
بسم الله الرحمن الرحيم

دانشکده مهندسی برق و کامپیوتر

پایان‌نامه

بررسی حملات تبانی جدید در واترمارکینگ ویدیو

Investigation of new collusion attacks in video watermarking

در رشته‌ی

مهندسی برق- مخابرات سیستم

بوسیله‌ی

علی امیرحمیدی جهرمی

استاد راهنما

دکتر علیرضا ذوالقدر اصلی

شهریور ۹۱

اظهارنامه

اینجانب علی امیرحمیدی جهرمی (۸۸۰۶۵۱) دانشجوی رشته برق- مخابرات گرایش سیستم دانشکده‌ی برق و کامپیوتر اظهار می‌کنم که این پایان‌نامه حاصل پژوهش خودم بوده و در جاهایی که از منابع دیگران استفاده کرده‌ام، نشانی دقیق و مشخصات کامل آن را نوشته‌ام. همچنین اظهار می‌کنم که پایان‌نامه و موضوع پایان‌نامه‌ام تکراری نیست و تعهد می‌نمایم که بدون مجوز دانشگاه دستاوردهای آن را منتشر ننموده و یا در اختیار غیر قرار ندهم. کلیه حقوق این اثر مطابق با آیین‌نامه‌ی مالکیت فکری و معنوی متعلق به دانشگاه شیراز است.

علی امیرحمیدی جهرمی

به نام خدا

بررسی حملات تبانی جدید در واترمارکینگ ویدیو

به کوشش

علی امیرحمیدی جهرمی

پایان نامه

ارائه شده به تحصیلات تکمیلی دانشگاه شیراز به عنوان بخشی

از فعالیت‌های تحصیلی لازم برای اخذ درجه کارشناسی ارشد

در رشته‌ی:

مهندسی برق- مخابرات سیستم

از دانشگاه شیراز

شیراز

جمهوری اسلامی ایران

ارزیابی کمیته پایان‌نامه، با درجه‌ی: بسیار خوب

دکتر علیرضا ذوالقدر اصلی، دانشیار بخش مخابرات و الکترونیک(رئیس کمیته) .....

دکتر مهران یزدی، دانشیار بخش مخابرات و الکترونیک .....

دکتر محمد علی مسندی شیرازی، استاد بخش مخابرات و الکترونیک .....

شهریور ۱۳۹۱

تقدیم به :

پدر عزیزم

کوه صبر واستقامت، کسی که شمع هستی‌اش را برای روشنی وجودم افروخته و همیشه مدیون زحماتش خواهم بود.

مادر فداکارم

که خود سوخت تا روشنی بخش راه زندگی‌ام شود. یادی باشد از دریای بیکران محبت‌هایش.

سپاسگزاری

خداوند سبحان را حمد گویم که جز او معبودی نیست و تمام ستایش ها مخصوص اوست. حمد و سپاس آن خدایی را که به ما عقل داد و از طریق عقل به ما علم آموخت. ستایش مخصوص آن خدایی است که فراموش نکند هرکه را که یادش کند و نعمتش را از کسی که سپاسگزاری کند کم نکند. خدایا تو را سپاس که به ما نعمت بزرگی عنایت کردی که محبت خاندان عصمت وطهارت (علیهم السلام) را در قلب ما جا دادی، سلام و درود بی پایان بر محمد(ص) و آل و اصحابش باد.

اکنون که این پایان نامه به اتمام رسیده است بر خود فرض می‌دانم که از استاد گرامی، جناب آقای دکتر علیرضا ذوالقدر اصلی که همانند پدری دلسوز با کمک‌ها و راهنمایی‌های بیدریغ خود، مرا در سرانجام رساندن این پایان‌نامه یاری کردند، کمال تشکر و قدردانی را داشته باشم.

همچنین لازم است تا از اساتید محترم مشاور جناب آقای دکتر مهران یزدی و جناب آقای دکتر محمد علی مسندی شیرازی که راهنمایی‌هایشان همواره گره‌گشا بوده است، تشکرهای ویژه‌ای را داشته باشم.

همچنین قدردان تمامی دوستانی هستم که در مراحل انجام پایان‌نامه همراه و راهنمای من بوده‌اند.

در نهایت از خانواده و بویژه پدرم که همواره در این مسیر مشوق بنده بوده‌اند، صمیمانه‌ترین تشکرها و سپاس‌ها را دارم.

باشد که فرصت جبران باقی باشد.

این پایان‌نامه از طرح حمایت مرکز تحقیقات مخابرات ایران از اجرای پروژه‌های کارشناسی ارشد بر طبق قرارداد شماره ۵۰۰/۱۳۲۲۶/ت بهره‌مند گردیده است.

چکیده

بررسی حملات تبانی جدید در واترمارکینگ ویدیو

توسط

علی امیرحمیدی جهرمی

با گذشت بیش از یک دهه از ظهور واترمارکینگ دیجیتال، این صنعت هنوز هم به عنوان یک صنعت جوان مطرح است. با وجود اینکه به طور گسترده در کاربردهای مربوط به امنیت از قبیل حفاظت از حق مؤلف مورد استفاده قرار گرفته است اما مطالعات کمی بر روی سالم باقی ماندن واترمارک‌های جایگذاری شده در محیط‌های خصومت‌آمیز انجام شده است. در این پایان‌نامه نشان داده می‌شود که کمبود چنین ارزیابی‌هایی منجر به نقص‌های امنیتی در برابر تحلیل‌های آماری از قبیل حملات تبانی می‌شود. چنین حملاتی چندین سند واترمارک شده را در نظر می‌گیرند و از ترکیب کردن آن‌ها با یکدیگر برای تهیه یک محصول بدون واترمارک استفاده می‌کنند. این خطر با در نظر گرفتن ویدیوی دیجیتال بیشتر می‌شود چرا که هر یک از فریم‌های تنهای ویدیو را می‌توان به عنوان یک سند واترمارک شده در نظر گرفت. برای مقابله با چنین ضعف‌هایی روش‌ها و ابزارآلاتی تولید شده است. از مهم‌ترین روش‌هایی که دراینجا مورد بررسی قرار می‌گیرد واترمارکینگ جبران‌سازی حرکت است که از آن برای تولید واترمارک‌هایی که توانایی مقابله با انواع حملات را دارد، استفاده می‌شود.

کلمات کلیدی: واترمارکینگ دیجیتال[1]، ویدیوی دیجیتال[2]، امنیت[3]، تبانی[4]، واترمارکینگ جبران‌سازی حرکت[5]

---

[1] Digital Watermarking
[2] Digital Video
[3] Security
[4] Collusion
[5] Motion Compensated Watermarking

فهرست مطالب

فهرست جداول

فهرست شکل‌ها

فصل ۱

۱- مقدمه

با قرار دادن یک اسکناس معمولی در برابر نور، واترمارکی در آن مشاهده می‌شود. این واترمارک[1] در حالت معمولی، نامرئی بوده و متناسب با هدفی که برای آن جایگذاری شده است، حاوی مقداری اطلاعات می‌باشد. به همین دلیل است که واترمارک‌های دو نوع اسکناس مختلف با یکدیگر متفاوتند، از این تکنیک‌های قدیمی برای محافظت از اسکناس‌ها در برابر روش‌های ابتدایی جعل، استفاده می‌شود.

از آنجایی که در چند سال گذشته استفاده و توزیع اطلاعات دیجیتال گسترش یافته است، به نظر می‌رسد که مکانیسم‌های سنتی حفاظت به اندازه ی کافی کارآمد نیستند، برای حفاظت از حق مؤلف[2] نیاز به ابزارهای جدیدی می‌باشد. بنابراین فیزیولوژی واترمارک کاغذ گذشته به اطلاعات دیجیتال انتقال داده شد، در اصطلاح، واترمارگینگ دیجیتال[3]، به هنر مخفی سازی اطلاعات همراه با مقاومت و نامرئی بودن گفته می‌شود. اگر چه واترمارکینگ دیجیتال به نسبت یک تکنولوژی جدید می‌باشد اما بسیاری از صنایع شروع به استفاده‌های تجاری گسترده از آن کرده اند.

۱-۱ واترمارکینگ دیجیتال

در انتهای قرن گذشته میلادی، اطلاعات از آنالوگ به دیجیتال تبدیل شدند و ابزارهای دیجیتال مثلCD های صوتی، DVD ها و اینترنت، رشد قابل توجهی داشتند. اما، صاحبان فیلم‌ها و موزیک‌ها علاقه‌ی چندانی به پخش دیجیتال آثار خود نداشتند چرا که اگر این محتویات دیجیتال بدون حفاظت می‌بودند سریعاً و در مقیاس زیاد کپی شده و به آسانی و بدون هیچگونه محدودیتی توزیع می‌شدند. حفاظت از محتویات دیجیتال برای مدتی طولانی بوسیله رمزنگاری[4] انجام می‌گرفت اما مشخص شد که

---

[1] Watermark
[2] Copyright
[3] Digital Watermarking
[4] Encryption

رمزنگاری به تنهایی نمی‌تواند گزینه مناسبی برای حفاظت از اطلاعات دیجیتال آن هم برای مدت زمان زیادی، باشد چرا که دیر یا زود محتویات دیجیتال رمزگشایی[1] شده و به راحتی در اختیار کاربران قرار می‌گیرند. در بسیاری از موارد محصولاتی که به روش رمزنگاری محافظت می‌شده اند حفاظت از آنها مدت زیادی طول نکشیده و کاربران توانسته اند آن‌ها را کپی و توزیع نمایند.

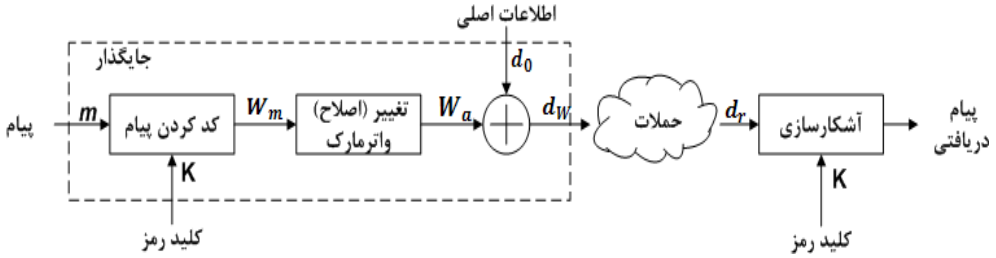
بنابراین واترمارکینگ دیجیتال به عنوان تکنولوژی حفاظتی، جایگزین دیگر تکنولوژی‌ها شد. ایده واترمارکینگ دیجیتال بر اساس مخفی سازی اطلاعات غیرقابل مشاهده در محتویات دیجیتال می‌باشد، این سیگنال واترمارک بایستی بعد از پردازش‌های سیگنالی ابتدایی که روی محتویات دیجیتال صورت می‌گیرد، سالم باقی مانده و همچنین در برابر پردازش‌هایی که برای حذف آن (واترمارک) انجام می‌گیرد، در صورت امکان مقاومت نماید.

فهم این نکته مهم است که واترمارکینگ دیجیتال جایگزین رمزنگاری نشده است بلکه هر دوی آنها تکنیکی مجزا هستند. از یک طرف، رمزنگاری از دسترسی کاربر به محتویات دیجیتالی که اجازه‌ای در مورد آن ندارد جلوگیری می‌کند و(به طور مشخص موقع ارسال) و از طرف دیگر واترمارکینگ دیجیتال، یک سند نامرئی در اطلاعات دیجیتال قرار می‌دهد تا کاربری که اجازه‌ی دسترسی به اطلاعات (به طور مشخص بعد از رمزگشایی) را دارد، استفاده‌ی غیرقانونی و غیر مجاز از این اطلاعات نکند (مثل تکثیر اطلاعات). بر اساس این نوع اطلاعاتی که در زمان پردازش استخراج در دسترس هست، آشکار سازی[2] واترمارک‌ها به دو دسته مجزا تقسیم می‌شود. اگر آشکار ساز هم به اطلاعات اصلی[3] وهم به اطلاعات واترمارک دسترسی داشته باشد، آشکار ساز واترمارک غیرکور[4] نامیده می‌شود. امروزه این نوع الگوریتم‌ها خیلی کم مورد استفاده قرار می‌گیرند چرا که نگه داشتن نسخه‌ی اصلی اطلاعات دیجیتال نیاز به فضا و حافظه ی زیادی دارد.

---

[1] Decryption
[2] Detection
[3] Orginal Data
[4] Non- Blind

بنابراین بیشتر آشکارسازهای واترمارک، از نوع کور[1] می‌باشند. یعنی، آشکارساز برای استخراج پیام مخفی تنها به اطلاعات واترمارک دسترسی دارد.



شکل ۱-۱- شمای کلی واترمارکینگ کور

۱-۱-۱ واترمارکینگ کور

شکل ۱-۱، شمای یک واترمارکینگ ساده با آشکارساز کور را نشان می‌دهد. هدف، جایگذاری پیام m در اطلاعات اصلی d_o می‌باشد. مرحله‌ی اول، رمزنگاری پیام می‌باشد تا پیام، به یک پیام مخفی با کلید رمز[2] K تبدیل شود. در ابتدا، از پیام نمونه برداری می‌شود تا از لحاظ بُعد[3] با بُعد اطلاعات اصلی مطابقت داشته باشد و همچنین پیام با یک نویز شبه تصادفی[4] XOR می‌شود تا یک سری عدد شبه تصادفی تولید گردد که این اعدد به عنوان کلید رمز K در ورودی در نظر گرفته می‌شوند، سپس سیگنال واترمارک تولید شده w_m تغیر داده می‌شود، یعنی، بوسیله‌ی ضریب واترمارکینگ، تغییر مقیاس داده می‌شود و در مرحله ی آخر، واترمارک اصلاح شده‌ی w_a به سادگی به اطلاعات اصلی اضافه می‌گردد تا اطلاعات واترمارک شده d_w تولید گردد. این نوع جایگذاری واترمارک می‌تواند در اکثر حوزه‌های مطلوب از قبیل فضایی[5]، تبدیل فوریه سریع (FFT[6]) و تبدیل کسینوسی مجزا (DCT[7]) اجرایی گردد، سپس اطلاعات واترمارک شده ارسال می‌گردد و در این جاست که به عملگرهای پردازش سیگنال‌های

---

[1] Blind
[2] Secret Key
[3] Dimension
[4] Pseudo- random
[5] Spatical
[6] Fast Fourier Transform
[7] Discrete Cosine Transform

متفاوت از قبیل فشرده سازی با از دست دادن اطلاعات[1]، اضافه کردن نویز و فیلتر کردن اجازه داده می‌شود تا روی این اطلاعات کار کنند. این نوع پردازش‌ها را می‌توان به عنوان حملاتی که سیگنال واترمارک را تهدید می‌کنند در نظر گرفت. برای فهمیدن این که آیا واترمارکی با کلید رمز K در اطلاعات دریافتی d_r جایگذاری شده است یا نه، اغلب الگوریتم‌های آشکار سازی از محاسبه‌ی ضریب همبستگی[2] بین اطلاعات دریافتی d_r و واترمارک تولید شده w_m استفاده می‌کنند. سرانجام، این ضریب همبستگی با یک مقدار آستانه[3] مقایسه می‌شود تا بتوان در مورد حضور یا عدم حضور واترمارک اظهار نظر کرد.

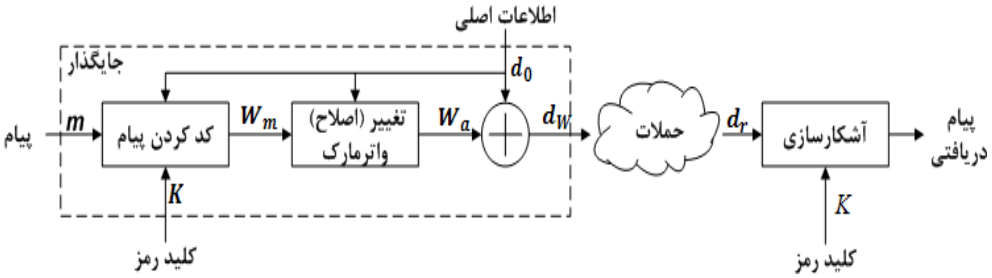
۱-۱-۲ واترمارکینگ غیر کور

در سال‌های اخیر، ضرورت ایجاد روش‌ها و گرایش‌های جدید در صنعت واترمارکینگ به خوبی دیده می‌شود. در حال حاضر به پروسه واترمارکینگ به دید انتقال یک سیگنال از میان یک کانال نویزی و به اطلاعات اصلی به دید نویز تداخلی که از مقدار قابلیت اعتماد به اطلاعات واترمارک می‌کاهد، نگاه می‌شود. در این دیدگاه جدید، Chen و Wornell از مقاله با ارزشی که توسط Costa نوشته شده است استفاده کردند[۱]. او نشان داده است که، اگر یک پیام از طریق کانالی ارسال شود که توسط دو منبع متوالی نویز سفید گوسی جمع شونده[4] تحت تأثیر قرار گرفته است و فرستنده، منبع نویز اول را می‌شناسد، این منبع نویز اول هیچ تأثیری بر روی ظرفیت[5] کانال ندارد. از دیدگاه واترمارکینگ، پیام را می‌توان به عنوان واترمارک و منبع نویز شناخته شده اول را به عنوان اطلاعات اصلی و منبع نویز نا شناخته دوم را به عنوان حملات[6] در نظر گرفت. حتی اگر مدل Costa به طور مشخص با سیستم واترمارکینگ واقعی متفاوت باشد، این

---

[1] Lossy Compression
[2] Correlation Score
[3] Threshold
[4] Additive White Gaussian Noise
[5] Capacity
[6] Attacks

بدان معنی است که، اطلاعات جانبی جایگذار، منجر به کاهش تداخل با اطلاعـات اصـلی می‌شود. در شکل ۱-۱، می‌توان جایگذار را کور در نظر گرفت، چرا که اطلاعات اصـلی در زمان کُد کردن پیام و مراحل ایجاد واترمارک مـورد اسـتفاده قـرار نگرفتـه اسـت. مـدل Costa، به طراحی یک الگوریتم جدید بر اساس شکل ۱-۲ کمک می‌کند که از اطلاعـات جانبی در طول اجرایی شدن دو مرحله فوق استفاده شده است. واترمارکینگ غیر کـور را می‌توان در زمان کُد کردن پیام (کُد کردن غیر کور) و یا ایجاد واترمارک (جایگذاری غیر کور)، اجرایی کرد. با کُـد کـردن غیـر کـور ، بـرای یـک پیـام معـین، یـک مجموعـه از واترمارک‌های متفاوت در دسترس است و جایگذار، یکی از آن‌ها را که تداخل کمتری بـا اطلاعات اصلی دارد انتخاب می‌کند. هدف از جایگذاری غیر کور ، ایجـاد یـک واترمـارک بهینه است تا آشکار ساز بتواند پیام مد نظر را استخراج نماید.



شکل ۱-۲- شمای واترمارکینگ غیر کور

۱-۲ برخی از خصوصیات واترمارکینگ

در مقالات متعدد در مورد خواص سیستم های واترمارک بحـث شـده اسـت، در عمـل تقریباً غیرممکن است که بتوان یک سیستم واترمارکینگ طراحی کرد که تمـام خـواص مطلوب را داشته باشد، از این رو بایستی با توجـه بـه کـاربرد، در مـورد اهمیـت خـواص تصمیم گرفته شود. در واترمارکینگ دیجیتال، یک مبادله پیچیده بین سـه پـارامتر نـرخ