# آشنایی با فناوری واترمارکینگ

زهره محسن پور

استاد دانشگاه آزاد اسلامی شیراز-استاد دانشگاه علوم پزشکی شیراز- فیزیست بخش رادیوتراپی و هسته ای بیمارستان نمازی شیراز

Z_MOHSENPOUR@YAHOO.COM

**چکیده :**

**با توجه به گسترش روز افزون ارتباطات در دنیای امروز ، ضرورت کنترل بهینه ارتباطات در محیطهای گوناگون اداری ، چندرسانه ای ، فیزیکی ، دیجیتالی و امنیتی بیش از پیش روشن می شود. دانش هوش مصنوعی از زیر مجموعه های مهم در دانش کامپیوتر ، در این زمینه گامهای بلندی برداشته است. حفاظت از داده ها در مقابل کپی برداری و جعل از اهمیت بالایی برخوردار است به همین دلیل باید از راهکارهایی برای کنترل کپی کردن استفاده نمود. یکی از این راهکارها ، استفاده از تکنیک واتر مارکینگ می باشد.واتر مارکینگ به معنای پنهان کردن داده ها در تصاویر است به نحوی که با چشم قابل تشخیص نباشد و فقط افراد مجاز قادر به استخراج این داده ها باشند.در این مقاله سعی شده است تا مخاطب با فناوری نوپای واترمارکینگ که تلفیقی از دانش هوش مصنوعی و رمزگذاری سنتی به شمار می رود ، آشنایی عمومی پیدا کند. درابتدا به تاریخچه مختصری از رمزگذاری از ابتدا تاکنون اشاره می شود. سپس با معرفی واترمارکینگ و کاربردهای آن ، بحث را به پایان خواهم رساند.**

**واژه های کلیدی :**

واتر مارکینگ، پنهان نگاری ، ، پنهان شناسی ، واتر مارکینگ دیجیتال

**مقدمه :**

در قرن ارتباطات ، به دلیل گسترش روز افزون ارتباطات جهانی و ابداع کانالهای ارتباطی گوناگون نظیر شبکه اینترنت ، ارتباطات ماهواره ای و مخابراتی دیگر ، اطلاعات به راحتی در اختیار طیف گسترده ای از مردم در سر تا سر دنیا قرار میگیرد .

تا چندی پیش ژورنال های معتبر بین المللی ، مقالات ، متون علمی ، داده های محرمانه یا مکاتبات اداری صرفا بصورت فیزیکی و کاغذی وجود داشت و هر یک در اختیار طیف محدودی از کاربران قرار می گرفت. به همان نسبت استفاده های غیر قانونی یا سوء استفاده از آنها یا جعل چنین اسنادی به دلیل عدم دسترسی آسان و همچنین نیاز به شگردهای خاص ، سخت تر و محدودتر بود اما امروزه ورود فناوری های دیجیتال به نظامهای اداری سر تا سر دنیا و به زندگی عموم مردم ، وجود شبکه جهانی اینترنت و سایر کانالهای ارتباطی ، دسترسی آسان تر به اطلاعات را فراهم ساخته است . امروزه نظامهای اداری " فاقد کاغذ " گسترش یافته است. از اینرو بسیاری از اسناد و اطلاعات در قالب داده های دیجیتالی تهیه و عرضه می شود.

این داده ها میتوانند در قالب های گوناگون نظیر متنی ، کتب الکترونیکی ، تصاویر ساکن ، تصاویر متحرک ، فیلم ، پایگاه های داده ، نرم افزارها ، بازیهای کامپیوتری یا انواع دیگر باشد. ماهیت دیجیتالی داده

ایجاب میکند که ایجاد ، تغییر ، به روز آوری ، اصلاحات ، اشتراک گذاری ، ذخیره و انتشار اطلاعات آسانتر از قبل شده باشد .[1]
از اینرو دسترسی و تبادل آزاد اطلاعات ، به همان نسبت امکان سوء استفاده از داده ها را بالاتر میبرد. بنابراین اهمیت و ضرورت پنهان سازی محتوای اطلاعات در اینجا روشن می شود.

**دانش "هوش مصنوعی" به خدمت گرفته میشود :**

سطوح پیشرفته تر دانش کامپیوتر بر آن است تا در این زمینه، چاره اندیشی کند. از جمله شاخه های مهم در این زمینه دردانش کامپیوتر ، شاخه " هوش مصنوعی" و زیرمجموعه "پردازش تصویر " میباشد.

**واترمارکینگ چیست ؟**

آنچه اول بار از "پنهان سازی" اطلاعات به ذهن افراد خطور می کند شاید،روش های متداول رمز گذاری باشد.در حالی که رمزگذاری شاید به تنهایی کافی نباشد. بعنوان مثال نقض در این مورد ، میتوان به سناریوی " فرار زندانی " که نخستین بار در سال ۱۹۸۳ توسط شخصی بنام سیمونز طرح شد ، اشاره نمود. [2]
برای حل اینگونه اشکالات در مسیر حفاظت اطلاعات تکنیکهای جدیدتر، از جمله تکنیک واترمارکینگ رو به گسترش است که در ادامه با آن آشنا خواهیم شد.با نگاهی تاریخی بر ماجرا در می یابیم که پنهان سازی اطلاعات ، قدمتی دیرینه دارد. البته روشهای پنهان نگاری در قدیم بسیار ابتدایی و متفاوت و گاه عجیب بوده اند. ترجیحا به تاریخچه مختصری در این باب بسنده می کنیم.

**تاریخچه ای از پنهان سازی اطلاعات :**

کریپتوگرافی و استگانوگرافی ( متدهای پنهان سازی اطلاعات ) هر کدام سیر تکاملی خود را از سالهای دور تاکنون پیموده اند : [3,4,5,6]

- ردپای رمز کردن اطلاعات را اول بار میتوان در حوالی سال ۱۹۰۰ پیش از میلاد جست، که در آن زمان مصریان باستان از نوعی الفبای هیروگلیف نا متعارف درکتیبه های خطی خود استفاده میکردند.
- در حدود ۵۰۰ سال قبل از میلاد ، یهودیان از الفبای "آتباش"که نوعی الفبای رمز وارونه است استفاده میکردند.
- در حدود سال ۵۰ تا ۶۰ قبل از میلاد "جولیوس سزار" از نوعی الفبای رمز برای مکاتبات حکومتی استفاده میکرد.
- طبق روایت هرودوت- مورخ یونانی – فرمانروای یونانی بنام "هیستیائوس " برای رساندن فرمان شورش علیه ایرانیان ، پیغام محرمانه خود را بر سر تراشیده یکی از بردگان معتمد خود خالکوبی کرد.
- هرودوت همچنین نقل میکند که " دمراتوس " پیام هشدار حمله دشمن را بر قرصهایی چوبی مینوشت و به مخاطب میرساند.
- سیر تکاملی رمز کردن اطلاعات همچنان ادامه یافت.رد پای رمز کردن داده در اروپای قرون وسطی نیز دیده میشود.
- شکسپیر و فرانسیس بیکن نیز از این متد ها استفاده میکردند.
- *در در زمان محاصره پاریس در جنگ سال ۱۸۷۰ ، برای رساندن نامه توسط کبوتران نامه بر ، از رمزگذاری استفاده میشد.
- *در جنگ جهانی دوم ، آلمانیها روش " ریز نقطه " را برای رمز گذاری مکاتبات محرمانه خود ابداع کردند.
- در زمان جنگ سرد ، آمریکا و شوروی نیز از رمز گذاری استفاده میکردند.
- در جنگ آمریکا ، نیروهای انگلستان و آمریکا هر دو ، از نوعی جوهرهای نامرئی برای رمز گذاری استفاده کردند.

- خانم مارگارت تاچر –نخست وزیر پیشین انگلستان- که از درزکردن اطلاعات محرمانه کابینه اش به بیرون ، ناخرسند بود ، در دهه ۱۹۸۰ از نوعی نرم افزار واژه پردازی برای کد کردن هویت نویسنده و شناسایی وزرای جاسوس و خائن کابینه اش استفاده کرد.
- امروزه سیر تکاملی کریپتوگرافی تا کریپتوگرافی کوانتومی وسایفرینگ در دنیای دیجیتال و رمز گذاری و . . . گسترش یافته است . DNA بر * در استگانوگرافی نیز پیشرفتهای قابل توجه مشابه ادامه دارد.
- واتر مارکینگ نیز بعنوان یک تکنیک در فرآیند استگانوگرافی امروز مورد توجه واقع شده است.

**تعاریف اولیه ، شباهت ها ، تفاوت ها :**

به رمز کردن محتوای یک پیام ، (Cryptography) گفته میشود.cryptography رمزنگاری به معنای "رمز" Crypto کریپتوگرافی از ریشه یونانی گرفته شده است. در فایل سیستم (Encryption) فرآیند رمزنویسی در محیط شبکه ای از Ciphering و فرآیند NTFS نوع جمله تکنیکهای کریپتوگرافی هستند. و به فرآیند رمزگذاری اصطلاحا فرآیند Encrypt گفته می شود. برای آنکه Decrypt رمزگشایی اصطلاحا رمزگشایی امکانپذیر گردد ، فرستنده پیام،حتما بایستی را برای گیرنده (Decryption Key)کلید رمزگشایی بفرستد.این کلید نبایستی در اختیار موجودیت دیگری غیر از گیرنده قرار بگیرد. کریپتوگرافی ذاتا انگیزه خرابکاران را برای یافتن الگوریتمها و راه های رمزشکنی بالا میبرد .به پنهان کردن وجود پیام رمز Steganography، گفته می شود. (Steganography )پنهان نگاری به معنای Stegano استگانوگرافی از ریشه یونانی "پنهان " گرفته شده است. [7,8]

در استگانوگرافی وجود پیام رمز اساسا انکار میشود. یک تفاوت مهم استگانوگرافی و کریپتوگرافی در آن است که استگانوگرافی حتما به میزبانی یک محیط ثانویه ( تک رسانه یا چند رسانه ای ) انجام پذیر است. بعنوان تفاوتی دیگر ، در استگانوگرافی به وجود کلید رمزگشایی نیازی نیست.اما برای پی بردن به وجود یا عدم وجود رمز نیاز داریم.Detect شناسایی در استگانوگرافی رمز ضمیمه شده به میزبان ، بایستی کمترین صدمه را به محتوای میزبانش وارد کند.

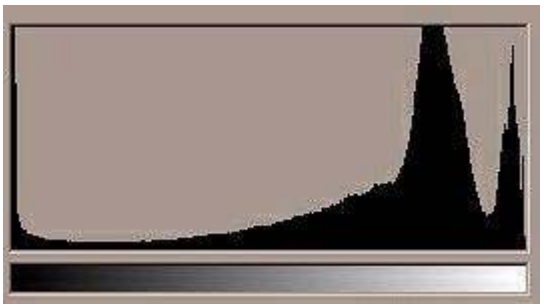
شکل ۱:تصویر اصلی که به صورت کاشی شده در آمده است.

شکل۲:گسترش یافته چشم سمت چپ شکل ۱

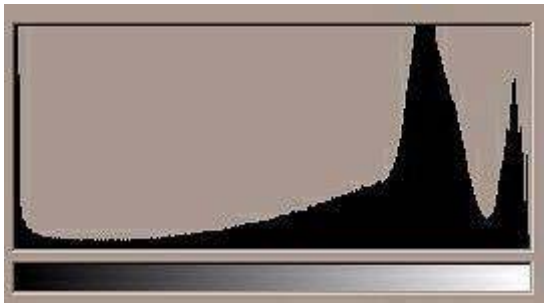
وجه برتری ذاتی پنهان نگاری در آن است که از آنجا که وجود پیام رمز از منظر عموم مخفی میگردد ، به همان نسبت تلاشهای و انگیزه های رمزشکنی فروکش میکند.نکته مهم آن است که ، نباید استگانوگرافی را بعنوان جایگزین برای کریپتوگرافی تصور کرد. بلکه استگانوگرافی مکمل مناسبی برای کریپتوگرافی بشمار میرود.برای بالا بردن ضریب امنیت و اطمینان ، میتوان از کریپتوگرافی و استگانوگرافی بصورت ترکیبی و همزمان استفاده کرد. همان طور که در شکل های شماره ۳و۴ مشاهده می شود از لحاظ ظاهری این دو شکل با هم تفاوتی ندارند.اما در تصویر شماره ۴ متن هایی مخفی شده است.سایز عکس اصلی ۲۳۵۹۳۵۲ بایت وسایز عکسی که متن در آن ذخیره شده است ۲۳۵۹۳۵۰ بایت می باشد.[10]

شکل ۳: تصویر ا. با پسوند bmp

شکل ۴: تصویر اصلی شکل ۳ که متن درآن ذخیره شده است[10]



شکل ۵ :نمودار هیستوگرام مربوط به تصویر شماره ۳



شکل ۶:نمودار هیستوگرام مربوط به تصویر شماره ۴[10]

با توجه به دو نمودار هیستوگرام فوق تغییر کمی را در شکل سمت چپ می بینیم که نشان دهنده این است که متن در تصویر ۴ ذخیره شده است.

واترمارکینگ شاخه ای از فرآیند : Watermarking پنهان نگاری محسوب میشود که نخستین بار در سال ۱۹۹۶ معرفی شد .واترمارکینگ بعنوان یک روش در حفاظت کپی رایت و جلوگیری از تکثیر غیر قانونی اطلاعات ، روش مناسبی محسوب میشود.تفاوت واترمارکینگ و پنهان نگاری در آن است که در پنهان نگاری تناسب موضوع و محتوا میان رمز و میزبان

الزامی نیست. محتـوای رمـز و میزبـان میتوانـد کـاملا مستقل از هم باشند. اما در واترمارکینگ محتوای رمـز و میزبان بایستی مرتبط با هم باشند.
مثلا میتوان در یـک فایـل حـاوی اطلاعـات گذرنامـه اشخاص ، از مشخصات ظاهری فرد نظیر اثر انگـشت ، رنگ چشم یا طرح عنبیه بعنوان واترمارک ضمیمه بـه فایل اصلی استفاده کرد. در فایل تولیـدات یـک مرکـز علمی می تـوان ، از اطلاعـات کپـی رایـت آن مرکـز ، لیست مشتری ها ، طرح لوگوی مرکز ، تاریخ و نظـایر آن بعنوان واترمارک استفاده کرد. [11,12]

**واترمارک نامرئی Invisible watermarking :**

نوعی از واترمارک است که اختصاصا به منظـور احـراز هویت کاربر یا مالک یـا حتـی ایجـاد قابلیـت افـزودن اطلاعات امنیتی یا مقابله با جعل اسناد و اوراق بهـادار نظیر اسکناس و چک های بانکی و نظـایر آن اسـتفاده میشود. اولویت اصلی درواترمـارک نـا مرئـی ، خدشـه ناپذیری در برابر حملات خرابکاران میباشد .این نوع از واترمارک هنوز بصورت سنتی و کاغذی هم در فرآینـد چاپ اسکناس مورد استفاده قرار میگیرد. [13]

**مفاهیم و اصطلاحات متداول دیگر :**

Watermark :بـه اطلاعـات جـا سـازی شـده در محیط میزبان ، واترمارک گفته میشود.
Stegomedium / Host / Carrier :به محیط یـا رسانه ای کـه واترمـارک را در خـود جاسـازی میکنـد میزبان یا حامل یا واسط پنهان نگاری گفته میشود.
Steganogram :بـه مجموعـه محـیط میزبـان و واترمـارک جاسـازی شـده در آن، روی هـم رفتـه " استگانوگرام " گفته میشود.
Steganoanalysis :به تجزیه و تحلیل اسـتگانوگرام برای کشف و بازیابی واترمارک اطلاق میگردد. [14]

**پارامترهای ارزیابی الگوریتم :**

نرم افزار هایی که برای ایجـاد و کـشف واترمارکینـگ استفاده میـشوند ، از الگـوریتم هـای گونـاگونی بـرای پیاده سازی واتر مـارک اسـتفاده میکننـد. در ارزیـابی الگوریتمها ، پارامترهای زیر متداول ترند : [15]
Robustness : این پـارامتر هـر چقـدر بـالاتر باشـد نشانه آن است که میزان تخریب و اثرپذیری واترمارک در اثر تغییرات در فایل میزبان کمتر است .
Data rate ظرفیت : این پارامتر مـشخص میکندکـه حداکثر حجم ممکن که میزبان بـرای واترمـارک قـادر است فراهم کند چقدر است.

Impercebtibilty درجـه مخفـی سـازی : ایـن پارامترمـشخص مینمایـد کـه حـداکثرمجاز اثرگـذاری واترمارک در فایل میزبان ( برای آنکه شناسایی نشود ) چقدر است.
Suitability تناسـب بـا فایـل میزبـان : ایـن پارامترمشخص مینماید که واترمارک با توجه به حجم و محتوا و دیگر ویژگیهای خود تا چه حـد بـرای فایـل میزبان مناسب است .
Security امنیت: این پارامتر شبیه به درجـه مخفـی سازی است و تعیین میکند کـه فایـل میزبـان تـا چـه میزان وجود واترمارک را میتواند را مخفی نگه دارد.

**ویژگیهای قابل تعریف در واترمارک :**

**Robust / Fragile :**
Robust: تغییر محتوای فایـل میزبـان بـه واترمـارک خدشه ای وارد نمی سازد .
Fragile: تغییر محتوای فایـل میزبـان بـه واترمـارک صدمه میزند یا حتی آن را از بین میبرد.

**Visible / Transparent :**

Visible: واترمارک بوسیله حس بینـایی یـا شـنوایی انسان قابل تشخیص است.
Transparent / Blind : واترمارک توسط سیـستم بینایی یا شنوایی انسان قابل تشخیص نیست .

**Public / Private :**

Public: کاربران مجاز به شناسایی و بازیابی واترمارک هستند.
Private : کاربران اجازه شناسایی و بازیابی واترمارک را ندارند.

**Symmetric / Asymmetric :**

Symmetric: از کلیدهای یکسان برای جاسازی و بازیابی چند واترمارک استفاده میشود.
Asymmetric: از کلیدهای متمایز برای جاسازی و بازیابی چند واترمارک استفاده میشود.

**Steganographic / Non-steganographic**

Steganographic: به تکنیکی اشاره میکند که در آن کاربران از وجود واترمارک بی اطلاع هستند، این شیوه در تشخیص اثر انگشت استفاده میشود.
Non-Steganographic: به تکنیکی اشاره میکند که در آن کاربران از وجود واترمارک آگاهی دارند.این روش در ردیابی استفاده های غیر مجاز کاربرد دارد. [16]

**محیط میزبان :**

محیط و رسانه های گوناگونی میتواند میزبان ( حامل ) واترمارک باشند.
محیط میزبان میتواند از نوع رسانه های دیجیتالی یا غیر از آن باشد .
موارد متداول تر به قرار زیر هستند :
رسانه تصویر ساکن - رسانه تصویر متحرک – رسانه صوتی- رسانه متنی – فایل سرآیند – نرم افزار – سخت افزار – فایل سیستم – دیسک – ژنوم– بسته های جاری در شبکه این میزبانها از الگوریتمهای مختلفی برای واترمارکینگ استفاده میکنند که پرداختن به آنها از حوصله بحث ما خارج است. ملموس ترین و ابتدایی ترین صورت واترمارک دیجیتالی و سنتی ، مخفی سازی یک پیغام یا طرح هندسی در یک تصویر ساکن است. نرم افزارهای واترمارک کردن تصاویر امروزه به راحتی قابل تهیه و استفاده است. [17,18]
اما بهترین کاربرد آن میتواند در کپی رایت تصاویر عکاسان و تصاویر موجود در اینترنت باشد. این نوع واترمارک بصورت مرئی یا نامرئی قابل تهیه است. نوع سنتی آن سالهاست که در فرآیند چاپ اسکناس مورد استفاده است.
اگر تصویر متحرک را بصورت چند فریم ( تصویر ساکن ) متوالی تقسیم بندی کنیم ، آنگاه واترمارک تصویر متحرک امکانپذیر میگردد. کاربرد عمده آن در واترمارک کردن ویدئو کنفرانس های بین المللی و اینترنتی است.
واترمارک در رسانه صوتی نیز امکان مناسبی را جهت حفاظت کپی رایت تولیدات موسیقی و همچنین حفاظت اسناد صوتی مورد نیاز دادگاه ها فراهم میسازد. واترمارک صوتی و تصویری هر دو ، برخطا پذیری سیستم بینایی و شنوایی انسان استوار است.
واترمارک متنی میتواند توسط نرم افزار های واژه پرداز تهیه شود. از این واترمارک میتوان برای رمز کردن فایل های موجود در اینترنت استفاده کرد. اساسا این نوعHtml واترمارک بر سه گونه معنایی ، دستوری ، یا فضای آزاد تقسیم بندی میگردد که هریک بحث خاص خود را میطلبد.
دو نمونه ای که در ذیل آورده خواهد شد در تقسیم بندیها ، خوانده میشود .( Null Cipher ) " رمز پوچ " [19]

۱. این واترمارک بصورت سنتی در جنگ جهانی اول توسط یک جاسوس آلمانی استفاده شد.

**متن میزبان :**

Apparently neutral’s protest is thoroughly discounted and ignored . Isman hard hit Blockade issue affects pretext for embargo on by-products , ejecting suets and vegetable oils.

با کنار هم قرار دادن حروف دوم کلمات این متن ، پیام رمز ظاهر میشود :

Pershing sails from NY June1

۲. نمونه ای دیگر :

متن میزبان :

Fishing freshwater bends and saltwater coasts rewards anyone , feeling stressed . Resourceful anglers usually find masterful leapers fun and admit swordfish rank overwhelming anyday.

با سر هم گذاردن حروف سوم کلمات ، پیغام رمز نمایان میشود :

Send Lawyers , Guns and Money

از فضای فایل های سرآیند ، برد مدارات سخت افزار ها ، کد نرم افزارها ، فضای بلا استفاده یا رزرو شده دیسک ها ، و سرآیند پکت های جاری در شبکه های اینترنتی نیز میتوان بعنوان میزبان واترمارک نام برد.
فایل سیستم ها نیز میتوانند بعنوان میزبان مناسبی جهت مخفی سازی فایل ها استفاده شوند. در این صورت ، فایل سیستم هر گونه شکی را در مورد عدم وجود یک فایل در دیسک برطرف میکند. در این صورت حتی با جستجوی کل دیسک هم نمیتوان به وجود فایل پی برد ( چنین فایلی حتی در تقسیم بندی فایلهای " مخفی " نیز به کاربر نشان داده نخواهد شد. مگر آنکه مالک حقیقی آن فایل ، نام کاربری و رمز عبوری منحصر به آن فایل را به سیستم عامل معرفی نماید ). در چنین واترمارکی نام کاربری و رمز عبور هر فایل ، بایستی منحصر به فرد باشد. بدین ترتیب ، فایلها از دسترسی خرابکاران در امان خواهند ماند.
در تازه ترین دستاوردها ، تلاشهایی جهت واترمارک کردن در انسان صورت گرفته است که آینده DNA رشته درخشانی را ترسیم خواهد کرد. [20]

**کاربرد های عملی واترمارکینگ :**

در اینجا به کاربردهای عملی واترمارک بطور گذرا اشاره میشود : ( بعضی از مثالهای ذکر شده ، در بیش از یک گروه قرار خواهند گرفت )

**Copyright protection :** " به معنای حفاظت کپی رایت "
نظیر حفاظت کپی رایت محصولات چند رسانه ای ، دستاورد های علمی ، کتب الکترونیکی ، اقلام نرم افزاری ، شناسایی کاربران مجاز به استفاده از محیطهای گوناگون نظیر کتابخانه های الکترونیکی ، پایگاه های داده ای ، سایتهای اینترنتی ، انگشت نگاری ، و ... . [21]

**Copy Protection :** " به معنای مقابله با تکثیر و دستکاری غیر قانونی محصولات دیجیتالی "
نظیر مقابله با تکثیر غیرقانونی تولیدات نرم افزاری ، فیلم ، موسیقی ، انیمیشن ، تصویر ، کتب الکترونیک ، نشریات و ...[22]

**Tracking / Product Serialization :**" به معنای ردیابی کاربران مجاز و غیر مجاز در محیطهای گوناگون "
نظیر ردیابی کاربران از طریق کنترل شماره سریال های واترمارک شده محصولات دیجیتالی مختلف. ردیابی موارد سوء استفاده یا استفاده غیر قانونی ، کنترل روند تغییرات مختلف در محیطهای گوناگون. [23]

**Tamper proofing :** " به معنای کنترل و اثبات اعتبار"
نظیر کنترل اصالت محتوا ، زیر نظر گرفتن تغییرات در محیط یا محتوا [24]

**Monitoring :** " به معنای تحت نظر گرفتن "
نظیر کنترل انتشار برنامه های رادیویی و تلویزیونی ، کنترل پخش تبلیغات بازرگانی در شبکه های مختلف ، کنترل انتشار محتوا در اینترنت . [25]

**Concealed communication** : " به معنای ارتباطات رمزی و محرمانه "
نظیر استفاده در ارگانهای نظامی و انتظامی ، تامین امنیت ملی کشور ها ، استفاده در اهداف جاسوسی ، استفاده در جنگها برای مخابره اخبار و آگاهی از وضعیت دشمن ، خرابکاری ، عملیات بمب گذاری [26].

**Filtering / Classification** : " به معنای تقسیم بندی کاربران و فیلتر کردن "
نظیر گروه بندی کاربران برای کنترل سطح دسترسی ها ، فیلتر کردن محتوا ، ممانعت از دسترسی کاربر ، تعریف و تامین سطوح امنیتی مختلف. [27]

**Assest / Content Management** : " به معنای مدیریت بهینه محتوا "
نظیر درج شبه داده های قابل اطمینان و معتبر ، کنترل سرآیندها [28]

**Rights management** : " به معنای مدیریت حقوق تجاری "
نظیر کنترل حقوق تجاری اشخاص و ارگانها در فرآیندهای تجاری. [29]

**Remote Trigging** :" به معنای واکنش خودکار از راه دور "
کنترل عملکرد سیستم های خودکار از راه دور. [30]

**E-Commerce / Linking** :" به معنای ارتباطات و تجارت الکترونیک " [31]

نظیر استفاده در خرید و فروش اینترنتی و دیگر نمونه ها در بحث تجارت الکترونیک .
از دیگر کاربرد های متفرقه واترمارک میتوان به فرآیند چاپ اسکناس ، صدور اوراق هویت ،صدور اوراق بهادار ، صدور اسناد تجاری ، بررسی اسناد دادگاهی و حفاظت از آنها ، کاربرد در پزشکی قانونی ، کاربرد در آموزش الکترونیک ، کاربرد در علامت گذاری و حفاظت از اسناد و مدارک پزشکی ، کاربرد در رمزگذاری ژنوم اشاره نمود. [32,33]

هر چند که بعضی از کاربردهای اخیر که اشاره شد ، صرفا در حد پیشنهاد و تئوری قرار دارد ، اما با پیشرفت فزاینده این فناوری ، عملی شدن آنها در آینده پیش رویمان ، دور از انتظار نخواهد بود.

**چشم انداز آینده :**

با کاربردهای پیشنهادی و کابردهای تحقق یافته ای که در بخش قبل اشاره شد ، واترمارکینگ آینده روشنی را نوید خواهد داد. اخیرا تحقیقاتی پیرامون کاربرد واترمارک در رمزگذاری ژنوم و کاربرد در پزشکی در حال شکل گیری است که دانش ژنتیک و پزشکی و به دنبال آن نظم کنونی حاکم را در جهت مثبت بر هم خواهد زد. بنابراین به موازات این دانش ، دولتمردان و صاحبنظران سایر علوم نیز باید از هم اکنون چاره اندیشی را آغاز کنند. [34]

**استفاده از واترمارکینگ در ایران و سایر کشورها :**

ایران : فرآیند چاپ اسکناس احتمالا متداول ترین و قدیمی ترین استفاده واترمارک در ایران می باشد.در حالی که درکشور ما واترمارک می تواند در ارگانهای نظامی و انتظامی یا مراکز پزشکی با صرف هزینه ای قابل قبول به کار گرفته شود. واترمارک همچنین می تواند به اجرا شدن قوانین مصوب کشوری در مورد کپی رایت در جهت حفاظت از مالکیت معنوی ( I .P.) کمک کند .[35].

**سایر کشورها :** در سایرکشورها استفاده از واترمارک پررونق تر است. بعنوان نمونه در آمریکا، ارتش این کشور از فناوری واترمارک برای حفاظت ارتباطات رادیویی خود استفاده میکند. در بعضی کشورها نظیر کشور سوئیس ( و حتی بعضی کشورهای در حال توسعه آسیا ) صدور گواهینامه ، صدورکارت پرسنلی ، صدور گذرنامه ، صدور اوراق هویت ، کنترل مبادی

ورود و خروج کشور و نظایر آن ، هم اکنون با استفاده از واترمارک انجام میشود. شرکتهای فعال در این زمینه عمدتا آمریکایی و اروپایی هستند. در حالی که صاحبنظران و دانشگاههای فعال در این زمینه عمدتا در شرق و جنوب آسیا هستند. [36,37]

**نتیجه گیری:**

واتر مارکینگ ،ایجاد شناسه های مخفی روی فایل های متنی ، صوتی و تصویری است و ایجاد این شناسه های مخفی روش قابل اعتمادی برای حمایت از حق کپی آثار ، اثبات حق مالکیت ، تشخیص تغییرات ایجاد شده در تصاویر و بانکهای اطلاعاتی و ارتباطات سری در اختیار کاربران متخصص می گذارد .عمده کاربرد واتر مارک، به زمینه حفاظت کپی رایت ، شناسایی خلافکاران و مجرمین و مسایل نظامی و انتظامی خلاصه شده است.وروش واتر مارکینگ دیجیتال به عنوان روش کار آمد برای رمزگذاری از سال ۱۹۹۶ معرفی شد و امروزه به سرعت در حال پیشرفت و گسترش است، این روش به میزبانی رسانه ها و محیطهای گوناگون انجام پذیر است و حجم استفاده از واترمارکینگ در ایران تا عمومی شدن و رسیدن به شرایط مطلوب فاصله زیادی دارد.

**منابع و مراجع :**


۱. www.icip2006.org/cfp.asp
۲. en.wikipedia.org/wiki/Digital_watermarking
۳. en.wikipedia.org/wiki/Steganography
۴. www.webopedia.com/TERM/S/steganography.html
۵. enpub.fulton.asu.edu/iacdev/courses/CSE465/Fall2005/files/ln_2/IA%20Steganographylia.
۶. deis.unibo.it/Courses/RetiDiCalcolatori/Progetti00/fortini/project.pdf
۷. www.csis.pace.edu/~ctappert/srd2005/d1.pdf
۸. csrc.nist.gov/nissc/1999/proceeding/papers/p10.pdf
۹. jp.fujitsu.com/group/labs/downloads/en/business/activities/activities-4/fujitsu-labs-imagevoice-003-en.pdf
۱۰. Hunt, William Leigh “PhotoTiled Pictures Homepage” URL:http://home.earthlink.net/~wlhunt/
۱۱. Tannenbaum, Andrew S. “Steganography Demo for Modern Operating Systems”, 2nd ed. URL: www.cs.vu.nl/~ast/books/mos2/zebras.html
۱۲. en.wikipedia.org/wiki/Digital_image_processing#_ref-0
۱۳. www.worldscientific.com
۱۴. www.digitalwatermarkingalliance.org
۱۵. www.digimarc.com
۱۶. www.watermarkingworld.org
۱۷. www.srlst.com
۱۸. www.tejaratbank.ir/portal/Default.aspx?tabid=120
۱۹. www.watermarker.com/watermark-protector
۲۰. www.alpvision.com/DOWNLOAD/watermarking.pdf
۲۱. www.ece.cmu.edu/~adrian/projects/wmark-realworld/wmark-realworld.pdf
۲۲. www.digitalwatermarkingalliance.org/docs/dwa_whitepaper_p2p.pdf
۲۳. www.watermarkingworld.org/faq.html
۲۴. www.wipro.com/pdf_files/Digital_Watermarking_Tech_Overview.pdf

۲۵. www.preemptive.com/documentation/watermarking.html
۲۶. www.webopedia.com/TERM/D/digital_watermark.html
۲۷. www.networkworld.com/newsletters/sec/0103sec1.html
۲۸. tech.yahoo.com/qa/20070226233220AAEuKxk
۲۹. www.watermarkingworld.org/stirmark/stirmark.htm
۳۰. www.watermarkingworld.org/optimark/index.html
۳۱. www.metois.com/Docs/audiowatermark.pdf
۳۲. www.wassenaar.org/faq/print_faq.html
۳۳. www.akkasee.com/forum/showthread.php?goto=lastpost&t=416
۳۴. www.ecwatermark.com/download.asp
۳۵. www.watermarkingworld.org/checkmark/checkmark.html
۳۶. www.ivertech.com/batchWatermarker/usersGuide.aspx

37.www.cs.ucla.edu/~miodrag/cs259-security/SoftwareWatermarking.pdf

**Abstract**

Would it not be wonderful if we could all communicate in private without having to wonder or worry about someone? What if you needed to get information in any media to someone and you wanted to make sure no one was able to easily read it at all? In our modern society, the need for optimum management of communications in a secure manner in different environments and media is aware evermore. Artificial intelligent has an important role in development in the control of communications. Protection of data against illegal copying is becoming such an important issue, therefore the necessity for implementation of a competent technique for data protection is vital. Information hiding is a general term encompassing many sub disciplines. Two important sub disciplines are: steganography and watermarking. Steganography means keeping the existence of the information secret while in watermarking the information becomes imperceptible. Cryptography is however about protecting the content of messages. The most important applications of this technique are; copyright protection, copy protection, content authentication, transaction tracking, broadcast monitoring.

**Keywords:**
Watermarking, steganography, Cryptography , digital watermarking

**Tecnology IntroduceingWatermarking**

**By**
**Zohreh Mohsenpour**