, Mineapolis, USA, August 1988.
- [13] T. W. Lee, M. Girolami, A. J. Bell, and T. J. Sejnowski, "A unifying information-theoretic framework for independent component analysis," *International Journal on Mathematical and Computer Modeling*, 1999.
- [14] A. Mansour, A. K. Barros, and N. Ohnishi, "Blind separation of sources: Methods, assumptions and applications," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. EA83A, no. 8, pp. 1498–1512, Aug 2000.

## **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 BBBB

*Supervisor:*

Dr. ...

August 2005