

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ



دانشکده مهندسی برق و کامپیوتر

پایان نامه

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

اظہار نامہ

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

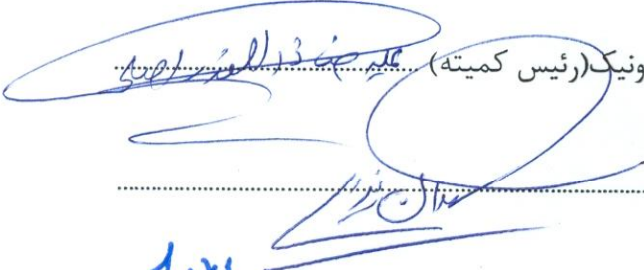
مهندسی برق - مخابرات سیستم

از دانشگاه شیراز

شیراز

جمهوری اسلامی ایران

ارزیابی کمیته پایان نامه، 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 ستایش‌ها 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 هر که 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 و طهارت (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 تنه‌های 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 در اینجا 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^۱، ویدیوی دیجیتال^۲، امنیت^۳، تبانی^۴، واترمارکینگ جبران‌سازی حرکت^۵

¹ Digital Watermarking

² Digital Video

³ Security

⁴ Collusion

⁵ Motion Compensated Watermarking

فهرست مطالب

۲	۱- مقدمه.....
۲	۱-۱-۱ واترمارکینگ دیجیتال.....
۴	۱-۱-۱-۱ واترمارکینگ کور.....
۵	۱-۱-۱-۲ واترمارکینگ غیر کور.....
۶	۲-۱ برخی از خصوصیات واترمارکینگ.....
۷	۱-۲-۱ نرخ داده.....
۷	۲-۲-۱ شباهت به اصل و مبدأ.....
۸	۳-۲-۱ مقاومت.....
۸	۳-۱ بخش بندی پایان نامه.....
۱۱	۲- کاربردها، طرح‌های کلی و چالش‌های واترمارکینگ ویدیو.....
۱۱	۱-۲ کاربردها.....
۱۲	۱-۱-۲ پنهان نگاری.....
۱۴	۲-۱-۲ مخفی سازی اطلاعات.....
۱۴	۱-۲-۱-۲ برچسب زنی برای بازیابی اطلاعات.....
۱۵	۲-۲-۱-۲ مخفی سازی اطلاعات برای فشرده سازی آنها.....
۱۶	۳-۲-۱-۲ مخفی سازی اطلاعات برای بازیابی خطا.....
۱۷	۳-۱-۲ حفاظت از حق مالکیت معنوی.....
۱۸	۱-۳-۱-۲ اثبات مالکیت.....
۱۹	۲-۳-۱-۲ کنترل دسترسی.....
۱۹	• سیستم به هم ریختن محتویات (CSS).....
۲۰	• سیستم حفاظتی آنالوگ (APS).....
۲۰	• سیستم مدیریت تولید کپی (CGMS).....

- پنج شرکت (5c) ۲۰
- واترمارکینگ ۲۱
- شناساگر فیزیکی ۲۱
- ۳-۳-۱-۲ نظارت بر پخش ۲۱
- ۴-۳-۱-۲ اثر انگشت ۲۳
- ۱-۴-۳-۱-۲ تعقیب مشتری خرابکار ۲۴
- ۱-۴-۳-۱-۲ سینمای دیجیتال ۲۶
- ۵-۳-۱-۲ تصدیق و تایید کردن ۲۶

- ۲-۲ طرح‌های کلی ۲۸**
- ۱-۲-۲ از واترمارکینگ تصاویر تا واترمارکینگ ویدیو ۲۹
- ۲-۲-۲ کامل کردن بُعد زمانی ۳۰
- ۱-۲-۲-۲ ویدیو به عنوان یک سیگنال تک بُعدی ۳۱
- ۲-۲-۲-۲ ویدیو به عنوان یک سیگنال زمانی ۳۴
- ۳-۲-۲-۲ ویدیو به عنوان یک سیگنال سه بُعدی ۳۵
- ۳-۲-۲ استفاده از فرمت‌های فشرده سازی ویدیو ۳۶
- ۱-۳-۲-۲ تغییر ضرایب درحوزه تبدیل ۳۷
- ۲-۳-۲-۲ تغییر اطلاعات حرکتی ۳۹

- ۳-۲ چالش‌ها ۴۰**
- ۱-۳-۲ پردازش‌های ابتدایی و غیرخصلانه ویدیو ۴۱
- ۱-۱-۳-۲ حملات فتومتریک (مربوط به شدت نور پیکسل‌ها) ۴۱
- ۲-۱-۳-۲ دسنکرون سازی فضایی ۴۲
- ۳-۱-۳-۲ دسنکرون سازی زمانی ۴۲
- ۴-۱-۳-۲ ویرایش ویدیو ۴۳
- ۲-۳-۲ سنکرون سازی زمانی ۴۳
- ۱-۲-۳-۲ کلید زمان بندی ۴۴
- ۲-۲-۳-۲ واترمارکینگ وابسته فریمی ۴۶
- ۳-۳-۲ ارزیابی اعوجاج ۴۷
- ۴-۳-۲ واترمارکینگ بلادرنگ ۴۸

- ۴۸ الگوریتم‌هایی با پیچیدگی کم..... ۱-۴-۳-۲
- ۴۹ پیش پردازش برای جایگذاری آسان واترمارک..... ۲-۴-۳-۲
- ۵۱ امنیت و حملات تبانی..... ۵-۳-۲
- ۵۲ اطمینان و اعتماد در محیط‌های خصومت آمیز..... ۱-۵-۳-۲
- ۵۳ امنیت نسبت به مقاومت..... ۲-۵-۳-۲
- ۵۶ بررسی مختصر انواع حملات..... ۱-۲-۵-۳-۳-۲
- ۵۶ فشرده‌سازی همراه با تلفات:.....
- ۵۷ فیلترینگ پایین گذر.....
- ۵۷ چرخش (Rotation).....
- ۵۷ تغییر اندازه (Scaling).....
- ۵۷ حذف قسمتی از تصویر (Cropping).....
- ۵۸ یکنواخت‌سازی هیستوگرام.....
- ۵۹ تصحیح گاما.....
- ۵۹ تغییر اندازه دوباره.....
- ۵۹ جایگذاری دوباره واترمارک.....
- ۶۱ امنیت در جهان واقعی..... ۳-۵-۳-۲
- ۶۳ حملات تبانی..... ۴-۵-۳-۲

۳- طرح‌های اصلی واترمارکینگ ویدیو و حملات تبانی پایه..... ۶۷

- ۶۷ ۱-۳ چارچوب مبنا.....
- ۶۸ ۱-۱-۳ واترمارکینگ فریم به فریم.....
- ۶۹ ۱-۱-۳-۳ سیستم SS.....
- ۷۰ ۲-۱-۳-۳ سیستم SS-1.....
- ۷۱ ۲-۱-۳ حملات تبانی پایه.....
- ۷۳ ۱-۲-۱-۳ میانگین گیری زمانی فریم‌ها (TFA).....
- ۷۴ ۲-۲-۱-۳ مدولاسیون دوباره تخمین واترمارک (WER).....
- ۷۶ ۲-۳ انتخاب گزینشی بین واترمارک‌های متعامد.....
- ۷۶ ۱-۲-۳ سیستم SS-N.....

۲-۲-۳ افزایش امنیت ۷۸

۳-۲-۳ نتایج آزمایش‌ها ۸۱

۴- بررسی یک حمله‌ی جدید و ارائه روش مقابله با آن ۸۶

۱-۴ ایجاد اختلال در کانال واترمارکینگ ۸۶

۱-۱-۴ میانگین گیری زمانی فریم بعد از ثبت (TFAR) ۸۷

۱-۱-۴-۱ تشریح حمله ۸۸

۱-۱-۴-۲ ارزیابی TFAR ۹۲

۲-۴ واترمارکینگ جبران سازی حرکت ۹۵

۱-۲-۴ واترمارکینگ با استفاده از موزائیک کردن ویدیو (SS-Reg) ۹۶

۱-۱-۲-۴ جایگذاری واترمارک ۹۶

۲-۱-۲-۴ آشکارسازی واترمارک ۹۹

۲-۲-۴ آنالیز سیستم ۹۹

۱-۲-۲-۴ افزایش امنیت ۱۰۰

۵- نتیجه گیری و پیشنهادات ۱۰۴

۱-۵ نتیجه گیری ۱۰۴

۲-۵ پیشنهادات ۱۰۵

مراجع ۱۰۶

فهرست جداول

- جدول ۱-۲- کاربردهای واترمارکینگ ویدیو و هدفهای مرتبط با آنها..... ۱۲
- جدول ۲-۲- ویژگیها و محدودیت‌های روش‌های مختلف واترمارکینگ ویدیو..... ۲۹
- جدول ۱-۳- خصوصیات ویدیوهایی که برای آزمایش‌ها در نظر گرفته شده‌اند..... ۸۱
- جدول ۲-۳- اثر حمله TFA بر ویدیوهای واترمارک شده..... ۸۳
- جدول ۳-۳- اثر حمله WER بر ویدیوهای واترمارک شده..... ۸۴

فهرست شکل‌ها

- شکل ۱-۱- شمای کلی واترمارکینگ کور..... ۴
- شکل ۲-۱- شمای واترمارکینگ غیر کور..... ۶
- شکل ۳-۱- مبادله در واترمارکینگ دیجیتال..... ۷
- شکل ۱-۲- استراتژی‌های متفاوت واترمارکینگ برای محافظت از ویدیو..... ۲۵
- شکل ۲-۲- فریم‌های اصلی و دست کاری شده..... ۲۸
- شکل ۳-۲- پیمایش خطی یک ویدیو..... ۳۲
- شکل ۴-۲- روند جایگذاری DEW..... ۳۸
- شکل ۵-۲- انواع کلیدهای زمان بندی برای واترمارکینگ ویدیو. به ازای هر حالت S_i از یک کلید جایگذاری یک تابع متناظر وجود دارد و فرض می‌شود که جایگذار با حالت S_k شروع می‌کند و K کلید رمز می‌باشد..... ۴۵
- شکل ۶-۲- بیان ژئومتریک استراتژی‌های مختلف جایگذاری زمانیکه آشکارساز همبستگی خطی در نظر گرفته شود. خط عمودی محدوده آشکارسازی در فضای رسانه را مشخص می‌کند. دایره‌های خالی بیانگر محتویات واترمارک نشده و دایره‌های توپر بیانگر محتویات واترمارک شده می‌باشند..... ۵۱
- شکل ۷-۲- دسته بندی حملات واترمارکینگ بسته به اینکه جزء مقاومت باشند یا امنیت..... ۵۴
- شکل ۸-۲: نمونه‌ای از تصاویر فشرده‌سازی: الف) عکس اصلی با فرمت BMP ب) فشرده‌سازی JPEG با ضریب کیفیت ۹۰٪..... ۵۶
- شکل ۹-۲: فیلترینگ پایین‌گذر: الف) تصویر اصلی ب) فیلتر پایین‌گذر گوسی با $(\Sigma=1.0)$ ۵۷
- شکل ۱۰-۲: مثال‌هایی از حمله ژئومتریک: الف) تصویر اصلی ب) تصویر تغییر اندازه یافته پ) چرخش تصویر ت) حذف قسمت‌هایی از تصویر در تمامی جهات ث) حذف قسمت‌هایی از تصویر فقط در گوشه‌ها..... ۵۸
- شکل ۱۱-۲: نمونه‌های متفاوتی از اعمال حملات بر روی تصویر LENA..... ۶۰
- شکل ۱۲-۲- تبابی در واترمارکینگ. مهاجمان چندین سند واترمارک شده را جمع آوری و ترکیب می‌کنند تا یک محصول دیجیتال بدون واترمارک را تهیه کنند..... ۶۵
- شکل ۱-۳- سیستم SS: یک واترمارک متفاوت در هر یک از فریم‌های ویدیو جایگذاری می‌شود..... ۶۸
- شکل ۲-۳- سیستم SS-1: واترمارک مرجع یکسانی در هر یک از فریم‌های ویدیو جایگذاری می‌شود..... ۷۱
- شکل ۳-۳- تشریح بصری حملات تبابی اصلی..... ۷۲

- شکل ۳-۴- سیستم SS-N: جایگذار یک واترمارک را که به صورت تصادفی از مجموعه N واترمارک مرجع انتخاب شده است را جایگذاری می کند..... ۷۸
- شکل ۳-۵- نحوه عملکرد سه طرح واترمارکینگ موجود (SS و SS-1 و SS-N) در برابر حملات تبانی WER و TFA..... ۸۲
- شکل ۴-۱- میانگین گیری زمان فریم بعد از ثبت (TFAR): مرحله A) در ابتدا اشیاء ویدیو حذف می شوند. مرحله B) فریم های همسایه ثبت می شوند. مرحله C) با هم ترکیب می شوند تا بتوان پس زمینه فریم فعلی را تخمین زد. مرحله D) اشیاء حذف شده ویدیو دوباره جایگذاری می شوند. در اینجا اندازه پنجره زمانی متوسط w برابر با یک می باشد..... ۹۰
- شکل ۴-۲- اثر جایگذاری TFAR بر سیستم های SS و SS-..... ۹۴
- شکل ۴-۳- روند جایگذاری واترمارکینگ برای حرکت دوربین (SS-REG): بخشی از الگوی واترمارک که با فریم ویدیویی فعلی مرتبط است بازیابی شده و دوباره ثبت می شود و سپس در قسمت پس زمینه فریم ویدیویی جایگذاری می شود..... ۹۸
- شکل ۴-۴- اثر TFAR بر سیستم SS-REG..... ۱۰۱

فصل ۱

۱- مقدمه

با قرار دادن یک اسکناس معمولی در برابر نور، واترمارکی در آن مشاهده می‌شود. این واترمارک^۱ 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 اندازه‌ی کافی کارآمد نیستند، برای حفاظت از حق مؤلف^۲ نیاز به ابزارهای جدیدی می‌باشد. بنابراین فیزیولوژی واترمارک کاغذ گذشته به اطلاعات دیجیتال انتقال داده شد، در اصطلاح، واترمارکینگ دیجیتال^۳، 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 کرده‌اند.

۱-۱ واترمارکینگ دیجیتال

در انتهای قرن گذشته میلادی، اطلاعات از آنالوگ به دیجیتال تبدیل شدند و ابزارهای دیجیتال مثل CD 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^۴ انجام می‌گرفت اما مشخص شد که

^۱ Watermark

^۲ Copyright

^۳ Digital Watermarking

^۴ 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^۱ 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^۲ واترمارک‌ها به دو دسته مجزا تقسیم می‌شود. اگر آشکار ساز هم به اطلاعات اصلی^۳ وهم به اطلاعات واترمارک دسترسی داشته باشد، آشکار ساز واترمارک غیرکور^۴ نامیده می‌شود. امروزه این نوع الگوریتم‌ها خیلی کم مورد استفاده قرار می‌گیرند چرا که نگه داشتن نسخه‌ی اصلی اطلاعات دیجیتال نیاز به فضا و حافظه‌ی زیادی دارد.

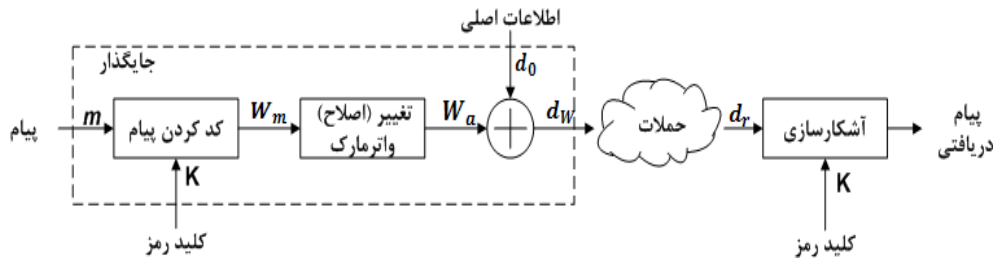
¹ Decryption

² Detection

³ Original Data

⁴ Non- Blind

بنابراین بیشتر آشکارسازهای واترمارک، از نوع کور^۱ می‌باشند. یعنی، آشکارساز برای استخراج پیام مخفی تنها به اطلاعات واترمارک دسترسی دارد.



شکل ۱-۱-۱- 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_0 می‌باشد. مرحله‌ی اول، رمزنگاری پیام می‌باشد تا پیام، به یک پیام مخفی با کلید رمز K^2 تبدیل شود. در ابتدا، از پیام نمونه برداری می‌شود تا از لحاظ بُعد^۳ با بُعد اطلاعات اصلی مطابقت داشته باشد و همچنین پیام با یک نویز شبه تصادفی^۴ XOR می‌شود تا یک سری عدد شبه تصادفی تولید گردد که این اعداد به عنوان کلید رمز K در ورودی در نظر گرفته می‌شوند، سپس سیگنال واترمارک تولید شده W_m تغییر داده می‌شود، یعنی، بوسیله‌ی ضریب واترمارکینگ، تغییر مقیاس داده می‌شود و در مرحله‌ی 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^۵، تبدیل فوریه سریع^۶ (FFT) و تبدیل کسینوسی مجزا^۷ (DCT) 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^۱، 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^۲ بین اطلاعات دریافتی d_r و واترمارک تولید شده w_m استفاده می‌کنند. سرانجام، این ضریب همبستگی با یک مقدار آستانه^۳ مقایسه می‌شود تا بتوان در مورد حضور یا عدم حضور واترمارک اظهار نظر کرد.

۲-۱-۱ واترمارک‌کینگ غیر کور

در سال‌های اخیر، ضرورت ایجاد روش‌ها و گرایش‌های جدید در صنعت واترمارک‌کینگ به خوبی دیده می‌شود. در حال حاضر به پروسه واترمارک‌کینگ 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^۴ تحت تأثیر قرار گرفته است و فرستنده، منبع نویز اول را می‌شناسد، این منبع نویز اول هیچ تأثیری بر روی ظرفیت^۵ کانال ندارد. از دیدگاه واترمارک‌کینگ، 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^۶ در نظر گرفت. حتی اگر مدل Costa به طور مشخص با سیستم واترمارک‌کینگ واقعی متفاوت باشد، این

¹ Lossy Compression

² Correlation Score

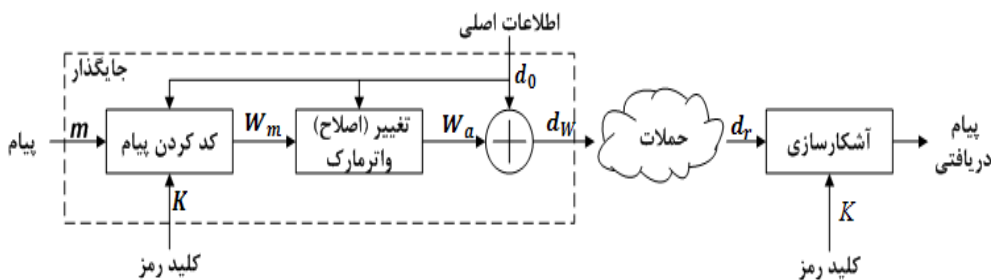
³ Threshold

⁴ Additive White Gaussian Noise

⁵ Capacity

⁶ Attacks

بدان معنی است که، اطلاعات جانبی جایگذار، منجر به کاهش تداخل با اطلاعات اصلی می‌شود. در شکل ۱-۱، می‌توان جایگذار را کور در نظر گرفت، چرا که اطلاعات اصلی در زمان کُد کردن پیام و مراحل ایجاد واترمارک مورد استفاده قرار نگرفته است. مدل Costa، به طراحی یک الگوریتم جدید بر اساس شکل ۱-۲ کمک می‌کند که از اطلاعات جانبی در طول اجرایی شدن دو مرحله فوق استفاده شده است. واترمارکینگ غیر کور را می‌توان در زمان کُد کردن پیام (کُد کردن غیر کور) و یا ایجاد واترمارک (جایگذاری غیر کور)، اجرایی کرد. با کُد کردن غیر کور، برای یک پیام معین، یک مجموعه از واترمارک‌های متفاوت در دسترس است و جایگذار، یکی از آن‌ها را که تداخل کمتری با اطلاعات اصلی دارد انتخاب می‌کند. هدف از جایگذاری غیر کور، ایجاد یک واترمارک بهینه است تا آشکار ساز بتواند پیام مد نظر را استخراج نماید.



شکل ۱-۲- شمای واترمارکینگ غیر کور

۲-۱ برخی از خصوصیات واترمارکینگ

در مقالات متعدد در مورد خواص سیستم‌های واترمارک بحث شده است، در عمل تقریباً غیرممکن است که بتوان یک سیستم واترمارکینگ طراحی کرد که تمام خواص مطلوب را داشته باشد، از این رو بایستی با توجه به کاربرد، در مورد اهمیت خواص تصمیم گرفته شود. در واترمارکینگ دیجیتال، یک مبادله پیچیده بین سه پارامتر نرخ