واتر مارک دیجیتال

سعید سریزدی*

مسعود رشیدی‌نژاد**

* عضو هیأت علمی دانشکده مهندسی برق دانشگاه شهید باهنر کرمان، مرکز علوم و تکنولوژی پیشرفتهٔ ماهان.

** عضو هیأت علمی دانشکده مهندسی برق دانشگاه شهید باهنر کرمان و مرکز تکنولوژی اطلاعات دانشگاه شهید باهنر کرمان.

چکیده

نقش کاغذهای واترمارک در بانکداری بر کسی پوشیده نیست. توسعهٔ شبکهٔ جهانی اینترنت و تولد بانکداری اینترنتی این سوال را مطرح می سازد که آیا مفهوم واترمارک قابل تعمیم در این حوزه می باشد؟ در این مقاله ضمن توضیح واترمارکینگ دیجیتال به تشریح خواص و مفاهیم مرتبط با آن می‌پردازیم. هم‌چنین کاربردها و روش‌های موجود برای واترمارکینگ دیجیتال مورد بررسی قرار می‌گیرند. معرفی این زمینه می تواند چشم اندازهای جدیدی را در سیستم نوین بانکداری فراهم نماید.

واژه‌های کلیدی: واترمارک دیجیتال، احراز سندیت، نهان‌نگاری، رمزنگاری.

۱- مقدمه

توسعهٔ روزافزون شبکهٔ اینترنت چشم‌اندازها و مفاهیمی جدیدی در عرصه‌های مختلف از جمله تجارت، اقتصاد، مدیریت، مخابرات، توریسم و غیره ایجاد کرده است. از سوی دیگر امکان کپی و جعل آسان تصاویر و مدارک دیجیتالی، لزوم طراحی و ابداع روش‌های موثر و جدید تامین امنیت این‌گونه مدارک را ایجاب می‌نماید. روش‌های موجود اثبات سندیت مدارک دیجیتال را می‌توان به دو گروه زیر دسته‌بندی نمود:

- روش‌های مبتنی بر "امضای دیجیتال"[1]
- روش‌های مبتنی بر "واتر مارک"[2]

در روش‌های مبتنی بر "امضای دیجیتال"، سندیت مدرک دیجیتال با بررسی مجموعه‌ای از ویژگی‌های منحصر به فرد تصویر -که رمزنگاری گردیده و در فایلی جداگانه به‌همراه تصویر ارسال می‌گردد- اثبات می‌شود.

در "واترمارکینگ" هدف احراز سندیت و یا محافظت از تصویر است که این مهم با قراردادن اطلاعات تصویری در داخل یک تصویر؛ "مثلا یک آرم و یا یک شمارهٔ سریال" که معمولاً به‌صورت غیر مرئی است صورت می‌پذیرد.

ایدهٔ "واترمارک دیجیتال" از نحوهٔ استفاده از کاغذهای واترمارک در احراز سندیت مدارک رسمی نظیر تمبر و اسکناس الهام گرفته شده است. ساخت اولین کاغذ واترمارک به‌عنوان هنری دستی در سال ۱۲۹۲ و در شهر "فابرینو" در ایتالیا صورت پذیرفت. این اختراع تحولی جدید در صنایع کاغذسازی ایجاد کرد؛ به‌نحوی که در سال‌های پایانی قرن سیزدهم میلادی، کاغذهای واترمارک در اندازه، کیفیت و قیمت‌های متفاوت توسط ۴۰ کارگاه کاغذسازی در فابرینو تولید و در فروشگاه‌های این شهر در معرض فروش قرار داشتند. به‌زودی کاغذهای واترمارک در سرتاسر ایتالیا و سپس اروپا توسعه پیدا کردند. به‌علت پیچیدگی کپی و جعل کاغذهای واترمارک، این کاغذها جایگاه خویش را در اسناد و اوراق بانکی تثبیت نمودند. به‌عنوان

[1] digital signature
[2] digital water mark

مثالـی زیـبا از نقش واترمارک در احراز سندیت، می‌توان به واقعه‌ای که در سال ۱۸۸۷ در فرانسه اتفـاق افـتاد، اشـاره کـرد: واترمارک‌های موجود در دو نامه به‌عنوان دلیل و اثباتی قاطع در مورد تـاریخ نوشـته‌شدن آن‌ها در دادگاهی علیه یکی از نمایندگان مجلس مورد استفاده قرار گرفت که نتیجهٔ آن، تبرئهٔ یک مامور پلیس، سقوط کابینه و استعفای رییس‌جمهور "گروی" بود.

نخستین مقالات علمی در زمینهٔ واترمارک دیجیتال در سال ۱۹۹۰ توسط تاناکا[1] و سپس در سـال ۱۹۹۳ توسـط تیرکل[2] و همکاران به چاپ رسیدند. "واترمارک‌های دیجیتال" را می‌توان به دو دسته تقسیم نمود:

- واترمارک مرئی: واترمارک مرئی عبارت است از یک الگوی بینایی مشخص (نظیر یک آرم، برچسـب یـا لوگـو) که به‌صورت مرئی و قابل دیدن در تصویر قرارداده می‌شود. از ایـن نوع واترمارک معمولا در تصاویر اینترنتی، و به‌منظور جلوگیری از استفادهٔ تجاری از ایـن تصـاویر، اسـتفاده مـی‌شود. لازم به ذکر است که نحوهٔ الصاق این واترمارک‌ها بایستی به‌نحوی باشد که به راحتی قابل حذف و یا جعل نباشند.
- واتـرمارک نامرئی: چنین واترمارکی، بعد از قرار گرفتن در تصویر قابل رویت نمی‌باشد. ایـن واتـرمارک نـیز بایسـتی در مقابل حذف و جعل - حتی وقتی که دشمن علی‌رغم نامرئی بودن آن از وجود آن آگاه است- مقاوم باشد.

در ایـن مقالـه و در قسمت بعدی به معرفی دقیق‌تر "واترمارک دیجیتال"، انواع و مفاهیم مرتبط با آن می‌پردازیم. در قسمت سوم کاربردهای مختلف واترمارک دیجیتال مورد بررسی قرار مـی‌گـیرند و نهایت، در قسمت چهارم به جمع‌بندی و چشم‌انداز استفاده‌های ممکن از "واترمارک دیجیتال" دریک شبکهٔ بانکی پرداخته خواهد شد.

---

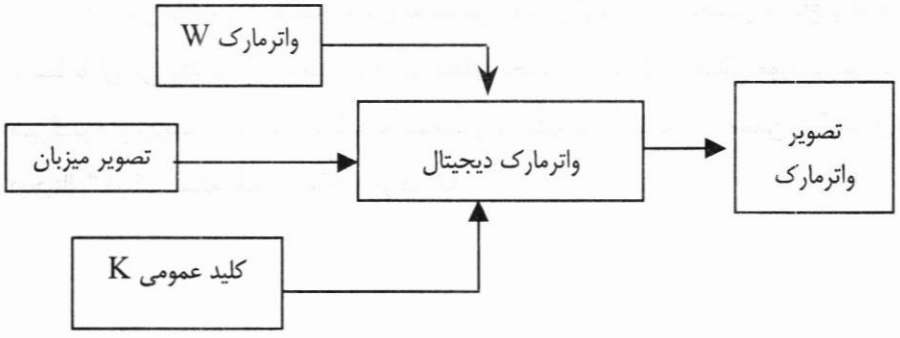
[1] Tanaka, 1990.
[2] Tirkel, 1993.

۲- بررسی روش‌های واترمارک دیجیتال

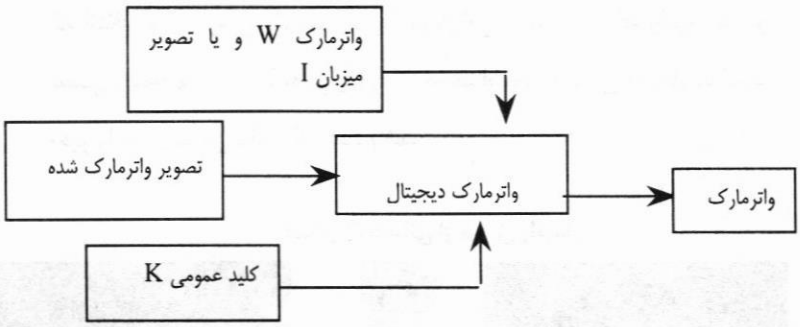
توسعه روزافزون و سریع شبکه‌های کامپیوتری، زمینه‌ای مناسب برای توزیع سریع و آسان اطلاعات دیجیتال نظیر تصویر، صوت و ویدیو را فراهم کرده است. به دلیل سهولت امکان تکثیر و استفادهٔ غیر مجاز، اهمیت روش‌های تضمین‌کنندهٔ امنیت افزایش یافته است. در سال‌های اخیر، مسألهٔ واترمارک دیجیتال به عنوان راه‌حلی مناسب و کارآمد مورد توجه قرار گرفته است. هدف از یک سیستم واترمارک، قرار دادن علائم واترمارک - که ممکن است یک آرم، اطلاعات مربوط به کپی رایت و یا یک عدد باشد- در داخل سند و یا تصویر دیجیتال است. نمودارهای (۱)و (۲) ساختار کلی یک سیستم واترمارک دیجیتال را به اختصار نشان می دهند.

از نظرحوزهٔ اعمال واترمارک، سیستم‌های واترمارک به دو دستهٔ حوزهٔ مکان و حوزهٔ فرکانس تقسیم‌بندی می‌شوند. ساده‌ترین نوع واترمارکینگ با قرار دادن اطلاعات واترمارک بر روی بیت با ارزش کمتر مقادیر پیکسل‌ها حاصل می‌گردد. اشکال اساسی واترمارک‌های حوزهٔ مکان به‌طور اعم و واترمارک بیت با ارزش کمتر به‌طور خاص، شکننده بودن آن‌ها (حذف و یا جعل ساده) است. هر چند که در مقایسه با روش‌های حوزه فرکانس از خاصیت نامرئی‌بودن بهتری برخوردار هستند.

نمودار (۱) : شمای کلی ساختار تزریق واترمارک



نمودار (۲) : ساختار بازیابی واترمارک



بـه‌طـور کلـی خصوصـیاتی که از یک سیستم واترمارک کارآمد انتظار داریم به شرح زیر است:

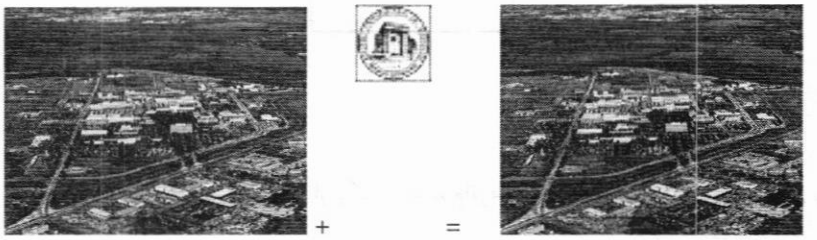
- نامرئـی بودن: تغییرات داده‌شده در تصویر بایستی به اندازهٔ کافی جزئی باشند تا نامرئی بودن واترمارک تضمین شود.
- انعطـاف‌پذیـری: واتـرمارک بایسـتی بـه انـدازهٔ کافـی در مقـابل تبدیل‌های متعارف و اسـتاندارد تصـویر مقـاوم باشـد. از ایـن تـبدیل‌ها می‌توان به فشرده‌سازی JPEG و یا تغییرکنتراست و یا میزان رنگ تصویر نام برد.
- کلید رمزنگاری: بیشتر سیستم‌های واترمارک از یک یا چند کلید سرّی رمزنگاری بهره می جویند. این امر امنیت واترمارک را افزایش می دهد.

عـلاوه برخصوصـیات عمومـی فوق الذکر، بسته به کاربرد واترمارک خصوصیات زیر ممکن است مدنظر قرار گیرند:

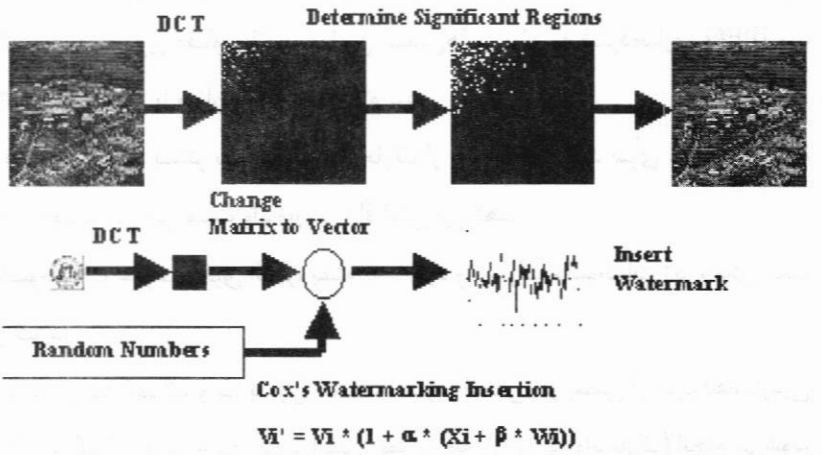
- بازیابـی بـه کمـک و یـا بـدون کمـک تصـویر اصـلی: در بعضی از کاربردها، بازیابی واتـرمارک از مقایسـه بـا تصویر اصلی(تصویر قبل از تزریق واترمارک) انجام می‌شود، بنابرایـن، در چنیـن کاربردهایی دسترسی به تصویر اصلی ضروری است. در بسیاری از کاربردها لازم است که بازیابی واترمارک بدون استفاده از تصویر اصلی صورت پذیرد.

- نحـوهٔ استخراج یا بررسی وجود یک واترمارک مشخص: بسته به کاربرد، ممکن است که انتظار ما از بازیابی واترمارک تنها تعیین این مطلب باشد که واترمارک مورد نظر در تصـویر موجـود است یا نه، و یا این‌که هدف استخراج دقیق واترمارک است. در حالت اخیر واتر مارک می‌تواند یک عدد باشد.

نمودار (۳): مثالی از تزریق واترمارک



نمودار (۳) مثالی از یک سیستم واترمارک (الگوریتم کوکس) را نشان می دهد.



۲-۱- روش‌های حوزه مکان

ساده‌ترین راه برای تزریق واترمارک در داخل یک تصویر در حوزهٔ مکان، افزودن یک دنبالهٔ شبه تصادفی به مقادیر سطح خاکستری پیکسل‌های تصویر است. این دنبالهٔ تصادفی معمولا مقادیر ۰، ۱ و یا ۱- را اختیار می‌کند. عمل تزریق با ضرب دنبالهٔ شبه تصادفی در یک ضریب کوچک و افزودن آن به تصویر میزبان انجام می‌شود. لازم به ذکر است که دنبالهٔ شبه تصادفی با اعمال یکی از روش‌های شناخته شدهٔ رمزنگاری به دنبالهٔ اطلاعات واترمارک توسط یک کلید رمزنگاری که به‌طور تصادفی انتخاب گردیده است، حاصل می‌شود. استفاده از کلید تصادفی به منظور افزایش امنیت سیستم است. عمل استخراج و یا تشخیص واترمارک، با محاسبهٔ همبستگی بین تصویر واترمارک‌شده و دنبالهٔ شبه تصادفی و مقایسهٔ مقدار آن با یک حد آستانه انجام می‌شود. بنابراین، در این روش‌ها جهت تشخیص واتر مارک نیازی به تصویر اصلی نیست هر چند که دنبالهٔ شبه تصادفی و البته کلید رمز ضروری هستند.

در مرحلهٔ تشخیص واترمارک، دو نوع خطا ممکن است اتفاق بیفتد:

- ممکن است حضور واترمارک تایید شود حال آن‌که واترمارکی وجود نداشته باشد، به‌این نوع خطا، خطای مثبت گفته می‌شود.
- حضور واترمارک تایید نمی شود، در حالی‌که واترمارک وجود دارد. این خطا را خطای منفی می‌نامند.

۲-۲- روش‌های حوزهٔ تبدیل

در این روش‌ها، واترمارک به جای تزریق در تصویر میزبان، در تبدیل‌یافتهٔ آن تزریق می‌شود. یکی از این روش‌ها، تزریق واترمارک در داخل فاز تبدیل فوریهٔ گسستهٔ (DFT) تصویر میزبان است. این روش از مقاومت خوبی برخوردار است زیرا چشم نسبت به اعوجاج فاز حساس است و هرگونه دست‌کاری در مولفه‌های فاز به‌منظور حذف و یا جعل واترمارک، سبب تنزل جدی در کیفیت تصویر می‌شود. از سوی دیگر، قرار دادن اطلاعات مربوط به واترمارک در فاز تصویر براساس مباحث تئوری مخابرات، مدولاسیون فاز تلقی می‌گردد و نشان داده شده است که

مدولاسیون فاز دارای امنیت نویز بالاتری نسبت به مدولاسیون دامنه (واترمارک‌های حوزهٔ مکان) می‌باشند. مزیت دیگر واترمارک حوزهٔ تبدیل فوریهٔ گسسته، مقاوم بودن آن در مقابل چرخش و جابجایی (انتقال) تصویر است.

حوزهٔ متداول دیگر برای تزریق واترمارک، حوزهٔ تبدیل کسینوسی گسسته (DCT) است. از آنجا که حساسیت سیستم بینایی انسان به فرکانس‌های پایین بیشتر است، درج واترمارک در مولفه‌های بالایی DCT به‌منظور دست‌یابی به نامرئی بودن واترمارک، مناسب به‌نظر می‌رسد. از طرف دیگر، از آنجا که در برخی از روش‌های فشرده‌سازی تصویر - از جمله روش استاندارد JPEG – مؤلفه‌های DCT کوانتیزه می‌شوند و گام کوانتیزاسیون درمورد فرکانس‌های بالا، بزرگ‌تر می‌باشد (به علت حساسیت کمتر سیستم بینایی نسبت به این فرکانس‌ها)، درج واترمارک در فرکانس های بالاتر موجب کاهش مقاومت واترمارک می‌گردد. بنابراین به‌منظور دست‌یابی هم‌زمان به نامرئی بودن و مقاومت مناسب، معمولاً فرکانس‌های میانی جهت تزریق واترمارک انتخاب می‌گردند.

یکی از روش‌های درج درحوزهٔ DCT ، روش درج مستقل از تصویر است. در این روش، ابتدا تصویر به بلوک های ناپوشای ۸×۸ تقسیم و سپس ضرائب DCT بلوک‌ها محاسبه می‌گردند. در قدم بعدی، این ضرایب هماهنگ با روش JPEG و مطابق شکل(۴)با ترتیب زیگزاگی مرتب می‌شوند. سپس فرکانس‌های میانی و پایینی- ضرایب (L+۱)ام تا (L+M)ام در ترتیب زیگزاگی- جهت درج واترمارک انتخاب می‌گردند. تزریق واترمارک به داخل ضرایب DCT توسط رابطهٔ زیر انجام می‌شود:

$$I_{DW}(L+i) = I_D(L+i) + k.\ W_D(i)$$

در رابطهٔ فوق، I_{DW} ضرایب DCT پس از تزریق واترمارک، I_D ضریب DCT انتخاب شده، W_D اطلاعات واترمارک و K بهره است.

جدول (۱) : نحوهٔ مرتب سازی ضرایب DCT

۰	۱	۵	۶	۱۴	۱۵	۲۷	۲۸
۲	۴	۷	۱۳	۱۶	۲۶	۲۹	۴۲
۳	۸	۱۲	۱۷	۲۵	۳۰	۴۱	۴۳
۹	۱۱	۱۸	۲۴	۳۱	۴۰	۴۴	۵۳
۱۰	۱۹	۲۳	۳۲	۳۹	۴۵	۵۲	۵۴
۲۰	۲۲	۳۳	۳۸	۴۶	۵۱	۵۵	۶۰
۲۱	۳۴	۳۷	۴۷	۵۰	۵۶	۵۹	۶۱
۳۵	۳۶	۴۸	۴۹	۵۷	۵۸	۶۲	۶۳

در نهایت I_{DW} جایگزین مقادیر قبلی ضرایب DCT می‌شود، سپس با محاسبهٔ تبدیل معکوس، تصویر واترمارک شده به‌دست می‌آید.

روش دیگر برای درج درحوزهٔ DCT، روش درج وابسته به تصویر است. در این روش نیز همانند روش قبلی از یک ناحیهٔ انتخاب‌شده در حوزهٔ DCT تصویر استفاده می‌شود، این روش مقاوم‌تر از روش قبلی است و از رابطهٔ زیر بهره می‌جوید:

$$I_{DW}(L+i) = I_D(L+i) + k \times I_D(L+i) \times W_D(i)$$

در دو روش اخیر، جهت آشکارسازی واترمارک، استفاده از تصویر اصلی ضروری است. روش دیگری که در آن آشکارسازی کور (آشکارسازی بدون استفاده از تصویر اصلی) امکان‌پذیر است، روش خود تشابه است. در این روش درج واترمارک در فرکانس‌های میانی و توسط رابطهٔ زیر صورت می‌گیرد:

$$I_{DW}(L+i) = I_D(L+i) + k \times |I_D(L+i)| \times W_D(i)$$

برای آشکارسازی کور، ابتدا ضرایبDCT تصویر واترمارک‌شده محاسبه وبه فرم زیگزاگ مرتب می‌شوند، سپس همبستگی میان این ضرایب و سیگنال واترمارک حساب شده و با یک مقدار آستانه مقایسه می‌گردد.

از دیگـر روش‌هـای حوزهٔ تبدیل، می‌توان از روش طیف گسترده و یا روش‌های مبتنی بر تبدیل‌های دیگر نظیر هادامارد، تبدیل کارونن لوو، تبدیل اسلانت و تبدیل موجک نام برد.

۳ - کاربردهای واترمارک دیجیتال

شـرایطی کـه یـک واترمارک کارآمد بایستی ارضا کند در حالت کلی به کاربرد واترمارک بسـتگی دارد. در ایـن فصـل مـا به تعدادی از کاربردهای مهم سیستم واترمارک دیجیتال اشاره می‌کنیم:

۳-۱- واترمارک برای اعمال حق کپی رایت

یکی از شایع‌ترین کاربردهای واترمارک دیجیتال استفاده از آن جهت حفاظت از حق کپی رایـت اسـت. هـدف از این کاربرد واترمارک، قراردادن اطلاعاتی در تصویر است که به کمک آن بتوان مالکیت را اثبات نمود. به‌عبارت دیگر، هدف اثبات حق مالکیت است و نه سد نمودن امکان کپـی‌برداری. بنابراین، این واترمارک بایستی از انعطاف‌پذیری بالایی برخوردار باشد. هم‌چنین باید در مقابل حذف و جعل مقاوم باشد.

۳-۲- واترمارک به‌عنوان اثر انگشت

درکاربـرد اخـیر، واترمارک حاوی اطلاعاتی در مورد استفاده‌کنندهٔ مجاز است و برخلاف کاربرد قبلی شامل اطلاعات مالک نمی‌باشد. به‌این ترتیب استفاده‌کنندهٔ مجاز، استفاده‌کننده است که اطلاعات وی در واترمارک آمده است. به این کاربرد اصطلاحا انگشت‌نگاری[1] اطلاق می‌شود. این واترمارک نیز مانند واترمارک کپی‌رایت بایستی انعطاف‌پذیر و مقاوم باشد.

۳-۳- واترمارک برای احراز سندیت تصویر

در احـراز سـندیت هـدف تشـخیص ویرایش احتمالی اطلاعات و یا تصویر است. به‌این مـنظور معمولاً از واترمارک‌های شکننده استفاده می‌شود. واترمارک شکننده، واترمارکی است که

[1] fingerprinting

از انعطاف‌پذیری کمی برخوردار است و بنابراین هر ویرایش غیر مجاز روی تصویر، منجر به مخدوش شدن واترمارک گردیده و دست‌کاری‌شدن مدرک تصویری آشکار می‌گردد.

۳-۴- واترمارک برای جلوگیری از کپی‌گرفتن

در سیستم‌های توزیع و فروش از طریق محیط‌های چند رسانه‌ای (نظیر اینترنت)، ایده‌آل این است که به‌توان به نحوی از کپی‌گرفتن جلوگیری نمود. هرچند که این کار در مورد سیستم‌های باز بسیار پیچیده است، اما در مورد شبکه های بسته و یا خصوصی امکان پذیر است. به‌عنوان مثالی از این نوع واترمارک می‌توان از سیستم DVD نام برد. در چنین سیستمی، اطلاعات مربوط به وضعیت کپی‌گرفتن در واترمارک قرارداده می‌شود و بنابراین دستگاه DVDPlayer اقدام به تکثیر فایل‌هایی که واترمارک آن حاوی پیام "کپی هرگز" باشد نمی‌نماید.

۴- جمع بندی

گسترش روزافزون شبکهٔ اینترنت بابی جدید را در ارائه سریع و موثر خدمات گشوده است. ازطرف دیگر گستردگی شبکه و سادگی دسترسی به آن، تمهیداتی ویژه جهت تامین امنیت سیستم را می‌طلبد. واترمارک دیجیتال پاسخی مناسب به این نیاز است. در این مقاله ضمن تشریح واترمارک دیجیتال و مفاهیم مرتبط با آن، به معرفی برخی از کاربردهای آن پرداختیم.

شک نیست که با توجه به کارآیی سیستم واترمارک دیجیتال و فلسفهٔ وجودی آن که از کاغذهای واتر مارک الهام گرفته شده است و هم‌چنین با عنایت به نقش مهم و انکارناپذیر واترمارک در اسناد و سیستم بانکی، می‌توان کاربردهایی زیبا از آن در سیستم نوین بانکی تصور نمود.

از جملهٔ کاربردهای نوعی، می‌توان به بررسی سندیت مدارک از روی کپی آن‌ها و درنتیجه امکان ارسال و دریافت ایمن مدارک از طریق شبکهٔ اینترنت، تشخیص صحت مدارک شناسایی عکس‌دار که تصویر آن‌ها از طریق اینترنت دریافت شده‌اند (در حالی‌که جعل این

مدارک با تعویض عکس و سپس تهیهٔ کپی آسان به‌نظر می‌رسد) اشاره نمود. با توجه به نو بودن زمینه و قدرت وکارآیی بالای روش‌های واترمارک دیجیتال، انتظار می‌رود که گسترش این روش‌ها در سیستم بانکی نوین، موجب تحولی بزرگ در خدمت رسانی بانکی گردند.

منابع و مآخذ

– Bloom, J., A., et al., (1999), ***"Copy Protection for DVD Video"***, Proceedings of the IEEE, Vol. 87, No. 7.

– Katzenbeisser, S., Petitcolas,F, (2000) ***"Information Hiding Techniques for Steganography and Digital Watermarking"***, Artech House Editions.

– Langelaar,G. and C.,et al., (1999) ***"Watermarking Digital Image and Video Data"***, IEEE Signal Processing Magazine, 1053-5888.

– Lee, W. and Chen, T. (2002) ***"A Public Verifiable Copy Protection Technique for Still Images"***, The Journal of Systems and Software, No. 62, pp. 195-204.

– Petitcolas, F., Anderson, R. J. and Kuhn, M. J. (1999) ***"Information Hiding: A Survey"***, Proceeding of IEEE special issue on Protection of Multimedia Contents.

– Tanaka, K., Nakamura,Y. and Matsui, K. (1990) ***"Embedding Secret Information into a Dithered Multilevel Image"***, Proceeding of the 1990 IEEE Military Communications Conference, pp. 216-220.

– Tirkel, A. et al. (1993) ***"Electronic Water Mark"***, Proceedings of DICTA, pp. 666-672.