فهرست مطالب

عنوان	صفحه

عنوان	صفحه

پیش‌گفتار ناشر

در سال‌های اخیر، با پیشرفت روزافزون فناوری اطّلاعات و گسترش و کاربردهای این فناوری در حوزه‌های مختلف، هر روز شاهد بروز و ظهور فناوری‌های نوین وابسته در این حوزه هستیم. یکی از فناوری‌های وابسته این حوزه، فناوری‌های مربوط به نهان‌نگاری و پنهان‌سازی اطّلاعات است. نهان‌نگاری و پنهان‌سازی اطّلاعات قدمت و پیشینهٔ طولانی دارند. سابقهٔ تاریخی ثبت‌شده توسط تاریخ‌شناسان این حوزهٔ فناوری، به سال ۴۴۰ قبل از میلاد برمی‌گردد. با پیشرفت فناوری اطّلاعات و با ظهور اینترنت در دهه‌های اخیر، این موضوع رشد فزاینده‌ای داشته است. گسترش و سهل‌الوصول‌بودن دسترسی به انواع داده‌ها از طریق اینترنت، این امکان را فراهم کرده‌است که تبادل اطلاعات پنهانی نیز به سادگی در این شبکه‌ها مورد استفاده قرار گیرند. در نگاه اوّل به این فناوری، شاید چنین به‌نظر رسد که این فناوری کاربردهای صرفاً امنیتی و نظامی دارد؛ درحالی‌که علاوه‌بر کاربردهای یادشده، در دهه‌های اخیر نهان‌نگاری و پنهان‌سازی اطلاعات (ته‌نقش‌نگاری) کاربردهای فراوانی نیز در تجارت، صنعت، تبلیغات و ... پیدا کرده‌است.

اوّلین روش‌های نهان‌نگاری و پنهان‌سازی اطّلاعات دیجیتال در دههٔ ۸۰ معرفی شدند و روش‌های جدیدتر مربوط به یک دههٔ اخیر هستند. از کاربردهای نهان‌نگاری و پنهان‌سازی اطلاعات در شاخهٔ ته‌نقش‌نگاری می‌توان به بهره‌گیری از ته‌نقش‌ها در تجارت الکترونیک،

تصدیق و اعتبارسنجی، شناسایی اثبات مالکیت شخصی و وابستگی، دنبال‌کردن و پی‌گیری مشتری، نظارت بر پخش آگهی‌های تبلیغاتی و ... نام برد.

انتشارات مؤسسهٔ فرهنگی هنری جهت افزایش آگاهی‌های عمومی از طرفی و از طرف دیگر آشنایی اولیهٔ دانشجویان رشته‌های مرتبط با این فناوری و سایر علاقه‌مندان، به پیشنهاد استاد فرهیخته جناب آقای دکتر جواد شیخ‌زادگان مبنی بر تألیف کتابی تحت عنوان آشنایی با نهان‌نگاری و پنهان‌سازی اطّلاعات، تألیف و انتشار این کتاب را در دستور کار قرار داد.

مؤلّف اندیشمند این اثر پس از سال‌ها آشنایی با مباحث این حوزه و تدریس موضوعات با این فناوری در دانشگاه در تابستان سال ۱۳۹۲ تألیف این اثر را به پایان رسانیدند و در زمستان همین سال توسط این مؤسسه به زیور چاپ آراسته شد.

مؤسسهٔ فرهنگی هنری، ضمن تشکر و سپاس از جناب آقای دکتر جواد شیخ‌زادگان، مؤلّف محترم این اثر، از همهٔ کسانی که اقدامات لازم را جهت آماده‌سازی این کتاب انجام داده‌اند و هم‌چنین مسئوولان پژوهشگاه توسعهٔ فناوری‌های پیشرفته به‌خصوص ریاست محترم این پژوهشگاه، جناب آقای مهندس ابوالفضل روحانی که امکانات لازم را جهت چاپ و انتشار آن فراهم کردند، سپاس‌گزاری می‌نماید. امیدواریم مطالعهٔ این کتاب برای خوانندگانش مفید واقع شود.

انتشارات مؤسسهٔ فرهنگی هنری
پردازش هوشمند علائم
زمستان ۱۳۹۲

پیش‌گفتار مؤلّف

از روزگاران بسیار قدیم، تأمین امنیت اطّلاعات و ارتباطات در تبادل پیغام‌ها و اطّلاعات دارای طبقه‌بندی (سرّی و محرمانه) به‌ویژه در ارتباطات نظامی، امنیتی و اطّلاعاتی، از اهمیت خاصی برخوردار بوده است. با توسعه و گسترش فناوری اطّلاعات و ارتباطات در چند دههٔ اخیر و نفوذ و فراگیری آن در اکثر فعالیت‌های مدنی از قبیل فعالیت‌های اقتصادی، اجتماعی، فرهنگی، علمی و اطّلاعاتی، فضای خیلی وسیع‌تری دررابطه با موضوع امنیت اطّلاعات و ارتباطات گشوده شد و به تبع آن مسائل، نیازمندی‌ها و عرصه‌های جدیدی در این زمینه به‌وجود آمد.

می‌دانیم که در تأمین امنیت تبادل پیام‌ها و اطّلاعات ، با دو مسألهٔ اساسی روبه‌رو هستیم. مسألهٔ اوّل اینست که امنیت محتوای پیام و اطّلاعات مورد تبادل تأمین شود. این بدین معنی است که دشمن (یا به‌طور کلی افراد غیر مجاز) درصورت استراق سمع ارتباط و دریافت پیام و اطّلاعات مورد تبادل، محتوای پیام و اطّلاعات برایشان نامفهوم باشد و نتوانند از اطّلاعات مورد تبادل بهره‌برداری کنند. این مهم، با بهره‌گیری از علوم و فنون رمزنگاری

حاصل می‌شود که یکی از ابزارهای شناخته شدهٔ تأمین امنیت اطّلاعات از روزگاران خیلی قدیم است که در چند دههٔ اخیر نیز فناوری‌های مرتبط با آن به‌نحو چشم‌گیری پیشرفت کرده‌اند. مسألهٔ اساسی دوم در تأمین امنیت تبادل پیام‌ها و اطّلاعات ، تأمین امنیت خود ارتباط است به‌نحوی که دشمن متوجه تبادل پیام‌ها و اطّلاعات طبقه‌بندی‌شده نشود. این مسأله خود به دو صورت قابل طرح است: یکی این‌که دشمن نتواند وجود ارتباط را حس کرده و استراق سمع (دریافت) کند که برای نیل به این هدف، سامانه‌های LPI[1] در مخابرات امن مطرح شده و راه‌کارهای طیف گسترده[2] به‌عنوان یکی از راه‌کارهای مفید و مؤثّر جهت پیاده‌سازی سامانه‌های LPI به‌طور وسیع در چند دههٔ اخیر مورد توجه قرار گرفته است. صورت دوم اینست که دشمن به‌طور کامل قادر به حس و استراق سمع ارتباط باشد، اما ارتباط برای او عادی جلوه نماید و به‌هیچ‌وجه از پیام‌ها و اطّلاعات دریافتی، به وجود پیام یا اطّلاعات طبقه‌بندی‌شده در ارتباط پی نبرد و بدین ترتیب دشمن درصدد تخریب ارتباط نیز نخواهد بود. مورد اخیر از طریق راه‌کارهایی محقق می‌شود که تحت عنوان "نهان‌نگاری و پنهان‌سازی اطّلاعات " مورد بحث قرار می‌گیرند. نهان‌نگاری و پنهان‌سازی اطّلاعات نیز نظیر رمزنگاری قدمت زیادی دارد، اما با توسعه و گسترش شگفت‌انگیز فناوری‌های اطّلاعات و ارتباطات در دو سه دههٔ اخیر، نهان‌نگاری و پنهان‌سازی اطّلاعات دیجیتال نیز رونق دوچندان گرفته است، به‌طوری که از یک دههٔ پیش، درس "نهان‌نگاری و پنهان‌سازی اطّلاعات " به‌عنوان یک درس تخصصی – اختیاری در تعدادی از دانشگاه‌های کشورمان در برخی از گرایش‌های تعدادی از رشته‌های مهندسی نظیر مخابرات، کامپیوترو فناوری اطّلاعات (IT) ارائه می‌شود. از این‌رو و به‌دلیل عدم وجود کتابی به زبان فارسی در این زمینه، اینجانب درصدد تألیف کتاب حاضر با عنوان "آشنایی با نهان‌نگاری و پنهان‌سازی اطّلاعات " برآمدم.

این کتاب شامل چهارفصل است که در فصل اوّل کلیّات نهان‌نگاری و پنهان‌سازی اطّلاعات از قبیل تاریخچه، تعاریف، اصطلاحات، مفاهیم اساسی و از این قبیل آورده شده‌اند که در مجموع حدود ۲۵ صفحه از کتاب را تشکیل داده است. فصل دوم مربوط به پوشانه‌های (متون پوششی) نهان‌نگاری و پنهان‌سازی اطّلاعات است که در آن انواع متون پوششی که در نهان‌نگاری و پنهان‌سازی اطّلاعات مورد استفاده قرار می‌گیرند، مورد بحث قرار گرفته است. در فصل سوم روش‌ها و راه‌کارهای نهان‌نگاری و پنهان‌سازی اطّلاعات در پوشانه‌های مختلف متنی، صوتی، تصویری و ... مورد بحث و بررسی قرار می‌گیرند و درنهایت در فصل چهارم دررابطه با تهدیدها و حملات مربوط به نهان‌نگاری و پنهان‌سازی اطّلاعات مطالبی نه‌چندان ریز و تخصصی، آورده شده است.

---

1 Low Probabilily of Intercept
2 Spread Spectrum

درس نهان‌نگاری و پنهان‌سازی اطّلاعات به‌طور عمومی به‌عنوان درس تخصصی-اختیاری در مقاطع کارشناسی ارشد برخی گرایش‌های مهندسی مخابرات، مهندسی کامپیوتر و فناوری اطّلاعات پیشنهاد می‌شود؛ اما مطالب کتاب حاضر به‌نحوی تدوین شده است که برای دانشجویان مقطع کارشناسی رشته‌های مذکور نیز قابل استفاده است؛ به‌خصوص اگر این دسته از دانشجویان، آشنایی خوبی با مباحث مربوط به پردازش سیگنال‌های دیجیتال (DSP[1]) داشته باشند. امید است که با تألیف این کتاب گامی هرچند کوچک در جهت ارتقای علمی دانشجویان، دانش‌آموختگان و کارشناسان حوزهٔ امنیت اطّلاعات و ارتباطات و درنهایت در راستای پیشرفت و پیشبرد اهداف عالیهٔ آموزشی و فرهنگی کشور عزیزمان ایران برداشته باشیم.

در خاتمه لازم می‌دانم که مراتب تشکر و قدردانی خود را از زحمات بی‌شائبهٔ آقایان محمداسماعیل قاصدی، مهیار قدوسی و رسول حمیدی که در راستای آماده‌سازی کتاب، حروف‌چینی و صفحه آرایی این اثر از هیچ‌کمکی دریغ نورزیدند، اعلام نموده و از مسئوولان پژوهشگاه توسعهٔ فناوری‌های پیشرفته (خواجه نصیرالدین طوسی) نیز که حمایت‌های لازم را در راستای چاپ و نشر این کتاب به‌عمل آوردند، تشکر و سپاس‌گزاری نمایم.

والسّلام
جواد شیخ‌زادگان
زمستان ۱۳۹۲

1 Digital Signal Processing

پیش‌گفتار مؤلّف

از روزگاران بسیار قدیم، تأمین امنیت اطّلاعات و ارتباطات در تبادل پیغام‌ها و اطّلاعات دارای طبقه‌بندی (سرّی و محرمانه) به‌ویژه در ارتباطات نظامی، امنیتی و اطّلاعاتی، از اهمیت خاصی برخوردار بوده است. با توسعه و گسترش فناوری اطّلاعات و ارتباطات در چند دهۀ اخیر و نفوذ و فراگیری آن در اکثر فعالیت‌های مدنی از قبیل فعالیت‌های اقتصادی، اجتماعی، فرهنگی، علمی و اطّلاعاتی، فضای خیلی وسیع‌تری دررابطه با موضوع امنیت اطّلاعات و ارتباطات گشوده شد و به تبع آن مسائل، نیازمندی‌ها و عرصه‌های جدیدی در این زمینه به‌وجود آمد.

می‌دانیم که در تأمین امنیت تبادل پیام‌ها و اطّلاعات ، با دو مسألۀ اساسی روبه‌رو هستیم. مسألۀ اوّل اینست که امنیت محتوای پیام و اطّلاعات مورد تبادل تأمین شود. این بدین معنی است که دشمن (یا به‌طور کلی افراد غیر مجاز) درصورت استراق سمع ارتباط و دریافت پیام و اطّلاعات مورد تبادل، محتوای پیام و اطّلاعات برایشان نامفهوم باشد و نتوانند از اطّلاعات مورد تبادل بهره‌برداری کنند. این مهم، بابهره‌گیری از علوم و فنون رمزنگاری حاصل می‌شود که یکی از ابزارهای شناخته شدۀ تأمین امنیت اطّلاعات از روزگاران خیلی قدیم است که در چند دهۀ اخیر نیز فناوری‌های مرتبط با آن به‌نحو چشم‌گیری پیشرفت کرده‌اند. مسألۀ اساسی دوم در تأمین امنیت تبادل پیام‌ها و اطّلاعات ، تأمین امنیت خود ارتباط است به‌نحوی که دشمن متوجه تبادل پیام‌ها و اطّلاعات طبقه‌بندی‌شده نشود. این مسأله خود به دو صورت قابل طرح است: یکی این‌که دشمن نتواند وجود ارتباط را حس کرده و استراق سمع

(دریافت) کند که برای نیل به این هدف، سامانه‌های LPI[1] در مخابرات امن مطرح شده و راه‌کارهای طیف گسترده[2] به‌عنوان یکی از راه‌کارهای مفید و مؤثّر جهت پیاده‌سازی سامانه‌های LPI به‌طور وسیع در چند دههٔ اخیر مورد توجه قرار گرفته است. صورت دوم اینست که دشمن به‌طور کامل قادر به حس و استراق سمع ارتباط باشد اما ارتباط برای او عادی جلوه نماید و به‌هیچ‌وجه از پیام‌ها و اطّلاعات دریافتی، به وجود پیام یا اطّلاعات طبقه‌بندی‌شده در ارتباط پی نبرد و بدین ترتیب دشمن درصدد تخریب ارتباط نیز نخواهد بود. مورد اخیر از طریق راه‌کارهایی محقق می‌شود که تحت عنوان "نهان‌نگاری و پنهان‌سازی اطّلاعات " مورد بحث قرار می‌گیرند. نهان‌نگاری و پنهان‌سازی اطّلاعات نیز نظیر رمزنگاری قدمت زیادی دارد، اما با توسعه و گسترش شگفت‌انگیز فناوری‌های اطّلاعات و ارتباطات در دو سه دههٔ اخیر، نهان‌نگاری و پنهان‌سازی اطّلاعات دیجیتال نیز رونق دوچندان گرفته است، به‌طوری که از یک دههٔ پیش، درس "نهان‌نگاری و پنهان‌سازی اطّلاعات " به‌عنوان یک درس تخصصی – اختیاری در تعدادی از دانشگاه‌های کشورمان در برخی از گرایش‌های تعدادی از رشته‌های مهندسی نظیر مخابرات، کامپیوترو فناوری اطّلاعات (IT) ارائه می‌شود. از این‌رو و به‌دلیل عدم وجود کتابی به زبان فارسی در این زمینه، اینجانب درصدد تألیف کتاب حاضر با عنوان "آشنایی با نهان‌نگاری و پنهان‌سازی اطّلاعات " برآمدم.

این کتاب شامل چهارفصل است که در فصل اوّل کلیّات نهان‌نگاری و پنهان‌سازی اطّلاعات از قبیل تاریخچه، تعاریف، اصطلاحات، مفاهیم اساسی و از این قبیل آورده شده‌اند که در مجموع حدود ۲۵ صفحه از کتاب را تشکیل داده است. فصل دوم مربوط به پوشانه‌های (متون پوششی) نهان‌نگاری و پنهان‌سازی اطّلاعات است که در آن انواع متون پوششی که در نهان‌نگاری و پنهان‌سازی اطّلاعات مورد استفاده قرار می‌گیرند، مورد بحث قرار گرفته است. در فصل سوم روش‌ها و راه‌کارهای نهان‌نگاری و پنهان‌سازی اطّلاعات در پوشانه‌های مختلف متنی، صوتی، تصویری و ... مورد بحث و بررسی قرار می‌گیرند و نهایتاً در فصل چهارم دررابطه با تهدیدات و حملات مربوط به نهان‌نگاری و پنهان‌سازی اطّلاعات مطالبی نه‌چندان ریز و تخصصی، آورده شده است.

درس نهان‌نگاری و پنهان‌سازی اطّلاعات عموماً به‌عنوان درس تخصصی – اختیاری در مقاطع کارشناسی ارشد برخی گرایش‌های مهندسی مخابرات، مهندسی کامپیوتر و فناوری اطّلاعات پیشنهاد می‌شود؛ اما مطالب کتاب حاضر به‌نحوی تدوین شده است که برای دانشجویان مقطع کارشناسی رشته‌های مذکور نیز قابل استفاده است؛ به‌خصوص اگر این دسته از دانشجویان، آشنایی خوبی با مباحث مربوط به پردازش سیگنال‌های دیجیتال (DSP[3]) داشته

---

1 Low Probabilily of Intercept
2 Spread Spectrum
3 Digital Signal Processing

باشند. امید است کـه بـا تـألیف ایـن کتـاب گـامی هرچنـد کوچـک در جهـت ارتقـای علمـی دانشجویان، دانش‌آموختگان و کارشناسان حوزهٔ امنیـت اطّلاعـات و ارتباطـات و در نهایـت در راستای پیشرفت و پیشبرد اهداف عالیه آموزشـی و فرهنگـی کشـور عزیزمـان ایـران برداشـته باشیم.

در خاتمه لازم می‌دانم که مراتب تشکر و قدردانی خود را از زحمـات بـی‌شـائبهٔ آقایـان محمداسماعیل قاصدی، مهیار قدوسی و رسول حمیـدی کـه در راسـتای آمـاده‌سـازی کتـاب، حروف‌چینی و صفحه آرایی این اثر از هیچ‌کمکی دریـغ نورزیدنـد، اعـلام نمـوده و از مسـؤولان پژوهشگاه توسعهٔ فناوری‌های پیشرفته (خواجه نصیرالدین طوسی) نیز که حمایـت‌هـای لازم را درراستای چاپ و نشر این کتاب به‌عمل آوردند، تشکر و سپاس‌گزاری نمایم.

والسّلام
جواد شیخ‌زادگان
زمستان ۱۳۹۲