دانشگاه بیرجند

دانشکده مهندسی

پایان‌نامه دوره کارشناسی ارشد مهندسی برق - مخابرات

واترمارکینگ تصویر دیجیتال با استفاده از منطق فازی

علیرضا بزرگیان

استاد راهنما:

دکتر حسن فرسی

استاد مشاور:

دکتر حمید فرخی

تابستان ۱۳۹۱

تقدیم به همسر مهربانم

با سپاس ازسه وجود مقدس:

آنان که ناتوان شدند تا ما به توانایی برسیم...

موهایشان سپید شد تا ماروسفید شویم...

و عاشقانه سوختند تا گرمابخش وجود ما و روشنگر راهمان باشند...

پدرانمان

مادرانمان

استادانمان

چکیده:

در این پایان‌نامه یک طرح واترمارکینگ دیجیتال در دامنه تبدیل فوریه گسسته مبتنی بر سیستم استنتاج فازی و سیستم بصری انسان معرفی میشود. در مرحله اول ، تصویر به بلوک های ۸×۸ تقسیم شده سپس سیستم فازی با توجه به ویژگی‌های بافت مختلف هر بلوک ضریبی به آن اختصاص میدهد که باعث افزایش مقاومت و شفافیت فرآیند واترمارکینگ خواهد شد. پس از آن با محاسبه‌ی تبدیل فوریه هر بلوک دامنه و فاز از هم جدا میشوند و واترمارک مورد نظر در دامنه پنهان میگردد. فرایند استخراج واترمارک کور خواهد بود که باعث امنیت بالای این روش می‌گردد. ضعفی که روش‌های موجود واترمارکینگ مبتنی بر تبدیل فوریه گسسته دارند اینست که از سیستم بینایی انسان استفاده نمیکنند و مولفان آن‌ها برای جلوگیری از کاهش کیفیت تصویر، استحکام کمی برای روش خود در نظر می‌گیرند. نتایج بدست آمده نشان می‌دهد این روش از شفافیت خوبی نسبت به روش‌های متداول برخوردار است و در برابر حملات برش ، تارکردن و روشن کردن تصویر ، افزودن نویز ، فیلترینگ و فشرده سازی (jpeg) مقاوم می‌باشد.

کلید واژه‌ها: منطق فازی[1] ، واترمارکینگ کور [2] ،تبدیل فوریه گسسته [3]، سیستم بینایی انسان [4]، فشرده سازی تصویر

[1] Fuzzy logic
[2] non-blind Watermarking
[3] Discrete fourier Transform
[4] Human visual system

فهرست مطالب

عنوان **صفحه**

فهرست شکل‌ها

عنوان **صفحه**

فصل ۱– مقدمه ای بر واترمارکینگ

۱–۱– مقدمه

با توجه به گسترش روز افزون ارتباطات در دنیای امروز ، ضرورت کنترل بهینه ارتباطات در محیطهای گوناگون چند رسانه ای بیش از پیش روشن می شود و حفاظت از داده ها در مقابل کپی برداری وجعل از اهمیت بالایی برخوردار است که برای حفاظت از محصولات دیجیتال چند رسانه ای در برابر کپی های غیر مجاز و حفظ حق انتشار برای داده های صوتی ، تصویری و ویدئویی دوتکنیک موجود است [۱]:

۱- رمزنگاری[1]

۲- واترمارکینگ[2]

در رمز گذاری داده های دیجیتال در فرستنده رمز می شوند و پس از دریافت در گیرنده رمزگشایی میشوند. این روش تنها دربازه زمانی انتقال اطلاعات بصورت دیجیتالی از فرستنده به گیرنده می تواند از اطلاعات محافظت کند [۲].

بعد از دریافت اطلاعات توسط گیرنده، اطلاعات دریافتی از اطلاعات اصلی قابل شناسایی است.

روش های مختلف رمزنگاری اگرچه دارای مزایایی هستند اما دارای چندین عیب نیز می باشند ازجمله می توان به گم شدن رمز عبور ، تغییر محتویات در طول انتقال ، صرف زمان جهت رمزگشایی و برگرداندن داده نام برد.

تکنیک واترمارکینگ می‌تواند مکمل تکنیک رمزنگاری باشد بطوری که یک سیگنال غیرمحسوس به سیگنال اصلی،(که همیشه ماندگار باشد) را به آن اضافه می کنند و این سیگنال جدید را می فرستند. این در واقع یک کد انحصاری برای آن داده تلقی می شود. برای استفاده از داده‌ی نهان نگاری شده نیازی به برداشتن سیگنال واترمارک نیست، زیرا این سیگنال طوری در داده میزبان درج می شود که هیچ تاثیر نامطلوب بر داده ی اصلی نمی‌گذارد.

در واترمارکینگ با استفاده از الگوریتم خاصی، اطلاعاتی را برای شناسایی اثر در درون ان می گنجانند تا ارتباط محصول مورد نظر با مؤلف واقعی آن از طریق این اطلاعات مخفی مشخص گردد.

واترمارکینگ کاربردهای گوناگونی دارد که مهمترین کاربرد آن حفظ حق کپی برداری است. از کاربردهای دیگر آن می توان به ردیابی شخص خائن اشاره کرد.

در واترمارکینگ ، باید پارامترهایی همچون شفافیت ، مقاومت و ظرفیت در نظر گرفته شود که در این میان ، شفافیت، نقش اصلی را ایفا می کند. برای حفظ شفافیت می بایست پس از درج وا ترمارک ، نتوان

---

[1] Encryption
[2] Watermarking

تصویر واترمارک شده را از روی تصویر اصلی تشخیص داد. برای مقاوم بودن نیز باید دامنه داده هایی که وارد می شود بزرگ باشد و این موضوع باعث محسوس شدن واترمارک می شود. با توجه به رابطه معکوس بین پایداری و نامحسوس بودن ، باید تعادلی را میان این دو در نظر گرفت.

منظور از مقاوم بودن این است که سیگنال واترمارکی که صحت داده میزبان را اثبات می کند در برابر تکنیکهای پردازش تصویر از قبیل فشرده سازی ، فیلترینگ، چرخش، تغییر شدت روشنایی ، برش وحملات عمدی و غیر عمدی دیگر مقاوم باشد .

می توان مقدار محدودی اطلاعات را در یک تصویر پنهان کرد ، اندازه این مقدار بستگی به نوع و روش واترمارکینگ دارد ونشان دهنده ظرفیت است. مقدار اطلاعات باید به اندازه ای باشد که اولا از کیفیت تصویر نکاهد و ثانیا در مقابل یک سری فرایندهای پردازش تصویر دوام داشته باشد. بنابراین بین ظرفیت و مقاومت رابطه عکس برقرار است، بدین ترتیب که هرچه ظرفیت بالاتر برود از مقاومت کاسته می‌شود.

ساده ترین روشی که در ابتدا مطرح شد قرار دادن داده ها در کم ارزش ترین بیت (LSB) اطلاعات شدت روشنایی تصویر بود. این روش هم به راحتی قابل استفاده بود، هم به زمان بسیار کمی نیاز داشت و هم اینکه میزان داده قابل پنهان کردن بسیار زیاد بود. مثلاً در یک تصویر با ابعاد ۲۵۶×۲۵۶ می‌توان ۸ کیلو بایت اطلاعات ذخیره کرد. این روش تغییر بسیار محسوسی در تصویر ایجاد می کند، ولی مشکل اساسی آن ، این است که با ایجاد کوچکترین تغییری در تصویر تمام داده ها تخریب می شوند و در ضمن داده ها از هیچگونه امنیتی برخوردار نیستند[۳] و[۴].

بعد از آن روش هایی مانند روش های آماری[۵] و[۶]، طیف گسترده[1] [۷] و[۸] و همچنین روش هایی بر پایهٔ تبدیلات کسینوسی [۹] ، فوریه[۱۰] و موجک [2][۱۱] مطرح شده است. امروزه دانشمندان در حال تحقیق در مورد روش هایی بر پایهٔ سیستم های بینایی انسان برای حفظ کیفیت تصویر در هنگام نهان نگاری ، کاهش زمان لازم برای استخراج داده و همچنین استخراج داده ها بدون کمک تصویر اولیه هستند[۱] و[۱۲].

۱-۲- تاریخچه ی واترمارکینگ

در یونان باستان از نهان نگاری فقط برای ارتباطات مخفیانه استفاده می شده است. داستان هایی در مورد لوح هایی که با روغن های نامرئی نوشته می شد و یا بردگانی که پیغام ها را بر روی پوست سرشان خالکوبی میکردند و یا پیک هایی که پیام ها را می بلعیده‌اند، همگی مؤید این مطلبند. در گذشته های دور معمولاً از انسان به عنوان سیگنال میزبان استفاده می شد. امروزه به جای انسان از محصولات چند رسانه ای برای سیگنال میزبان استفاده و نهان نگاری به نهان نگاری دیجیتال تبدیل شده است[۳] و[۷].

---

[1] Spread spectrum
[2] Wavelet

کاغذهای واترمارک شده از ۷۰۰ سال پیش توسط دست بشر ساخته می شد. 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 شد وقتیکه واترمارکِ دو نامه که به عنوان سند در محکمه ارائه شده بود نشان داد که نامه‌ها جعلی است و سرانجام به سقوط کابینه‌ی هیئت وزرای آن زمان منجر شد.

واترمارکینگ دیجیتال در سال ۱۹۵۴ توسط یکی از مهندسان شرکت موزاک ابداع شد. در این ابداع یک کد شناسایی به گونه‌ای غیرقابل تشخیص یا به اصطلاح نامرئی ، به فایل حاوی موسیقی دیجیتالی وصل شد تا بتواند برای اثبات حق مالکیت به کار رود. از آن زمان به بعد از واترمارکینگ دیجیتالی استفاده فراوانی شد اما تا سال ۱۹۹۰ به عنوان یک موضوع تحقیقاتی با ارزش، توجه دانشمندان را به خود جلب نکرده بود. اولین انتشاراتی که روی استفاده از واترمارک در تصاویر دیجیتال تمرکز کرد در سال ۱۹۹۰ و بعد از آن در ۱۹۹۳ بود. در دهه‌ی ۱۹۹۰ این موضوع به عنوان یک موضوع جذاب تحقیقاتی مورد توجه قرار گرفت و تا امروز همچنان جذابیت واهمیت خود را حفظ کرده است [۱۳].

در دهه گذشته در نحوه استفاده و انتقال اطلاعات دیجیتالی (مالتی مدیا) اقدامات گسترده ای انجام گرفته است.

۱-۳- طبقه‌بندی واترمارکینگ

یک روش طبقه‌بندی برای الگوریتم های واترمارکینگ که توسط [۱۴] ارائه شده است را در زیر بیان می کنیم. این طبقه بندی براساس معیار های مختلف صورت گرفته است:

۱-۳-۱- حوزه قرار دادن و استخراج :

_ حوزه فضایی:

ساده‌ترین و سرراست‌ترین روش نهان‌نگاری ، قراردادن داده‌های نهان‌نگاری در حوزه مکان است[۱۵]و [۱۶]. در این روش ها مقادیر پیکسل ها بر اساس یک الگوی نویزی شبه تصادفی یا تغییر بیت کم ارزش مقادیر پیکسل ها صورت می گیرد. نهان نگاری در حوزه مکان ساده و سریع است ولی معمولاً شکننده است. روش کلی برای نهان نگاری در حوزه مکان را می توان بدین صورت توصیف کرد که داده نهان‌نگاری با اعمال تغییرات اندکی در مقادیر پیکسل ها در تصویر قرار داده می شوند. فرض کنید نهان نگار باینری w را بخواهیم در تصویر X قرار دهیم. فرآیند قرار دادن را می توان به صورت زیر توصیف کرد:

$$\acute{X}_i = X_i + \alpha_i w_i \qquad (۱-۱)$$

که i مکان نهان نگاری را نشان می دهد و α_i فاکتور قدرت است . مقدار α_i از رابطه زیر تعیین میگردد:

$$\alpha_i = C.\frac{\beta_i}{max\ (\beta_i)} \qquad (۲-۱)$$

که c یک مقدار ثابت ، تعریف شده توسط کاربر است و معمولا مقدار ۱۰ دارد و β_i مقداری برای کنترل α_i است، به طوری که تغییرات برای چشم انسان قابل رؤیت نباشد. چون چشم انسان به تغییرات شدت نور به صورت لگاریتمی پاسخ می دهد الگوریتم نهان نگاری باید به همین صورت عمل کند ، بنابراین β_i مقدار لگاریتم واریانس بین پیکسل های همسایه در یک پنجره مربعی است و به صورت زیر محاسبه میگردد:

$$\beta_i = var(window(X_i, n) + \varepsilon)$$
$$\varepsilon \in R^+ \qquad \varepsilon \ll 1 \qquad (۳-۱)$$

که ε یک عدد حقیقی مثبت کوچک می باشد که β_i را در یک محدوده عملیاتی محدود می کند[۱۷].

روش مناسب برای ارزیابی میزان شفافیت محاسبه PSNR است که در فصل پنجم توضیح داده میشود. در واقع هر چقدر مقدار PSNR بیشتر باشد قابلیت درک کمتر خواهد بود و نهان نگاری بهتری خواهیم داشت. PSNR برای روش ارائه شده در بالا مقدار مناسبی دارد.

_ حوزه تبدیل DFT ، DWT ، DCT :

نهان نگاری در حوزه تبدیل روشی است که بیشترین تمرکز بر روی آن صورت گرفته و اغلب روش-های ارائه شده در این حوزه است. تبدیلات DFT ،DCT وDWT مهمترین ابزار در پردازش داده های مالتی مدیا هستند، بنابراین در زمینه نهان نگاری در داده های مالتی مدیا نیز به عنوان یک ابزار مهم به شمار می روند. نهان نگاری در حوزه تبدیل به صورت اتوماتیک وابسته به محتوای تصویر[۱] است و بنابراین از مقاومت بیشتری بر خوردار می باشد ویژگی‌ای از تبدیلات که در نهان نگاری مهم است میزان فشرده سازی انرژی توسط تبدیل است که در مقاومت نهان نگاری تأثیر می گذارد .

در نهان نگاری تصویر در حوزه تبدیل سه گام اصلی وجود دارد :

الف) اعمال تبدیل برروی تصویر

ب) تغییر ضرایب تصویر[۲]

ج) بازسازی مجدد تصویر[۳]

---

[1] Content Dependent
[2] Watermark Casting
[3] Watermark Recover

تبدیل می تواند بر کل تصویر اعمال شود مانند روش پیشنهادی [۱۸]، یا به صورت بلاک به بلاک بر تصویر اعمال شود مانند روش پیشنهادی[۱۹]. بعد از این مرحله، انتخاب ضرایب تبدیل و قرار دادن بیت-های نهان نگاری انجام می شود. برای نهان نگاری از یک قانون کلی استفاده می شود که معمولاً به قانون ضربی[۱] یا جمعی[۲] معروف است.

$$X_i' = X_i.(1 + rw_i) \qquad i \in [0, L-1] \qquad (۴-۱)$$

که X و X' تصویر اصلی و نهان نگاری شده، L طول واترمارک، W واترمارک، i مکان نهان نگاری و r فاکتور قدرت[۳] است. برای تشخیص و بررسی در سمت گیرنده از همبستگی استفاده می شود.

$$R_{x'',w} = \frac{1}{L} \sum_{i=0}^{L-1} X_i'' \, w_i \qquad (۵-۱)$$

که X'' تصویر دریافتی است که ممکن است مورد حمله قرار گرفته باشد. برای چک کردن وجود نهان نگار یک سطح آستانه T تعریف می شود که برای تصمیم گیری استفاده می شود.

$$\begin{cases} R_{x'',w} \geq T \rightarrow watermark\ is\ present \\ R_{x'',w} < T \rightarrow watermark\ is\ not\ present \end{cases} \qquad (۶-۱)$$

۱-۳-۲- در دسترس بودن داده مرجع (مثلاً تصویر اصلی) در فرآیند استخراج:

_ غیر کور:

روش‌هایی که گیرنده به تصویر میزبان و واترمارک نیاز دارد. در این روش‌ها که معمولا برای اثبات مالکیت تصویر بکار می‌روند، فقط هدف اثبات وجود یک داده پنهان شده خاص در تصویر است. این روش‌ها به روش‌های غیر کور[۴] معروفند.

_ نیمه کور:

الف-روش‌هایی که در گیرنده نیاز به تصویر میزبان نیست ولی واترمارک مورد نیاز است.

ب- روش‌هایی که در گیرنده به تصویر میزبان نیاز است ولی واترمارک نیاز نیست.

---

[1] Multiplicative Rule
[2] Additive Rule
[3] Strength
[4] non- blind

_ کور:

روش‌هایی که گیرنده به تصویر میزبان و واترمارک نیاز ندارد. این روش‌ها دارای کاربرد بیشتری هستند.

۱-۳-۳- عناصر لازم برای استخراج:

_ کلید خصوصی :

کلیدی که فقط به یک کاربر اختصاص دارد وهر کاربربا کلید مخصوص به خود میتواند از اطلاعات استفاده کند.

_ کلید عمومی :

کلیدی که در دسترس عموم قرار دارد.

_ نامتقارن :

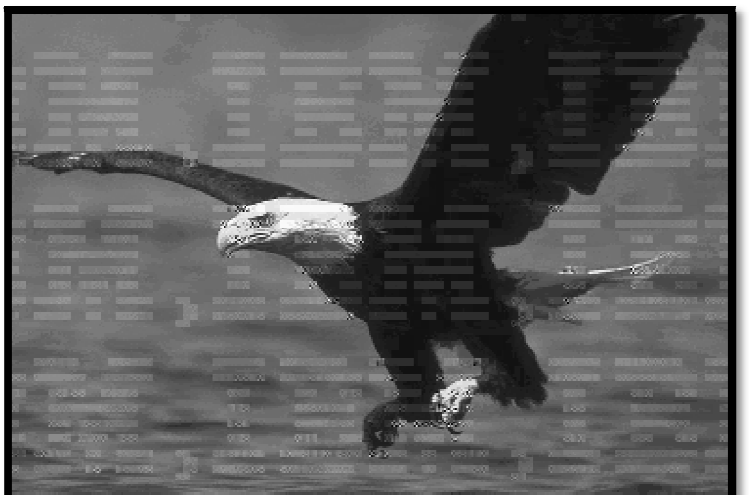
هر شخصی باید دو کلید داشته باشد یکی کلید عمومی و یک کلید خصوصی.

۱-۳-۴- ویژگی و مشخصه نهان نگار:

_ قابل درک[1] :

اگر نهان نگار پس از نهان نگاری توسط انسان قابل رؤیت و قابل تشخیص باشد، همانند قراردادن لوگو درگوشه تصاویر، نهان نگاری قابل درک (قابل رؤیت) است. نمونه نهان نگاری قابل درک در شکل ۱-۱ نشان داده شده است.

[1] Perceptible



شکل ۱-۱ نهان نگاری قابل رؤیت[۵۸]

_ غیر قابل درک[1] :

اگر نهان نگار قابل رؤیت نباشد نهان نگاری غیر قابل درک (غیر قابل رؤیت) است که کاربرد آن در پنهان سازی داده ها و کنترل حق تکثیر می‌باشد .

۱-۳-۵- مقاومت و شکنندگی :

_ مقاوم:

نهان نگاری که، نهان نگار در برابر انواع حملات عمدی و غیر عمدی مقاوم باشد و از بین نرود، نهان نگاری مقاوم است و کاربرد آن در پنهان سازی اطلاعات است.

_ شکننده:

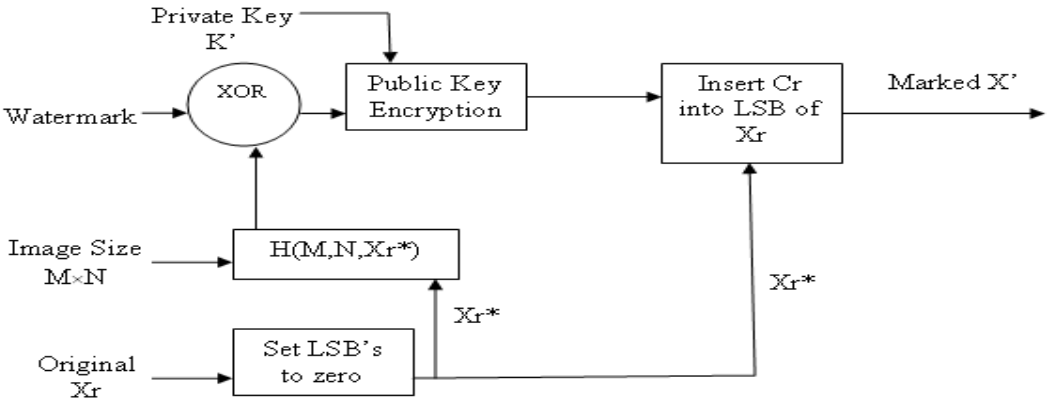
نهان نگاری که ، نهان نگار پس از هر نوع دستکاری و اصلاح بر روی تصویر نهان نگاری شده ، قابل تشخیص و استخراج نباشد نهان نگاری شکننده است، یعنی نسبت به کوچکترین اصلاح حساس می باشد. یک روش نهان نگاری شکننده توسط [۲۰] ارائه شده است. این روش بیت‌های با ارزش کمتر[2] پیکسل های تصویر را تغییر می دهد، از رمز نگاری کلید عمومی نیز استفاده می کند تا در مقابل حملات حساس تر باشد. بلاک دیاگرام این روش در شکل ۱-۲ نشان داده شده است.

---

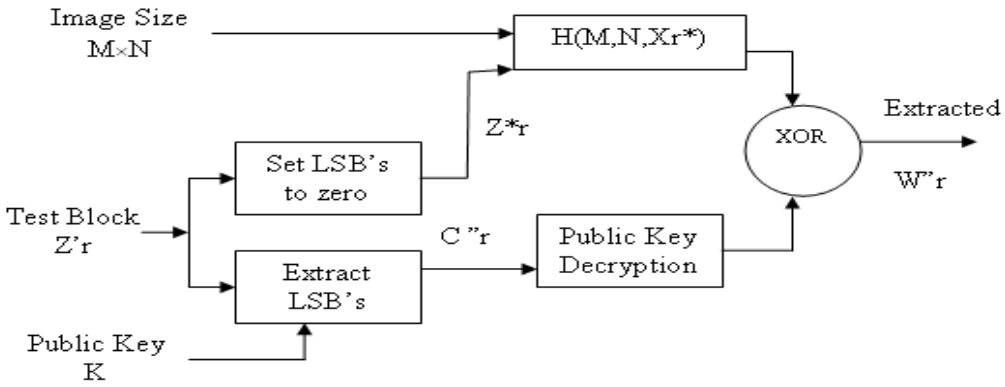
[1] Imperceptible
[2] Least Significant Bit (LSB)

_ نیمه شکننده[1] :

نهان نگاری نیمه شکننده در برابر دستکاری های مجاز مقاوم ودر برابر دستکاری های غیر مجاز حساس می باشد. این روش ها بیشتر برای کاربرد های تأیید سندیت بکار می روند.



(الف) نهان نگاری شکننده، فرآیند قرار دادن



(ب) نهان نگاری شکننده، فرآیند استخراج

شکل ۱-۲ نهان نگاری شکننده، روش ارائه شده توسط [۲۰]

۱-۳-۶- هدف و کاربرد واترمارکینگ:

_ کنترل تکثیر ، ردیابی

_ تأیید سندیت تصویر و کشف محل دستکاری[2]

[1] Semi-fragile
[2] Tamper detection

_ پنهان سازی داده و برچسب گذاری تصویر

۱-۳-۷- نوع داده میزبان :

_ تصاویر ثابت
_ ویدئو
_ صوت
_داده های مالتی مدیا خاص مانند نقشه ، کارتون

۱-۴-لزوم اجرای روش واترمارکینگ به منظور حفاظت از اطلاعات

_ اگرچه داده های دیجیتالی نسبت به آنالوگ ازمحاسن بیشتری برخوردارند، اما تولید کنندگان نسبت به ارائه سرویس های دیجیتالی راغب نیستند. به دلیل اینکه ازکپی برداری نامحدود وانتشار نسخه های کپی برداری شده که بازار را دچار بی اعتمادی می کند ، می ترسند.
_ به خاطر محتمل بودن قضیه ی کپی‌برداری می بایست از نقطه اصلی و قوت وسایل ضبط دیجیتالی محافظت شود [۲۱].
_ بسیاری ازکمپانی های صوتی و تصویری درابتدا از تولید مصالح DVDها به خاطر مسئله کپی برداری خودداری کردند. تااینکه بیانیه‌ی حقوق مصرف کننده و تولیدکننده دربرابر تهاجمات کپی برداری درسال۱۹۹۸به رسمیت شناخته شد[۲۲] و[۲۳] و [۲۴].

۱-۵-کاربردهای واترمارکینگ

- انگشت نگاری کردن[1]:

برای ردیابی منبع کپی برداری غیرقانونی، صاحب اطلاعات میتواند از تکنیک انگشت نگاری استفاده کند. به این ترتیب که صاحب اطلاعات میتواند با دادن سریال مخصوص به اطلاعات کپی شده آنها راپخش وارسال کند. سپس با مقایسه شماره سریال ومشتریانش متوجه شود که کپی برداری غیرقانونی توسط اطلاعات با کدام سریال انجام شده است. از آنجا که سریال ها را فقط صاحب اطلاعات در دست دارد متوجه می شود که کدام مشتری خاص مجرم و خطاکارمی باشد.

- محافظت از کپی برداری[2]:

[1] Fingerprinting
[2] Copy protection

اطلاعات ذخیره شده توسط واترمارک میتوانند بصورت مستقیم وسایل رکورد دیجیتالی را برای اهداف محافظت از کپی برداری کنترل کنند[۲۵]. بدین ترتیب که اطلاعات واترمارک اضافه شده بصورت یک بیت درسیگنال اصلی اضافه می شود و این نشان می دهد که داده غیرقابل کپی می باشد وآشکارسازهای واترمارک درثبات مشخص می کنند که آیا اطلاعات فرستاده شده به ثبات قابلیت ذخیره دارد یا نه.

- کنترل برانتشار داده ها :

با جاسازی کردن اطلاعات واترمارک به داده اصلی درآگهی های تجاری ،یک دستگاه هوشمند کنترلی میتواند مشخص کند که آیا این آگهی ها انتشار یافته اند یا نه![۲۶]. همچنین محصولات تلویزیونی نیز میتوانند با این روش دربرابر کپی شدن محافظت شوند و مشخص شوند که آیا درسایر دستگاه ها و شبکه های دیگر این اطلاعات لو رفته اند یا نه [۲۷].

آیتم های خبری ارزش فوق العاده زیادی دارند و آنها را دربرابر کپی برداری آسیب رسان می کند. یک سیستم نظارتی بر انتشار می تواند با چک کردن تمام کانال های انتشاری از صحت داده اصلی مطلع شود و با طرف مقابل قرارداد ببندد.

- سندیت اطلاعات :

واترمارک‌های ضعیف[۲۸] میتوانند برای چک کردن اعتبار یک داده بکار برده شوند. یک واترمارک ضعیف نشان می دهد آیا اطلاعات دچار تغییر شده اند یا نه!

تکنیک واترمارکینگ تنها به منظور حفاظت از اطلاعات بکار نمی رود وکاربردهای دیگری ازجمله موارد زیر را نیزداراست:

- شاخص گذاری:

درفهرست بندی ازاین تکنیک استفاده می شود. مثلا در فهرست بندی فیلم‌ها وآیتم‌های خبری که توسط موتور جستجو آشکار می شوند.

- ایمنی سلامت:

با قرار دادن تاریخ و اسم بیمار در تصاویر پزشکی می‌توان امنیت مفیدی را در این زمینه به وجود آورد[۲۶].

- مخفی کردن اطلاعات:

ازتکنیک واترمارکینگ همچنین درانتقال اطلاعات شخصی و... استفاده می‌شود. بعضی از نویسندگان[۲۹] از تکنیک واترمارکینگ با اضافه کردن چند بیت به داده اصلی جهت محافظت از اثر خود استفاده می کنند.

۱-۶- شاخص های ارزیابی روش های واترمارکینگ

برای ارزیابی روش های نهان نگاری شاخص هایی تعریف شده اند که با استفاده از آنها می توان روش مناسب با کاربرد مورد نظر را انتخاب نمود. شش شاخص اصلی تعریف شده عبارتند از : مقاومت[۱] ،ظرفیت[۲]، امنیت[۳] ،شفافیت[۴] (قابلیت رؤیت[۵]،غیر قابل درک بودن[۶])، قابل کشف نبودن[۷] و پیچیدگی[۸].از دیدگاه طراحی الگوریتم سه شاخص شفافیت،مقاومت وظرفیت بسیار مورد توجه قرار گرفته اند ولی معمولاً این سه شاخص با یکدیگر در تناقض هستند که باید بین آنها مصالحه ایی برقرار کرد. شاخص مقاومت نشان دهنده میزان باقی ماندن پیام درون تصویر پس از تغییراتی است که ممکن است به صورت عمدی یا مشکلات ناشی از خطوط انتقال ایجاد گردد، می باشد. ظرفیت ، بیانگر حجم اطلاعاتی است که می توان درون تصویر قرارداد و نهان نگاری کرد. امنیت بیانگر امکان کشف پیام به صورت تصادفی است که توسط عواملی چون کلید یا افزایش پارامتر ها تأمین می شود. شاخص شفافیت یکی از مهمترین نیازهای روش های نهان نگاری است و به معنای قابل تشخیص نبودن اطلاعات نهان نگاری توسط انسان است که به معنای غیر قابل رؤیت و غیر قابل درک بودن آن توسط سیستم بینایی انسان است. پیچیدگی نشانگر زمان و امکانات سخت افزاری مورد نیاز برای نهان نگاری و باز گشایی اطلاعات درون تصویر می-باشد .

باید توجه داشت که امکان بهینه سازی تمام شاخص ها همزمان وجود ندارد و با بهبود یکی، امکان تضعیف یک یا چند شاخص دیگر وجود خواهد داشت. بنابر این در هر روش با توجه به کاربرد میزان مناسبی از هر یک تأمین می گردد[۱]. [۳۰] وابستگی متقابل این شاخص ها و رابطه آنها را با کور یا غیرکور بودن نهان نگاری به صورت شکل ۱-۳ بیان کرده است.

---

[1] Robustness
[2] Capacity
[3] Security
[4] Transparency
[5] Visibility
[6] Imperceptibility
[7] Undetectability
[8] Complexity