پایان‌نامه دوره کارشناسی ارشد برق

گرایش مخابرات سیستم

بررسی انواع حملات در واترمارکینگ تصاویر دیجیتال

حامد فرخاری

استاد راهنما:

دکتر اسدپور

تابستان ۹۰

چکیده

هم اکنون حفاظت از حق کپی داده های چندرسانه ای دیجیتال به صورت یک موضوع مهم درآمده است. یک تکنیک برای حل این مشکل، واترمارکینگ دیجیتال می‌باشد که اطلاعاتی را به صورت مستقیم در داخل داد ه های چندرسانه‌ای تعبیه و جاسازی می‌کند. به اطلاعات تعبیه شده واترمارک گفته می‌شود که بعد از اعمال حمله نیز می-بایست قابل آشکارسازی باشد به این ترتیب واترمارکینگ دیجیتال می‌تواند برای شناسایی مالک حقیقی رسانه استفاده شود. در سال های اخیر طرح های واترمارکینگ بسیاری پیشنهاد شده است .از میان این طرح ها، آنهایی که برای استخراج واترمارک احتیاج به تصویر اصلی و کلید رمز دارند طرح های واترمارک خصوصی نامیده می شوند. طرح هایی که احتیاج به اطلاعات واترمارک و کلید رمز دارند طرح های نیمه خصوصی و یا نیمه کور نامیده می شوند و در نهایت طرح هایی که برای استخراج واترمارک تنها به کلید رمز احتیاج دارند طرح های عمومی و یا کور نامیده میشوند.

فهرست

فصل اول

مقدمه

۱

مقدمه

با گسترش روز افزون اینترنت به عنوان محیطی برای انتقال سریع و آسان انواع اطلاعات (صوتی، تصویر، فیلم و غیره) این امکان برای افرادی که خواستار به اشتراک گذاشتن اطلاعات خود هستند به وجود آمده است. با وجود مزایای آن، این گونه انتقال اطلاعات می‌تواند مشکلات جدی برای مولفانی که نمی‌خواهند آثارشان بدون اجازه خودشان پخش شود ایجاد کند. به همین دلیل حفاظت از اطلاعات دارای حق کپی امری ضروری است. یکی از بهترین روش‌ها برای پاسخ گویی به مشکلات فوق نهان نگاری می‌باشد که دارای کاربردهای زیادی از جمله مخابرات مخفی، زمان بندی پخش برنامه‌ها، اثبات مالکیت و غیره است. نهان نگاری روشی است که در آن اطلاعات مالک (سیگنال الگو یا نهان شونده) به گونه‌ای نامحسوس در سیگنال اصلی یا میزبان نهان می‌شود و به این صورت سیگنال الگو گذاری شده یا نهان نگاری شده ایجاد می‌شود. این نهان کردن الگو نباید باعث کاهش کیفیت اطلاعات اصلی شود. به اقتضای کاربرد نهان نگاری بصورتهای مقاوم، نیمه شکننده و شکننده انجام می پذیرد. در این میان کاربردهای روشهای مقاوم از مابقی بیشتر است. همچنین از نقطه نظر آشکارسازی روشهای نهان نگاری به سه گونه کور، نیمه کور و بینا تقسیم می‌شوند.[1]

در ادامه ابتدا به معرفی واترمارکینگ پرداخته و تاریخچه‌ی آن را بیان می‌کنیم سپس انواع واترمارکینگ را بیان کرده و انواع رایج حملات از جمله نویز گوسی، نویز فلفل نمک، حمله‌ی برش، حمله‌ی چرخش و حمله‌ی تغییر اندازه را در دو تصویر واترمارک شده یکی به روش LSB و دیگری به روش DCT اعمال می‌کنیم و پس از آن عملیات آشکارسازی تصاویر را به روش مونت کارلو انجام می‌دهیم بدین صورت که هر تصویر واترمارک شده پس از اعمال هر حمله چندین بار عملیات آشکارسازی بر روی آن انجام می‌پذیرد و در هر بار میزان شباهت بین پیام آشکار شده و پیام اصلی محاسبه می‌گردد همین طور میزان شباهت بین تصویر واترمارک شده و تصویر پوش استفاده شده نیز بصورت مونت کارلو مورد محاسبه قرار می‌گیرد و در نهایت مقدار میانگین مربوط به چندین بار آشکارسازی و محاسبه‌ی مقدار شباهت در آن مرحله ثبت می‌گردد تا در انتها از مقادیر میانگین بدست آمده نمودار مربوطه رسم گردد، البته برای اینکه امکان مقایسه بین دو روش فراهم گردد برای هر حمله ی اعمالی نتایج یک بار بصورت جداگانه و یکبار بصورت یک جا یعنی رسم دو نمودار مربوط به یک حمله بر روی دو تصویر واترمارک شده با دو روش جداگانه بر روی هم ترسیم گردیده است.لازم به ذکر است که تعداد دفعات آشکارسازی در روش مونت کارلو برای هر تصویر ۲۰ می‌باشد تا ضمن افزایش دقت، صحت مقادیر بدست آمده نیز تضمین گردد. پس از ارائه‌ی نمودارهای مربوط به شبیه سازی‌ها نتایج و نتیجه‌گیری مربوط به هر یک ذکر گردیده و در انتها روش‌ها و راه‌کار-هایی نیز بیان شده است.

فصل دوم

معرفی واترمارکینگ

۲

مقدمه

در این فصل ابتدا به تاریخچه ی مربوط به واترمارکینگ می‌پردازیم و مقایسه‌ای بین واترمارکینگ و رمزنگاری را بیان کرده پس از آن به معرفی دو ابزار که در گذشته برای این عمل ابداع شده بودند می‌پردازیم سپس به معرفی واترمارکینگ تصاویر و روش‌های موجود پرداخته و توضیحاتی را برای هر یک بیان می‌کنیم.

۲-۱- تاریخچه واترمارکینگ

پیدایش واترمارکینگ به سال‌ها قبل حدود ۷۰۰ سال پیش برمی‌گردد.شاید در بسیاری از فیلم‌های قدیمی دیده باشید که نامه ای حاوی متنی معمولی و بدون اینکه شک برانگیز باشد برای شخص مهمی و به صورت محرمانه ارسال می‌شود در صورتی که متن نامه حاوی اطلاعات مهمی نیست و یا حاوی اطلاعات گمراه کننده و غلط می‌باشد و هنگامی که نامه در مجاورت حرارت و یا رطوبت قرار گیرد متنی مهم و سری بر روی نامه آشکار می‌شود، بله این روش همین واترمارکینگ است! که امروزه با متد جدیدی به روز شده است. اما این روش و استفاده ازکاغذهای واترمارک شده از ۷۰۰ سال پیش توسط دست بشر ساخته می‌شده و مورد استفاده قرار می‌گرفته است. واترمارک‌های کاغذی تکنیک بسیار خوبی برای آن زمان بود که(در کاربرد خاصی نظیر آسیاب) تشخیص بدهند که هر کاغذ آسیاب برای چه کسی است. قدرت قانونی واترمارکها در سال ۱۸۸۷ در فرانسه ثابت و در دادگاه بصورت قانونی برای محاکمه مورد استفاده قرار گرفت، همچنین اولین انتشاراتی که روی استفاده از واترمارک در تصاویر دیجیتال تمرکز کرد در سال ۱۹۹۰ و بعد از آن در سال ۱۹۹۳ بود. کاغذهای واترمارکی که در اسکناس‌ها، در بانک‌ها یا روی تمبرها استفاده می‌شد ایده ی استفاده از واترمارک در داده ی دیجیتال را بوجود آورد.[2]

۲-۲- لزوم استفاده از واترمارکینگ

یکی از مهم‌ترین ویژگی‌های اطلاعات دیجیتال آن است که بسیار راحت تولید می‌شود و قابلیت آن را دارند که تعداد نامحدودی کپی از آن گرفته شود. که این شامل موسیقی، فیلم، عکس و ... می‌شود. بنابراین مشکلات زیادی را با توجه به حفظ مدارک و حقوق تولید ناشی می‌شود. این حقیقت نیازمند تحقیق در باره‌ی راه‌های تعبیه اطلاعات کپی رایت و شماره سریال‌ها و داده است.

پنهان نگاری و واترمارکینگ باعث به وجود آمدن انواع زیادی از روشهای پنهان کردن اطلاعات به طور نایافتنی و یا غیرقابل انتقال در داده می‌شود.پنهان نگاری و واترمارکینگ دو بخش اصلی حوزه‌ی وسیع پنهان سازی اطلاعات هستند.

۲-۳- مقایسه رمزنگاری و واترمارکینگ

هدف اصلی واترمارکینگ پنهان کردن پیام m در داده‌ی d (صوت یا تصویر) است تا داده‌ی جدید d’ بدست آید که عملاً توسط انسان غیرقابل تشخیص از d است به طوری که فردی که استراق سمع می‌کند نمی‌تواند وجود m را در d’ تشخیص دهد.هم‌چنین گفته می‌شود که هدف رمزنگاری پنهان کردن پیام در ارتباطات یک به یک است، در حالی که واترمارکینگ در ارتباط یک با چند نفر است.[3]

معمولاً متدهای رمزنگاری نیاز ندارند که امنیت زیادی در برابر حذف یا تغییر پیام پنهان شده، داشته باشند، در حالیکه روشهای واترمارکینگ باید مقابل عملیات حذف و تغییرات پیام بسیار مقاوم باشند.[4]

۲-٤- کاربردهای استگانوگرافی

- ایجاد ارتباطات سرّی امن در جایی که متدهای پنهان شناسی در دسترس نیست.
- در بعضی شرایط مثل کاربردهای ارتش برای ارتباطات محرمانه.
- در کاربردهای پزشکی، در تصاویر پزشکی از پنهان‌نگاری بسیار استفاده می‌شود.

۲-۵- کاربردهای واترمارکینگ

کاربرد عمده‌ی واترمارکینگ در بوجود آوردن مدرک حق مالکیت اسناد دیجیتال است. [5]سایر کاربردها:

۱- واترمارک‌های حق مولف[۱]

۲- واترمارک‌های اثر انگشت[۲]

۳- واترمارک‌های پخش همگانی[۳]

۴- واترمارک‌های حاشیه نویسی[٤]

۵- واترمارک‌های مجتمع[٥]

۶- واترمارک‌های پنهان سازی داده[٦]

۲-۵-۱- واترمارک‌های حق مولف

تصاویر را با اطلاعاتی از قبیل مالک یا سازنده‌ی آن مارک دار می‌کنیم. هم‌چنین جستجوی تصویر در رشته ویدئویی ساده‌تر می‌شود. نوعاً این واترمارک‌ها باید خیلی قوی باشند و می‌توانند قابل رؤیت یا غیرقابل رؤیت و عمومی یا خصوصی باشند.

۲-۵-۲- واترمارک‌های اثر انگشت

برای پیگیری و ردیابی کردن کپی‌های یک تصویر به کار می‌رود. همچنین می‌تواند عامل یک فعالیت جاسوسی را شناسایی کند و سخت افزار احراز هویت را فعال می‌کند. معمولاً غیر قابل رؤیت و خصوصی است و باید بسیار قوی باشد.

---

[1] Copyright Watermarks
[2] Fingerprint Watermarks
[3] Broadcast Watermarks
[4] Annotation Watermarks
[5] Integrity Watermarks
[6] Data Hiding Watermarks

۲-۵-۳- واترمارک‌های پخش همگانی

برای جلوگیری از کپی شدن رسانه‌ها به کار رفته و برای وسیله‌های سخت‌افزار و نرم‌افزاری حفاظتِ کپی رایت ایجاد می‌کند. همچنین از جعل پول رایج، گذرنامه، گواهینامه و... جلوگیری می‌کند. اغلب اوقات غیرقابل رؤیت و عمومی است و باید بسیار قوی باشد. در بعضی شرایط خاص قابل رؤیت است (مثلاً در زیر نوع خاصی از نور).

۲-۵-۴- واترمارک‌های حاشیه نویسی

این واترمارک‌ها غیرقابل رؤیت و عمومی هستند و باید تا حد امکان قوی باشند.

۲-۵-۵- واترمارک‌های مجتمع

اطمینان می‌دهد که یک تصویر تغییر پیدا کرده یا حداقل روشن می‌کند که از زمانی که اصل آن ساخته شده، تغییر کرده است. این واترمارک‌ها نوعاً بسیار شکننده هستند به طوری که حتی تغییرات بسیار کوچک در تصویر تغییرات شدیدی در واترمارک تولید می‌کند. می‌توانند قابل رؤیت یا غیرقابل رؤیت باشند و هم‌چنین عمومی یا خصوصی باشند، اما همیشه بسیار شکننده‌اند.

۲-۵-۶- واترمارک‌های پنهان سازی داده

برای این منظور استفاده می‌شود که اطلاعات سری یا پنهانی را در یک تصویر مخفی کند. می‌تواند برای افزایش امنیت رمزگذاری شود. همیشه غیرقابل رؤیت است و باید بسیار قوی باشد. با توجه به سناریوی مورد استفاده می‌تواند خصوصی یا عمومی باشد.

۲-۶- ویژگی های واترمارکینگ

یک راه حل قدرتمند برای ادعای حق مالکیت یک اثر آن است که از واترمارکینگ استفاده کنیم، که درون داده پنهان می‌شوند و چنین ویژگی‌هایی دارند[6]:

۱) غیر قابل حذف شدن توسط هکرها هستند.

۲) به طور ادراکی غیرقابل دیدن هستند، بدین معنی که می توانند به گونه ای ساخته شوند که توسط چشم تشخیص داده نشوند.

۳) به طور آماری غیر قابل کشف هستند.

۴) مقاوم در برابر فشرده سازی پراتلاف هستند(منظور فشرده سازی به فرم JPEG).

۵) مقاوم در برابر دستکاری‌های تصاویر و عملیات پردازش هستند(مثل کپی کردن و...).

۲-۷- استحکام واترمارکینگ

استحکام[1]: هرچه اطلاعات بیشتری در تصویر ذخیره کنیم استحکام کمتری خواهد داشت که البته در هر تصویر ظرفیت محدودی از اطلاعات را می‌توان پنهان کرد. در استحکام این عوامل نیز مؤثر هستند:

[1] Robustness

سیگنال به نویز[1]که یکی از معیارهای دیداری مبتنی بر پیکسل است و عامل دیگر خصوصیت ادراکی است که استفاده از مناطقی که تضاد رنگی زیادی ندارند مد نظر می‌باشد.

برای داشتن استحکام باید نسبت به موارد زیر مقاوم باشد: فشرده سازی، تبدیلات هندسی (تقارن افقی یا عمودی، چرخش[2] کردن، بریدن[3] و تغییر اندازه)، تکنیک‌هایی نظیر تیز کردن[4]، اعمال فیلتر پایین گذر[5]، تغییرات هیستوگرام[6] و نویز.

دو نمونه از وسایلی که در گذشته برای رمزنگاری و واترمارکینگ استفاده می‌شدند در ادامه آورده می‌شوند.

۲-۸- دیسک رمزنگار

شکل ۲-۱- دیسک رمزنگار[13]

به نظر وسیله ساده‌ای می آید. دو صفحه چرخان که روی هر کدام حروف انگلیسی نوشته شده است. از آن برای نوشتن پیام‌های رمزنگاری استفاده می‌کردند و برای باز کردن رمز باید صفحات را در مکان مناسب قرار داد. مثلا در این تصویر G =M است. به نظر شکستن رمزش آسان می آید اما جاسوس‌ها پیام‌ها را به زبانی غیر از انگلیسی می نوشتند! بنابراین اول باید می‌دانستید که پیام به چه زبانی نوشته شده است و همین کار را بسیار سخت می‌کرد. اما روش دومی که از رمزنگاری بیان خواهیم کرد در جنگ جهانی دوم توسط آلمانها بکار گرفته شده است.

۲-۹- ماشین تایپ رمزنگار

[1] SNR
[2] Rotate
[3] Crop
[4] Sharpening
[5] Low pass Filtering
[6] Histogram Modification

شکل ۲-۲- ماشین تایپ رمزنگار[13]

این روزها انواع روش‌های رمزنگاری و الگوریتم‌های پیچیده برای این کار وجود دارد. اما در جنگ جهانی دوم از کامپیوترهای امروزی خبری نبود. این ماشین تایپ مخصوصی است که آلمانی‌ها اختراع کرده بودند. آنها می دانستند که ارسال پیام‌ها از طریق بیسیم به صورت رمزنگاری نشده کار خطرناکی است. بنابراین، این دستگاه را ساختند. آنها پیام را به راحتی روی آن تایپ می‌کردند و پیام نوشته شده توسط یک بخش الکترونیکی به رمزهای مخصوص تبدیل می‌شد و آنها متن کد شده را ارسال می‌کردند. آلمانی ها تصور می‌کردند که این الگوریتم غیر قابل شکستن است. در حالی که در آن طرف متفقین آن را شکسته بودند و پیام‌های آلمان ها را می خواندند.

نکته در اینجا است که آلمان ها در جنگ جهانی دوم هم اطلاعاتی که از طریق شبکه های بیسیم منتقل می‌شد را رمز نگاری می‌کردند اما هنوز خیلی از کاربران فعلی اینترنت شبکه بیسیم‌شان را همینطور بدون رمزنگاری مناسب رها کرده‌اند.

فصل سوم

انواع روش‌های واترمارکینگ

۳

مقدمه

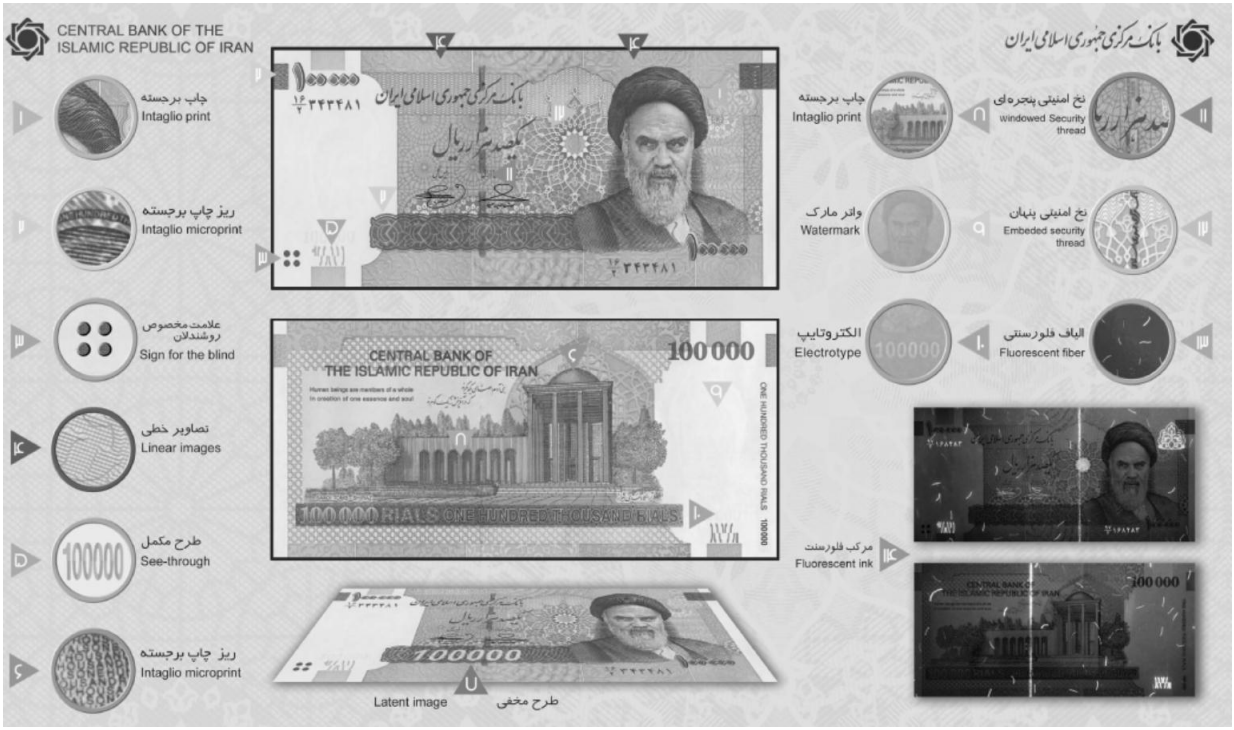
در این فصل انواع روش‌های واترمارکینگ تصاویر به همراه توضیحات مربوط به آنها ذکر خواهد شد و همچنین چند نمونه از کاربرد واترمارکینگ نیز بیان خواهد شد.

۳-۱- انواع واترمارکینگ

یک روش برای تقسیم بندی انواع واترمارکینگ دو نوع آشکار یعنی قابل رویت و غیر قابل رویت می باشد.[7] حال اگر بخواهیم به زبان خیلی ساده توصیفی از واترمارکینگ داشته باشیم می‌توانیم بگوییم که واترمارکینگ در واقع قرار دادن یک دیتا در داخل دیتای دیگر است. درنوع قابل رویت واترمارکینگ تصاویر، دیتای اول به صورت یک ماسک شفاف بر روی دیتای دوم قرار می‌گیرد. دراین نوع بیشتردر اسناد PDF و یا تایپی ویا عکس ها و معمولاً به صورت مایل در همه ی صفحات سند قرار داده می‌شود تا امکان کپی برداری غیرمجاز مطالب بسیار کاهش یابد. نمونه‌ای از این روش همین کلمه‌ی واترمارکینگ است که در شکل ۳-۱ آمده و می‌تواند در تمام صفحات بصورت مورب و کم رنگ قرار داده شود.

شکل ۳-۱- واترمارکینگ قابل رویت در اسناد

اما در روش واترماکینگ غیرقابل رویت از تکنیک‌هایی استفاده میشود که تشخیص داده‌ی واترمارک شده به راحتی امکان پذیر نباشد و روش‌های مختلفی برای این امر وجود دارد که به تفضیل در ادامه آورده میشود. مثالی دیگراستفاده از واترمارکینگ قابل رویت برای افزایش ضریب امنیتی در اسکناس‌ها و چک پول ها:



شکل ۳-۲- موارد امنیتی اسکناس ۱۰۰۰۰ تومانی و استفاده از واترمارکینگ قابل رویت در آن[14]

همانطور که در شکل ۳-۲ مشاهده می‌شود در بخشی که با شماره‌ی ۹ مشخص گردیده است از واترمارکینگ مرئی برای افزایش ضریب امنیتی اسکناس استفاده شده است.

۳-۲- تقسیم بندی واترمارکینگ کور و غیرکور

تقسیم بندی سیستم‌های واترمارکینگ بر اساس نوع ورودی و خروجی بدین ترتیب است[8][9]:

۱) واترمارکینگ غیرکور خصوصی[1]:

طرحهایی که برای استخراج واترمارک احتیاج به تصویر اصلی و کلید رمز وجود دارد طرح های واترمارک خصوصی نامیده می شوند .

در این‌جا برای استخراج یا یافت واترمارک به اصل داده ی نقاب[2] نیاز دارند.

- نوع اول از این سیستم‌ها از داده‌ی نقاب اصلی برای استخراج واترمارک و تشخیص آن که واترمارک‌ها در کجای داده وجود دارد، استفاده می‌کند.
- نوع دوم این سیستمها یک کپی از واترمارک تعبیه شده نیاز دارد و فقط می‌تواند بگوید که آیا داده‌ی پنهان نگاری شده حاوی واترمارک هست یا نه!

۲) واترمارکینگ شبه کور[3]:

[1] Private Non-blind Watermarking
[2] cover-data
[3] Semi-private (semi-blind) Watermark

طرح هایی که احتیاج به اطلاعات واترمارک و کلید رمز دارند طرح های نیمه خصوصی و یا نیمه کور نامیده می-شوند. این سیستم از داده‌ی نقاب اصلی برای جستجو استفاده نمی‌کند بلکه فقط وجود یا عدم وجود واترمارک را پاسخ می‌دهد (این برنامه‌های کاربردی برای شهادت دادن در دادگاهها به کار می‌رود).

۳) واترمارکینگ کور عمومی[1]:

در نهایت طرح‌هایی که برای استخراج واترمارک تنها به کلید رمز احتیاج دارند طرح های عمومی و یا کور نامیده می‌شوند. در این‌جا نه داده ی نقاب و نه واترمارک تعبیه شده برای استخراج لازم نیستند.

روشهای مختلفی برای واترمارک وجود دارد که بعضی از آنها از تکنیک‌های کد کردن و بعضی از حوزه فرکانسی استفاده می‌کنند. در بیشتر روش‌ها واترمارک یک رمز یا یک عدد تصادفی است که از دنباله ای از بیت‌ها تشکیل شده و فقط توسط «نظریه جستجو» می‌تواند یافت شود. بر اساس این نظریه در فاز تطبیق، تصویر اصلی از تصویر مورد سؤال تفریق شده و شباهت بین حاصل تفریق و واترمارک خاصی محاسبه خواهد شد.

۳-۳-واترمارک

واترمارکینگ دیجیتال اطلاعاتی را به صورت مستقیم در داخل داده های چندرسانه ای تعبیه و جاسازی می کند .به اطلاعات تعبیه شده واترمارک گفته می شود که بعد از اعمال حمله نیز میبایست قابل آشکارسازی باشد (البته منظور حمله در اینجا مجاز و با داشتن کلید و .. است که توضیح داده خواهد شد) به این ترتیب واترمارکینگ دیجیتال می تواند برای شناسایی مالک حقیقی رسانه استفاده شود.

در واترمارکینگ تصویر دو گزینه متفاوت برای نمایش و استفاده واترمارک وجود دارد .در گزینه اول واترمارک معمولاً دنباله ای از اعداد حقیقی تصادفی با توزیع نرمال (میانگین صفر و واریانس یک) می باشد این نوع واترمارک به آشکارساز اجازه می دهد تا به صورت آماری وجود و یا عدم وجود واترمارک را در تصویر مشخص نماید. در گزینه دوم، واترمارک یک تصویر است که در تصویر میزبان درج می شود و نمایانگر آرم یک کمپانی و یا دیگر موارد حق کپی می‌باشد در این نوع واترمارکینگ، آشکارساز واترمارک را به طور کامل بازسازی می کند وکیفیت دیداری آن را با استفاده از معیار مناسب بازسازی میکند.[2]

۳-٤- کلید رمز

کلید کاربر به عنوان رمزی است که می‌تواند فرایندهای مختلف پنهان سازی را با استفاده از تکنولوژی مشابه انجام دهد. بعلاوه یک کلید کاربری به عنوان یک پارامتر در طول گامهای استخراج واترمارک به کار می‌رود.[2][3] در این جا یک کلید کاربری باید موارد زیر را تعریف کند:

۱ - جستجوی الگوی تولید کننده‌ی اعداد شبه تصادفی:

موقعیت اولیه‌ی جایگشت شبه تصادفی باید تعریف شود.

۲- انتخاب ضرایب فرکانسهای میانی:

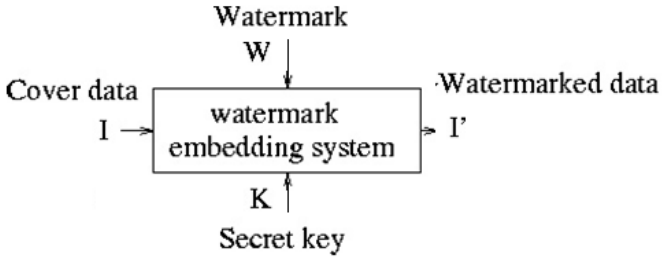
[1] public blind watermarking

تعداد ضریب فرکانس میانی باید از بین ضرایب DCT برای هر بلوک جدا شود که در کلید کاربری ضرایبی که قرار است پردازش شوند باید مشخص شود.

۳- نگاشت ضرایب انتخاب شده به بلوکهای کاهش یافته:

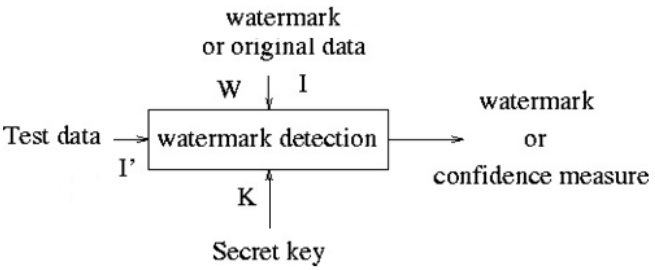
روشهای مختلفی برای این نگاشت وجود دارد. چگونگی این نگاشت باید توسط کلید کاربری مشخص باشد.

۳-۵- فرم کلی سیستم‌های تعبیه و استخراج واترمارک



شکل ۳-۳- فرم کلی سیستم های تعبیه واترمارک[10]

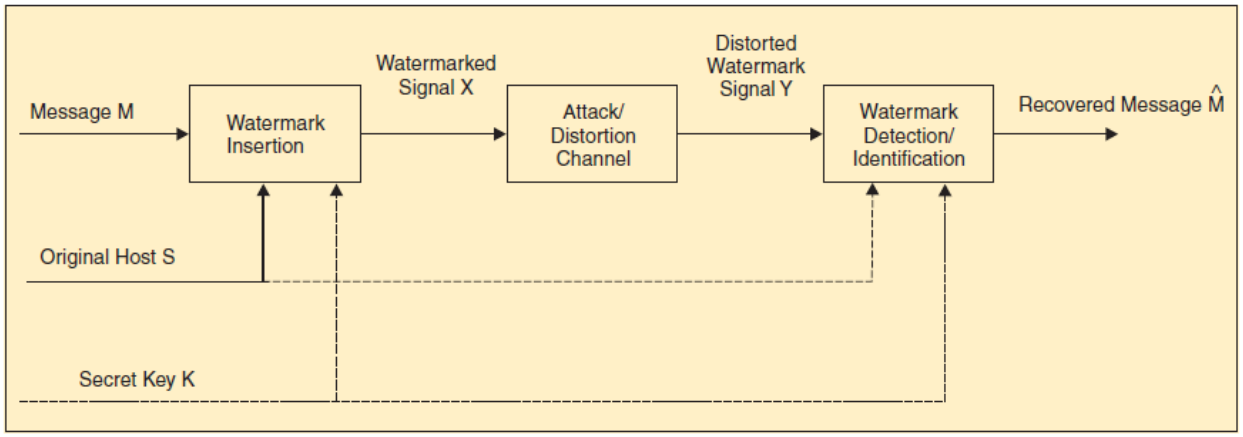
ورودی سیستم واترمارک، داده‌ی نقاب و یک کلید[1] است که ممکن است عمومی[2] یا سرّی[3] باشد. خروجی داده‌ی واترمارک شده است(کلید برای ایجاد امنیت به کار می‌رود).



شکل ۳-٤- فرم کلی سیستمهای استخراج واترمارک[10]

ورودی این سیستم داده‌ی واترمارک شده، کلید عمومی یا سری است و بسته به متد به کار رفته داده‌ی اصلی هم به عنوان ورودی لازم است. خروجی داده‌ی واترمارک شده است یا ممکن است ضریب اطمینان باشد که نشان می‌دهد چقدر احتمال دارد واترمارک داده شده در داده‌ی مورد بررسی وجود داشته باشد.[10]

[1] key
[2] public
[3] secret



شکل ۳-۵- بلوک دیاگرام سیستم واترمارکینگ[10]

در شکل ۳-۵ بلوک دیاگرام سیستم واترمارکینگ آورده شده است که در بخش نخست عمل واترمارکینگ انجام می-شود و پس از عبور از کانال و اعمال حملات مختلف و نویز در بخش گیرنده عملیات آشکارسازی انجام می‌گردد.

۳-٦- روش‌های واترمارکینگ تصاویر

در این بخش روش‌های مختلف واترمارکینگ تصاویر به همراه توضیحات مربوطه آورده می‌شود.

۳-۶-۱- روش‌های جایگزینی داده

در روشهای جایگذاری داده، بیت‌های واترمارک در بیت‌های کم ارزش تصویر جایگذاری می‌شود. با وجود اینکه این متد بسیار ساده و غیرقابل رویت است اما بسیار حساس و شکننده می‌باشد.[10]

۳-۶-۲- جایگزینی در LSB

هر یک از $\boldsymbol{R_1, G_1, B_1, \dots, R_N, G_N, B_N}$ ها به صورت دنباله از بیت‌ها می‌باشد که برای جاسازی بیت‌های پیام در تصویر از کم ارزش‌ترین بیت[1] هر یک یا بعضی از R و G وB ها استفاده می‌کنند. یعنی LSB بلوک باینری با بیتی از پیام سری جابجا می‌شود البته متدهای مختلف واترمارکینگ در این بخش متفاوت هستند (انتخاب LSB همه یا بعضی از بلوک‌ها).[12]

۳-۶-۳- جایگزینی در بیت‌های پریتی

در این روش اگر بیت توازن از بلوک تصویر برابر با بیت متناظر آن در پیام باشد این بلوک دست نمی‌خورد در غیر این صورت یکی از بیت‌هایش تغییر می‌کند.در این روش تغییرات ناشی از واترمارک کردن پیام در تصویر کمتر می-شود ولی همان طور که بیان شد این روش نیز بسیار آسیب پذیر است.[10]