پروژه کارشناسی ارشد – مخابرات

بهبودعملکرد واترمارکینگ مبتنی برSVDو DCT به منظور سندیت

رضا چشمه‌جهان

استاد راهنما:

دکتر سربیشه‌ئی

تابستان ۹۱


بسم الله الرحمن الرحيم

چکیده :

امروزه با توجه به پیشرفت‌های روز افزون شبکه‌های ارتباطی مانند اینترنت ، ارتباط کاربران با یکدیگر و دسترسی آن‌ها به منابع اطلاعاتی مختلف به راحتی صورت می‌گیرد و کاربران شانس زیادی را در استفاده از اطلاعات چند رسانه‌ای دارا می‌باشند. بنابراین حفظ حقوق این رسانه‌ها به یک موضوع مهم تبدیل شده است. هم چنین کاربران می‌خواهند بدانند که آیا اطلاعاتی که در دسترس آن‌ها می‌باشد تصدیق شده می باشند یا نه و از نظر اعتبار در چه سطحی قرار دارند.

در سیستم های نظارت ویدئویی اتوماتیک (VS) موضوع تصدیق کردن مضمون ویدئو از اهمیت ویژه‌ای برخوردار است. تصاویر ویدئویی و عکس‌های دیجیتالی می‌توانند به سادگی دستکاری شوند و اگر احتمالی برای سندیت قانونی آنها وجود نداشته باشند، هیچ ارزشی برای ارائه شدن به عنوان یک مدرک قانونی ندارند. از این رو در این پروژه روش های مختلف سندیت مورد بررسی قرار گرفته است.

در بخش‌های ابتدایی، سندیت رسانه با تصدیق بسته‌های اطلاعات چند رسانه‌ای ، مطرح گشته است. سندیت رسانه-ها در این سطح با استفاده از گراف‌های مختلف مانند گراف پروانه‌ای انجام می‌شود.

این گراف‌ها با ایجاد افزونگی از اتلاف بسته‌ها در یک شبکه پراتلاف، جلوگیری می‌کنند. ولی هرکدام از آن‌ها دارای مزایا ومعایبی می‌باشند.لازم به ذکر است پارامترهای موجود در این طرح‌ها،با یکدیگردر کشمکش می‌باشند و بهبود یکی ممکن است باعث تخریب دیگری گردد.

در بخش چهارم واترمارک بعنوان ابزاری مهم برای سندیت مطرح شده است. هدف عمده توسعه تکنیک‌های واترمارکینگ تصویر، بهبود در مقاومت و غیر مشاهده بودن آنهاست. در پایان این فصل یک تکنیک واترمارکینگ ترکیبی مبتنی بر ویولت و تجزیه مقادیر منفرد مورد بررسی قرار گرفته است.

در فصل پنجم الگوریتم‌های مبتنی بر SVDوDCTمورد بررسی قرار گرفته و شبیه‌سازی شده است. از ویژگی‌های عمده این الگوریتم‌ها کیفیت بالای تصویر در ضرایب جاسازی واترمارک پایین می‌باشد که می‌توان از این ویژگی برای سندیت به طرز مطلوبی بهره برد. همچنین با تغییر در چینش فرکانسی در جاسازی واترمارک مقاوت این الگوریتم‌ها به طرز قابل قبولی بالا رفته است. در پایان ارائه هر الگوریتم نیز شبکه عصبی به عنوان ابزاری مفید برای رسیدن به مقادیر مطلوب ضرایب جاسازی واترمارک مورد استفاده قرار گرفته است.

فهرست مطالب

فهرست شکل‌ها

فهرست جدول‌ها

فصل اول

مقدمه

۱- ۱ - مقدمه

مخابره رسانه در سراسر شبکه‌ها بطور روز افزون و پیوسته در حال افزایش می‌باشد. این هدف با رشد سریع پهنای باند شبکه، بهبود فرمت‌های فشردگی، پیشرفت تکنولوژی‌های انتقال، مثل شبکه‌های انتقال داده و سیستم‌های نظیر به نظیر[۱] تحقق یافته است. هم‌چنین این امر در بسیاری از سرویس‌های تجاری و شبکه‌های اینترنتی، انتقال پیام چند رسانه‌ای، ویدئو کنفرانس‌ها و نظارت‌های ویدئوی[۲] مشهود است.

بنابراین موضوع امنیت از قبیل قابلیت اطمینان، تصدیق و اتخاذ رسانه‌های ایمن به طور جدی مورد توجه قرار گرفته است. برای مثال فرستنده اطلاعات می‌خواهد مطمئن باشد که اطلاعاتش فقط در دسترس افراد مجاز و معتبر قرار خواهد گرفت. هم چنین گیرنده این اطلاعات هم می‌خواهد اطمینان پیدا کند که این اطلاعات در دسترس، توسط فرستنده مورد نظر فرستاده شده و این اطلاعات از روی عناد و یا احیاناً به طور تصادفی تغییر نکرده‌اند. ایجاد قابلیت اعتماد در نگه‌داری مفهوم واستفاده از شیوه‌های مختلف رمزنگاری که دسترسی کاربران مختلف به اطلاعات را محدود می‌کند، در سال های اخیر مورد توجه قرار گرفته است.

جاری ساختن[۳] رسانه و اطلاعات از طریق کانال‌های مختلف به عنوان یک چالش، مطرح می‌باشد. دلیل این چالش نامطمئن بودن کانال‌های انتقال می‌باشد. چون ایجاد اتلاف بسته در این کانالها باعث نقص در رسانه دریافت شده می گردد. این مشکل وقتی که کانال پراتلاف باشد نمود بیشتری پیدا می‌کند. چون گم شدن بسته‌های مختلف با اهمیت-های گوناگون می‌تواند سندیت[۴] رسانه را با مشکل روبه رو سازد.

تاکنون روش‌های مختلفی برای سندیت و امنیت رسانه به وجود آمده است. این روش‌ها می‌توانند در مقابل اتلاف بسته‌ها از خود مقاومت نشان دهند و با بهره‌گیری از آنها می‌توان میان دستکاری‌های مغرضانه و اتفاقی تمایز قائل شد.

در این پروژه روش‌های مختلف سندیت تصویر مورد بررسی قرار خواهد گرفت. که این روش‌ها مبتنی بر انواع مختلف گراف‌ها و هم چنین سیگنال‌های واترمارک می‌باشند.

در فصل اول، مقدمه‌ای کوتاه درباره لزوم سندیت تصویر، با توجه به پیشرفت‌های شبکه‌های انتقال رسانه،و همچنین افزایش تصاویر دیجیتال، ارائه شده است. فصل دوم مفاهیم کلی سندیت را ارائه کرده و مخاطب می‌تواند جوانب مختلف سندیت را در نظر بگیرد و با انواع مفاهیم وتعاریف و هم چنین اصطلاحات موجود در روش‌های سندیت آشنا شود. در این فصل سعی شده است که مفاهیم کلی سندیت مبتنی بر جاری ساختن و سندیت مبنی بر مفهوم به خوبی ارائه شود.

---

[۱] Peer-to-peer system.
[۲] Video surveillance.
[۳] Stream
[۴] Authentication.

فصل سوم سندیت مبنی بر جاری ساختن را با استفاده از روش‌های مبنی بر گراف، به صورت تخصصی مورد بحث قرار داده است و به انواع گراف‌های مختلف برای سندیت و معایب و محاسن آنها اشاره شده است. در فصل چهارم هم سندیت مبنی بر واترمارک مورد بحث قرار گرفته و انواع مختلف واترمارک و روش‌های مختلف جاسازی واترمارک، برای تحقق سندیت ارائه داده شده است. این روش‌ها در دو حوزه مکان و تبدیل عمل کرده و هر کدام معایب و مزایای مختص خود را دارا می‌باشند. همچنین این روش‌ها می‌توانند کیفیت بصری بالایی را در رسانه واترمارک شده فراهم آورند. در فصل پنجم چند الگوریتم در حوزه DCT[1] و SVD[2] پیشنهاد داده شده است که یکی از موارد استفاده آنها سندیت می‌باشد. ادغام DCT و SVD با یکدیگر سبب شده است این الگوریتم‌ها مقاومت خوبی داشته باشند و از لحاظ بصری نیز کیفیت بالایی را دارا باشند. در پایان هر الگوریتم شبکه عصبی برای رسیدن به مقادیر مطلوب ضرایب جاسازی واترمارک مورد استفاده قرار گرفته است.

[1] Discrete cosine transform

[2] Singular value decomposition

فصل دوم

مفاهیم و تعاریف

۲-۱- مقدمه

سندیت رسانه یک حوزه تحقیقاتی نسبتاً جدیدی می‌باشد که در سال‌های اخیر مورد توجه قرار گرفته است. محققان در حوزه‌های گوناگون و با تکنیک‌های متفاوت ممکن است تعاریفی گوناگون از سندیت را به کار ببرند. برای مثال انجمن زیست سنجی ممکن است از لفظ سندیت برای شناسایی یا تأیید منبع استفاده کنند. (برای مثال، صورت و اثر انگشت). انجمن واترمارکینگ چند رسانه‌ای واژه سندیت را برای حفظ صحت مضمون مورد استفاده قرار می‌دهند. لازم به ذکر است که حفاظت از صحت مضمون مبتنی بر واترمارکینگ دیجیتال یکی دیگر از حوزه‌های تحقیقاتی می باشد که در کاربردهای مختلف مثل نظارت ویدئویی مورد استفاده قرار می‌گیرد. در بعضی مواقع سندیت به عنوان فرایندی تعریف می شود که یک گیرنده مجاز بتواند با احتمال خیلی بالا موارد زیر را تعیین نماید.

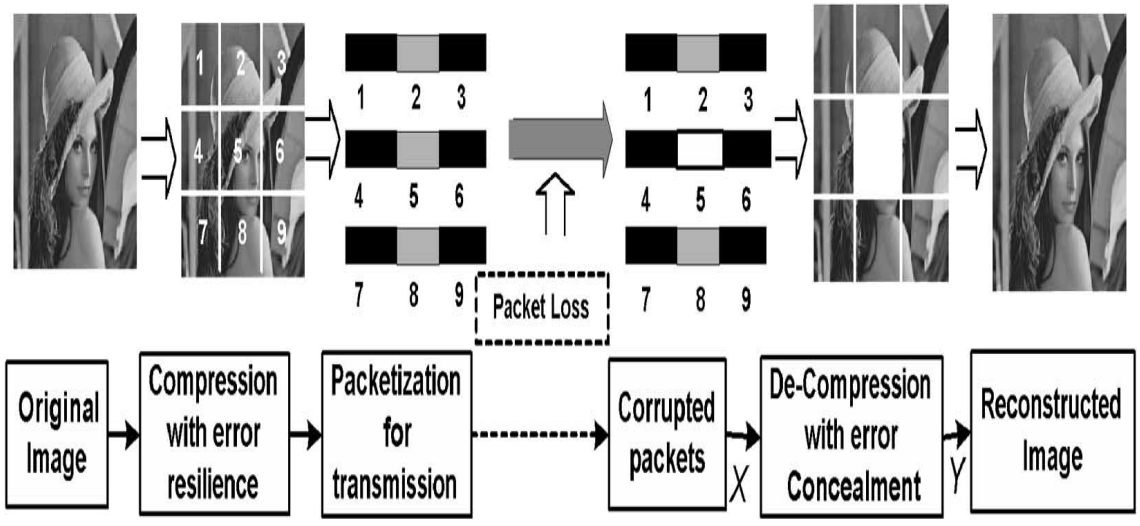
۱- اطلاعات موجود توسط یک فرستنده مجاز فرستاده شده‌اند.

۲- اطلاعات موجود مورد تغییر یا دستکاری قرار نگرفته‌اند.

بنابراین سندیت به دو سوال پاسخ خواهد داد، یعنی چه کسی اطلاعات را فرستاده است و آیا اطلاعات تغییر کرده است یا نه، در این صورت لفظ سندیت می‌تواند بر تصدیق هر دوی اطلاعات و منبع دلالت کند.

به منظور حفظ کارایی امنیت در یک سطح محاسباتی غیرعملی برای مهاجمان پنهانی، تعاریف بالا مستلزم این امر می باشند که رسانه دریافت شده دقیقاً همان چیزی باشد که فرستاده شده است، ولی هنگامی که جاری کردن رسانه در یک کانال با اتلاف و غیر قابل اطمینان انجام شود این‌نیاز برآورده نمی‌شود.

چون در این انتقال بعضی اطلاعات گم می‌گردند. مفهوم مشکل یاد شده در شکل ۲-۱ نشان داده شده است.



شکل ۲-۱ انتقال تصویر از طریق کانال نامطمئن[۱]

همان طور که در شکل ۲-۱ نشان داده شده است تصویر اصلی کد می‌شود و سپس بسته‌بندی می‌گردد. بسته‌های حاصل توسط یک کانال پراتلاف منتقل می‌گردند. از آنجا که کانال امن و مورد اطمینان نیست بعضی از بسته‌ها به طور طبیعی گم می‌شوند، یا اینکه قبل از رسیدن به گیرنده، مورد دستکاری قرار می‌گیرند. در گیرنده تصویر خراب شده قبل از نمایش یا پردازش‌های دیگر، مورد بازسازی قرار می‌گیرد. به طور کلی کانال‌های پراتلاف، رسانه کد شده را ناقص می‌کنند و کیفیت رسانه کشف رمز شده را پایین می‌آورند.

بنابراین سندیت و تصدیق باید با رسانه دریافت شده انجام گردد. با این تعریف رسانه تصدیق شده برابر است با رسانه‌ای که منحصراً از تصدیق بسته‌های رسیده شده، آشکار گشته است.

با این تعریف یک بسته فقط در صورتی که دریافت شده و قابل رمزگشایی و تصدیق باشد مورد استفاده قرار می گیرد. بنابراین در جاری ساختن رسانه باید به دو مورد زیر توجه شود:

۱- حتی اگر رسانه دریافت شده ناتمام باشد، هدف تصدیق کردن همه بسته‌های رسیده شده می‌باشد، با فرض اینکه تمام بسته‌های دریافت شده می‌توانند به صورت ایده آل تصدیق گردند.

۲- بسته‌های دریافت شده تنها زمانی مورد استفاده قرار می‌گیرند که اولاً قابل به رمزگشایی باشند و دوم اینکه تصدیق شده باشند. به دلایل امنیتی یک بسته دریافت شده و رمزگشایی شده در صورتی که تصدیق نگردد، نمی‌تواند مورد استفاده قرار بگیرد. به طور مشابه اگر بسته‌ای که دریافت می‌شود، تصدیق گردد ولی غیرقابل رمزگشایی باشد هم مورد استفاده قرار نمی‌گیرد.

در شکل ۲-۱ تصدیق کردن می‌تواند در نقطه **X** یا **Y** انجام گیرد که با توجه به کاربردهای مختلف این کار انجا می گردد. این دو نقطه روش‌های تصدیق موجود را به ۲ کلاس زیر تقسیم می‌کنند.

۱- سندیت مبنی بر مفهوم

۲- سندیت مبنی بر جاری ساختن

روش‌های مبتنی بر جاری ساختن، مزایا و معایت خاص خود را دارند. این روش سطح امنیتی خوبی را ایجاد می کنند و مهم‌تر اینکه، سطوح امنیت فراهم شده بوسیله قوانین ریاضی قابل اثبات می‌باشند. از نواقص این روش وجود مخارج کلی ناشی از بیت ریت‌های اضافی می‌باشدو دشواری محاسبات می‌تواند بالا باشد. هم چنین کیفیت رسانه تصدیق شده نسبت به همان رسانه که تحت همان اتلاف قرارگرفته ولی نیازی به تصدیق ندارد می‌تواند پایین‌تر باشد.

از سوی دیگر، روش‌های مبنی بر مفهوم که توسط بعضی از فرم‌های واترمارکینگ دیجیتال بوجود می‌آیند، مخارج بیت ریت کمتری دارند و معمولاً نسبت به اغتشاش مقام‌تر می‌باشند. هر چند در این روش ایجاد سطوح امنیتی که توسط قوانین ریاضی قابل اثبات باشد کاری سخت و دشوار می‌باشد. بعبارتی سطح امنیت بصورت قابل توجهی پایین می‌آید.

نواقص موجود در روش های جاری ساختن ما را برای بازنگری در این روش‌ها مصمم تر کرده است و اینکه آیا می توان کیفیت رسانه دریافت شده را با استفاده از اطلاعات رسیده شده از مفهوم رسانه بهینه کرد؟ از دیگر عوامل، برای ایجاد این انگیزه، این است که، هر نوعی خاص از اطلاعات از بسته‌های مختلفی تشکیل شده است و هر یک از این بسته ها دارای اهمیت‌های مختلفی که ناشی از فشردگی و مفهوم رسانه است، می‌باشند.

بنابراین تخصیص منابع از اهمیت ویژه‌ای برخوردار می‌گردد. در این صورت طبیعی است که به بسته‌های با اهمیت بیشتر، منابع سندیت بیشتری تخصیص دهیم.

نکته دیگری که باید به آن توجه کرد این است که رسانه معمولاً قبل از جاری شدن، توسط استانداردهای فشرده سازی کد می‌گردد. که این باعث ایجاد وابستگی‌های کدگذاری در بین بسته‌های مختلف می‌گردد.بنابراین برای تخصیص منابع این وابستگی‌ها هم باید مورد توجه قرار گیرند. و بالاخره هدف تکنیک‌های قبلی سندیت مبتنی بر جاری کردن، بهینه ساختن احتمال تصدیق هر بسته بود. در حالی که هدف عمده جاری ساختن اطلاعات بیشینه کردن کیفیت رسانه دریافت شده می‌باشد. یعنی به جای بهینه کردن احتمال تصدیق افزایش کیفیت رسانه مورد توجه قرار گرفته است.

۲-۲- تعاریف

۲-۲-۱- سندیت، درستی[۱] و انکارناپذیری[۲]

معمولاً سندیت با صحت اطلاعات، شناسایی منبع و انکارناپذیری پیوند خورده است. چون این مسائل معمولاً به هم وابسته هستند. اطلاعاتی که به طور موثر تغییر کرده است، باید منبع جدیدی داشته باشد و اگر منبع شناسایی نشود، موضوع تغییرات هم تعیین نشده باقی می‌ماند. روش‌هایی که سندیت اطلاعات را بوجود می‌آورند روش‌های امضای دیجیتالی (**DSSs**) و کدهای سندیت پیام (**MACs**) می‌باشند.

امضاهای دیجیتالی از یک جفت رمز عمومی/ خصوصی نامتقارن استفاده می‌کنند. در صورتی که **MAC** ها از یک رمز خصوصی متقارن استفاده می‌کنند. هر دوی تکنیک‌های **DSS** و **MAC** بر مبنای یک تابع هش یک طرفه بنا شده اند.

۲-۲-۲- تابع هش یک طرفه

یک تابع هش یک طرفه، تابع تولید کننده هشی است که فقط در یک مسیر کار می‌کند و برای هر اطلاعات داده شده دلخواه با اندازه‌های مختلف، رشته بیت‌هایی با درازای ثابت تولید می‌کند. توابع هش، این امر را تضمین می-

---

[۱] Integrity

[۲] Nonrepudiation

کنند که حتی اگر یک بیت از اطلاعات ورودی فرق کند، هش‌های تولیدی در خروجی متفاوت خواهند بود. بنابراین با استفاده از توابع هش، می‌توان مشخص کرد که آیا اطلاعات تغییر کرده است یا خیر. دو تابع هش**MD5** (۱۲۸ بیت) و **SHA-۱** (۱۶۰بیت) بطور متداول مورد استفاده قرار می‌گیرند.

۲-۲-۳- روش‌های امضای دیجیتالی

اساس این روش‌ها شامل موارد زیر می‌باشند:

۱- رویه‌ای برای محاسبه امضای دیجیتالی که از رمز خصوصی فرستنده استفاده می‌کند.

۲- رویه‌ای برای تأیید امضا درگیرنده که از رمز عمومی استفاده می‌کند.

تولید امضای دیجیتالی بسیارگران می‌باشد و به طول اطلاعاتی که قرار است علامت‌دار شود بستگی دارد. بنابراین به جای اینکه اطلاعات را به طور مستقیم علامت‌دار کنیم بهتر این است که اول مقادیر هش اطلاعات را محاسبه کنیم و سپس مقادیر هش به دست آمده را علامت‌دار نماییم. **Dss** ها یک تکنولوژی رایج هستند که به عنوان یک استاندارد جهانی شناخته شده می‌باشند. امضاهای تولید شده حدود ۱۰۲۴ بیت می‌باشند.

۲-۲-۴- تصدیق مفهوم[۱]

تصدیق مفهوم این هدف را دنبال می‌کند که رسانه دریافت شده را از نظر مفهوم مورد بررسی قرار دهد و مشخص کند که آیا این رسانه از نظر مفهوم مورد تغییر قرار گرفته است یا خیر. این گونه سنديت‌ها برای کاربردهایی که در آن اطلاعات رسانه مورد دستکاری قرار می‌گیرد ولی مفهوم رسانه تغییر نمی‌کند قابل قبول می‌باشد.

۲-۲-۵- تحاریف غیرعمدی و تحاریف عمدی

تحاریف و دستکاری‌های غیرعمدی به تغییراتی گفته می‌شود که براثر اعمالی مثل رمزگذاری وفشردگی یا اتلاف بسته و ... ایجاد می‌گردد. تعاریف عمدی به تغییراتی گفته می‌شود که توسط مهاجمین صورت می‌گیرد. مثلاً کپی – پیست تصویر یا تغییرات در متن موجود در یک تصویر و یا افزودن بسته، و در برخی کاربردها، هدف روش‌های سنديت، تحمل دستکاری‌ها و تحاریف غیرعمدی و رد و شناسایی تحاریف عمدی می‌باشد.

۲-۲-۶- احتمال تصدیق

احتمال اینکه بسته دریافت شده هم چنان قابل تصدیق و رسیدگی باشد.به طور ایده‌ال همه بسته‌های دریافت شده، قابل تصدیق شدن می‌باشند، تصدیق این بسته‌ها هزینه بالایی را در بر خواهد داشت. بنابراین، این نیاز احساس می‌شود که روش‌هایی بوجود آیند، که احتمال تصدیق بالا و هزینه‌ای کم و بهینه را دارا باشند.

---

[۱] Content authentication

۲-۲-۷- مخارج محاسباتی[۱]

منظور از مخارج محاسباتی ، منابع محاسباتی مورد نیاز برای تولید و تصدیق امضاء در فرستنده و گیرنده می‌باشد. به عبارتی دیگر به تعداد عملیات تابع هش و عملیات مربوط به امضاء و تصدیق درگیرنده و فرستنده، مخارج محاسباتی گویند.

۲-۲-۸- مخارج مخابره‌ای[۲]

منظور از مخارج مخابره‌ای ، تعداد بایت‌های اضافی که همراه بسته‌ها فرستاده می‌گردند و برای سندیت بکار می‌روند می‌باشند. این بایت‌های اضافی، مقادیر توابع هش و **MAC** ها می‌باشند. بنابراین، بسیار مهم می‌باشد که تا حد ممکن این هزینه‌ها کم گردد، به خصوص در محیط‌های بی‌سیم که دارای پهنای باند محدود و کم‌یابی می‌باشند.

۲-۲-۹- تأخیر فرستنده[۳]

به یک تأخیر اضافی که به بسته‌ها، قبل از فرستاده شدن تعلق می‌گیرد تا تحت پردازش‌های سندیت قرار بگیرد، تأخیر فرستنده گویند. یک تأخیر فرستنده بالا معمولاً به یک بافر بزرگ در فرستنده نیاز دارد.

۲-۲-۱۰- تأخیر گیرنده[۴]

به مدت زمانی که یک بسته وقتی به گیرنده می‌رسد، تا زمانی که این بسته بتواند تحت پردازش‌های سندیت قرار بگیرد، تأخیر گیرنده گویند.یک تأخیر گیرنده بالا معمولاً به یک بافر بزرگ درگیرنده نیاز دارد. .
یک بسته در حین جاری ساختن رسانه معمولاً دارای ضرب الاجلی معین می‌باشد. بنابراین تأخیر گیرنده باید به گونه‌ای باشد که ضرب الاجل بسته با اتمام نرسد. بسته‌ای که ضرب الاجل آن به اتمام رسیده باشد بی‌استفاده باقی خواهد ماند.

۲-۲-۱۱- مقاومت در برابر اتلاف بسته

در جاری ساختن اطلاعات، بسته‌های ارسالی باید با احتمال تصدیق بالایی، تحت پردازش‌های سندیت قرار بگیرند. حتی اگر شبکه انتقال، یک شبکه پراتلاف باشد. این نیاز باید به بهترین شکل تأمین گردد.
هم‌چنین فراهم آوردن شرایط مطلوب با توجه به نیازهای ذکر شده در قسمت های قبل امری سخت ودشوار خواهد بود. برخی از این نیازها با هم در کشمکش و تقابل خواهند بود. یعنی بهبود یکی باعث تخریب در دیگری می‌گردد.

---

[۱] Computation Overhead.
[۲] Communication Overhead
[۳] Sender Delay
[۴] Receiver Delay

برای مثال، تأخیر گیرنده معمولاً با تأخیر فرستنده در تضاد می‌باشد و یا اینکه ایجاد مقاومت و پایداری باعث افزایش هزینه سندیت می‌گردد.

۲-۳- سندیت مبنی بر مفهوم

سندیت مبنی بر مفهوم یک کلاس از راه حل‌های ممکن برای دستیابی به سندیت می‌باشد. هدف این کلاس از سندیت این است که رسانه در سطح مفهوم، تحت پردازش‌های سندیت قرار بگیرد. اساس کار این روش در شکل ۲-۲- نمایش داده شده است.

یک عکس ۵۱۲ × ۵۱۲ با JPEG در دو حالت مورد فشرده‌سازی قرار گرفته است.تصویر اول در سمت چپ با سطح کیفی۱۰ (بهترین کیفیت) مورد فشرده‌سازی قرار گرفته است و تصویر دوم در سمت راست با کیفیت JPEG ۴ فشرده شده است.

اندازه فایل از ۱۵۱ کیلو بایت در بهترین سطح کیفی فشردگی به ۳۶ کیلوبایت کاهش می‌یابد. مادامی که نمایش دو بیتی تصویر کاملاً متفاوت می‌باشد، اما هنوز بسیاری از مفاهیم رسانه که به طور عمده از جزئیات ثابت و نامتغیر تشکیل شده است،حفظ گردیده است.

شکل ۲-۲ مفهوم رسانه[۱]

این جزئیات و ویژگی‌ها نسبت به بعضی از دستکاری های قابل قبول و از پیش تعیین شده مقاوم می‌باشند. در حالی که به دستکاری‌های مغرضانه حساس هستند.

بنابراین، سندیت مفاهیم رسانه با تصدیق این جزئیات حاصل می‌گردد. برای تصدیق رسانه در این سطح می‌توان از واترمارک استفاده کرد[۱].