ششمین کنفرانس بین المللی انجمن رمز ایران
۱۵ و ۱۶ مهر ماه ۱۳۸۸، دانشگاه اصفهان
انجمن رمز ایران
دانشگاه اصفهان

واترمارکینگ تصاویر رنگی بر پایه تئوری فوق آشوب

مریم شاه‌پسند، مهدی یعقوبی

دانشگاه آزاد اسلامی واحد مشهد

m.shahpasand@gmail.com
yaghubi@mshdiau.ac.ir

چکیده

در این مقاله روش جدیدی در زمینه واترمارکینگ‌های قدرتمند ارائه شده است که در تصاویر رنگی بر پایه سیستم فوق آشوب اعمال می‌شود. بر خلاف روش‌های معمول واترمارکینگ کیاتیک که بر اساس سیستم آشوبی با سه حالت اولیه صورت می‌گرفت در این روش با استفاده از سیستم فوق آشوب رشته شبه تصادفی تولید شده است تا جایگاه واترمارک در تصویر را مشخص کند و به منظور بالابردن امنیت، پارامتر چهارم سیستم فوق آشوب هر تکرار به عنوان عامل تعیین کننده ترتیب ورودی‌ها در تکرار بعد استفاده شده است. ایده پیشنهادی افزایش مقاومت، طول و فضای کلید را در بر داشته است. همچنین در روش پیشنهادی استخراج واترمارک بدون نیاز به تصویر اصلی صورت می‌گیرد. نتایج تجربی نشان می‌دهد روش ارائه شده کوچک‌ترین تغییرات در واترمارک را مشخص می‌کند و این در حالی است که در مقابل حملات آماری و تفاضلی کاملا مقاوم است و حساسیت زیاد سیستم فوق آشوب به شرایط اولیه امنیت سیستم را به نحو قابل توجهی بهبود داده است.

واژه‌های کلیدی

واترمارک، احراز مالکیت، آشوب، امنیت، کپی‌رایت.

۱- مقدمه

با رشد سریع تکنولوژی چند رسانه‌ای و شبکه، رسانه‌های دیجیتالی نیز به سرعت گسترش یافته است. از آنجایی که محصولات دیجیتالی به آسانی تولید و کپی شده و یا به راحتی تغییر می‌یابند چگونگی حفاظت از کپی‌رایت و جامعیت آن‌ها به مشکلی بزرگ تبدیل شده است. برای حل این مشکل تکنیک‌های زیادی در دهه اخیر ارائه شده است که در بین آن‌ها دیجیتال واترمارکینگ روشی کاملا موثر و امیدبخش می‌باشد[۱،۲،۳]. پس از اعمال واترمارک در یک تصویر دیجیتالی، واترمارک از دید اشخاص غیرقابل رویت می‌گردد و باید در مقابل حملات مختلف از جمله حملات آماری و تفاضلی مقاوم باشد[۴].

در سال‌های اخیر نگاشت‌های آشوبی جهت افزایش امنیت دیجیتال واترمارک به صورت گسترده‌تر نسبت به گذشته مورد استفاده قرار گرفته‌اند[۵]. مهم‌ترین خصوصیت آشوب حساسیت به شرایط اولیه است بدین صورت که با انتخاب شرایط اولیه متفاوت اما بسیار مشابه، خروجی سیستم مقادیر کاملا متفاوت است بنابراین می‌توان یک رشته شبه تصادفی تولید کرد[۶]. خصوصیات ویژه نگاشت آشوبی با افزایش حالات در سیستم‌های فوق آشوب به صورت موثرتری ظاهر می‌شود و بر این اساس در الگو پیشنهادی از این سیستم در ایجاد رشته شبه تصادفی جهت تعیین جایگاه واترمارک در تصویر استفاده شده است. شرایط اولیه پس از تعیین، با استفاده از روش RSA رمزنگاری شده و بدین صورت مقادیر اولیه به گیرنده ارسال می‌گردد. این عمل استخراج واترمارک را بدون نیاز به تصویر اصلی امکان‌پذیر می‌سازد.

مقاله در قالب این بخش‌ها ارائه شده است: ابتدا به بررسی خصوصیات نگاشت‌های آشوبی و جزئیات نگاشت فوق آشوب لورنز می‌پردازیم و سپس روش پیشنهادی معرفی می‌گردد. در ادامه نتایج تجربی به دست آمده را بیان کرده و در پایان نتیجه‌گیری صورت می‌گیرد.

۲- آشوب و کاربردهایش در واترمارک

آشوب پدیده‌ای است که در سیستم‌های غیر خطی تعریف‌پذیر رخ می‌دهد که حساسیت زیاد به شرایط اولیه و رفتار شبه تصادفی از خود نشان می‌دهند. چنین سیستم‌هایی در حالتی که شرایط معادلات نمایی لیاپانوف را برآورده سازند در مد آشوب به حال پایدار باقی خواهند ماند. همواره خروجی این سیستم تحت تاثیر مقادیر اولیه ورودی می‌باشد از سوی دیگر پیش‌بینی این نوع سیگنال بدون داشتن مقادیر اولیه تقریبا غیر ممکن خواهد بود و شکل ظاهری این سیگنال مشابه نویز می‌باشد. توابع کیاتیک، دارای خواص زیر می‌باشند:

- حساسیت بسیار زیاد به شرایط اولیه: اگر پارامترهایی با اختلاف بسیار کم به سیستم تولید کلید بدهیم، کلیدهایی با اختلاف زیاد و معنی‌دار تولید می‌کند.
- قطعیت[1]: با وجود رفتار به ظاهر اتفاقی، توابع کیاتیک کاملاً قطعی هستند. یعنی با محاسبه صحیح، بکارگیری پارامترهای دقیق برای تولید کلید همیشه نتیجه یکسانی می‌دهد و این به طرفین انتقال اطلاعات اجازه می‌دهد هر یک به طور مستقل کلیدهای صحیح و مشابه را تولید کنند.
- عدم پیشبینی آماری[2]: به خاطر رفتار به ظاهر اتفاقی دنباله‌های کیاتیک، دنباله یا رشته اعداد تولید شده توسط آن‌ها توسط هیچ راه آماری مشهودی به هم مرتبط نمی‌شوند، به این معنا که روش‌های مختلف آماری تاثیر بلافاصله و جدی در کاهش تعداد کلیدهای بیشمار مرتبط با دنباله کیاتیک، ندارند.

با توجه به خصوصیات سیستم آشوبی می‌توان از آن در جهت افزایش امنیت در واترمارک تصاویر استفاده کرد[۷]. سیستم‌های فوق‌آشوب به دلیل این که توان‌های لیاپانوف مثبت آن‌ها بیش از یکی است، دارای خصوصیات دینامیکی پیچیده‌تری نسبت به سیستم‌های آشوبی می‌باشند. پیچیدگی در ایجاد نگاشت منجر به افزایش امنیت می‌گردد لذا سیستم فوق آشوب برای ایجاد نگاشت واترمارک روش پیشنهادی انتخاب شده است. از میان سیستم‌های فوق آشوبی ارائه شده سیستم لورنز برگزیده شده است. این سیستم در یک بازه پیوسته خاصیت فوق آشوب دارد در صورتی که دیگر سیستم‌ها فاقد این خاصیت هستند. این مسئله منجر به افزایش کارایی و کاهش پیچیدگی زمانی روش می‌شود. از آنجایی که ورودی مرحله $(n+1)$ام بر اساس خروجی مرحله nام تعیین می‌گردد، در بازه گسسته قرار داشتن هر خروجی در بازه فوق آشوبی باید چک شود. در مقیاس وسیع نیز برای هر خروجی باید توان‌های لیاپانوف محاسبه گردد که این امر باعث افزایش پیچیدگی زمانی و در نتیجه کاهش کارایی روش می‌شود.

سیستم فوق آشوب لورنز با افزودن یک بازخورد (پارامتر k) به سیستم آشوب لورنز حاصل می‌شود[۸]. این سیستم به این صورت تعریف می‌شود: (x_1، x_2، x_3 و x_4 متغیرهای حالت سیستم هستند)

$$-۴ < k < ۴ \qquad (۱)$$

$$\dot{x}_1 = 10(x_2 - x_1)$$

$$\dot{x}_2 = 28x_1 + x_2 - x_1x_3 - x_4$$

$$\dot{x}_3 = x_1x_2 - \frac{8}{3}x_3$$

$$\dot{x}_4 = 0.1x_2x_3 + k$$

۳- روش پیشنهادی

در این مقاله یک روش واترمارکینگ مقاوم برای تصاویر رنگی پیشنهاد می‌دهیم. همانطور که گفته شد در این روش از سیستم فوق آشوب لورنز جهت تولید رشته شبه تصادفی استفاده می‌شود.

فرض می‌شود تصویر رنگی با سایز M*N و واترمارک یک متن با L کاراکتر باشد. در این روش واترمارک می‌تواند از هر نوع داده دیجیتالی انتخاب شود اما نهایتا برای قرارگیری در تصویر باید به صورت باینری تبدیل گردد. مسلما در استخراج واترمارک نوع داده ورودی موثر است زیرا پس از استخراج، داده‌ها بر اساس نوع داده ورودی خوانده می‌شوند.

۳-۱ قراردادن واترمارک

أ. محاسبه سایز تصویر

$$\text{ImageSize} = M*N \qquad (۲)$$

ب. محاسبه سایز واترمارک

$$L = \text{CharacterNumber} \qquad (۳)$$

$$\text{WatermarkSize} = (L*۸) + ۲۰ \qquad (۴)$$

تعداد کاراکترها در ۸ ضرب می‌شود زیرا واترمارک در LSB پیکسل‌ها قرار گرفته بنابراین برای هر کاراکتر نیاز به ۸ پیکسل داریم. ۲۰ بیت به سایز واترمارک اضافه می‌گردد که مشخص کننده سایز مارک است. سیستم فوق آشوب لورنز به تعداد پیکسل‌های مورد نیاز برای واترمارک تکرار می‌گردد بنابراین این مقدار باید برای گیرنده مشخص باشد تا بر اساس آن تکرار سیستم را داشته باشد و واترمارک را استخراج کند.

ت. مقایسه

[1] Determinism
[2] Resilient Statistically

در این بخش سایز واترمارک و تصویر مقایسه می‌گردد و در صورتی که سایز واترمارک بزرگ‌تر از تصویر باشد به کاربر اطلاع داده می‌شود تا تصویر انتخابی خود را تغییر دهد.

If (ImageSize<= WatermarkSize) Continue;

Else Change Image;

ث . ایجاد واترمارک

ابتدا سایز تصویر به صورت آرایه ۲۰ بیتی به فرم باینری تبدیل می‌گردد و سپس متنی که قرار است به عنوان واترمارک در تصویر قرار گیرد مشابه جدول زیر به صورت باینری درمی‌آید.

جدول ۱: تبدیل اطلاعات سایز واترمارک به باینری

	۱	۲	۳	...	۲۰
۱	۱	۰	۱	...	۱

جدول ۲: تبدیل اطلاعات واترمارک به باینری

	۱	۲	۳	۴	...	۸
۱	۱	۰	۱	۱	...	۱
۲	۰	۰	۱	۰	...	۱
۳	۰	۰	۱	۱	...	۰
...	...	...	...	...	...	...
M	۰	۱	۰	۰	...	۰

ج . ایجاد شرایط اولیه

ابتدا شرایط اولیه سیستم مشخص شده و این شرایط با روش RSA رمز شده و برای گیرنده تصویر ارسال می‌گردد تا بر اساس آن ورودی سیستم فوق‌آشوب را ایجاد و رشته شبه تصادفی را تولید نماید. با داشتن تصویر واترمارک شده و رشته شبه تصادفی که جایگاه واترمارک را مشخص می‌کند نیازی به تصویر اصلی نیست و واترمارک بدون وجود تصویر اصلی استخراج می‌شود.

سیستم نامتقارن

RSA : Rivest , Shamir , Adlemen

$$X = Y^e \bmod r \qquad (۵)$$

ح . تولید رشته تصادفی بر اساس سیستم فوق‌آشوب لورنز

در محاسبه محل واترمارک نیاز به سه پارامتر سطر، ستون و صفحه می‌باشد که می‌توان سه پارامتر اول خروجی سیستم لورنز را برای این کار انتخاب کرد این پارامترها باید به صورت تعریف شده برای تصویر تبدیل گردد که به صورت زیر مشخص می‌شود.

جایگاه واترمارک = $(P_{Row}\ ,\ P_{Col}\ ,\ P_P\ )$

$$P_{Row} = \mathrm{mod}(x, RowNum) \qquad (۶)$$

$$P_{Col} = \mathrm{mod}(x, ColNum) \qquad (۷)$$

هر پیکسل با سه بایت RGB یا به عبارتی سه صفحه قرمز، سبز و آبی مشخص می‌گردد.

$$\mathrm{Pixle}(P_{red},\ P_{green},\ P_{blue}) \qquad (۸)$$

$$P_P = \mathrm{mod}(x,3) \qquad (۹)$$

خروجی چهارم سیستم را جهت افزایش امنیت به کار می‌بریم بدین صورت که بر اساس جدول زیر ترتیب سه ورودی اول را برای مرحله بعد تعیین می‌کنیم. فرض می‌کنیم خروجی مرحله nام به صورت z،y،x باشد این ترتیب مستقیما به عنوان ورودی مرحله (n+۱)ام انتخاب نمی‌شود و عامل تعیین کننده پارامتر چهارم است که بر اساس جدول زیر عمل می‌کند.

(۱۰)

$$ModSelecto\,r = \mathrm{mod}(x_4, 6) \qquad \text{(پارامتر چهارم)}$$

جدول ۳: نوع ورودی مرحله (n+۱)ام بر اساس خروجی چهارم مرحله nام

ورودی تکرار(n+۱)	خروجی چهارم در تکرار n
Xyz	۰
Xzy	۱
Yxz	۲
Yzx	۳
Zxy	۴
Zyx	۵

رشته شبه تصادفی که با سه پارامتر ذکر شده جهت تعیین جایگاه واترمارک تولید شده است به صورت زیر می‌باشد.

جدول ۴: رشته شبه تصادفی تولید شده جهت تعیین موقعیت واترمارک در تصویر

	۱	۲	۳	...	Watermark Pixle
P_{Row}	۱۱۱	۲۲	۱۲۱	...	۱۲۵
P_{Col}	۹۴	۱۵۲	۲۱۷	...	۲۴۰
P_P	۲	۱	۳	...	۲

خ . اعمال واترمارک در تصویر

هر کدام از بیت‌ها مشخص شده در جدول ۱ و ۲ بر اساس جدول ۴ در تصویر قرار می‌گیرد.

۲-۳ استخراج واترمارک

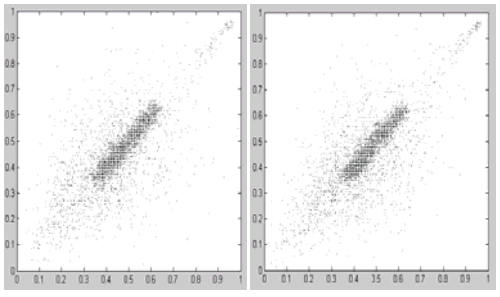
در استخراج واترمارک ابتدا گیرنده بر اساس شرایط اولیه دریافت شده و الگوریتمی که ارائه گردید رشته شبه تصادفی خود را با ۲۰ تکرار تولید می‌کند تا سایز متن واترمارک را به دست آورد سپس بر اساس آن رشته شبه تصادفی را به صورت کامل بر اساس سایز واترمارک تولید و واترماک را استخراج می‌کند. هر ۸ خروجی به عنوان یک کاراکتر در نظر گرفته می‌شود.

۴- نتایج تجربی

شکل ۱: تصویر واترمارک شده(سمت راست) و تصویر اصلی(سمت چپ)

۴-۱ تشابه پیکسل‌های مجاور

در این قسمت تشابه پیکسل‌های مجاور مورب، افقی و عمودی مورد بررسی قرار گرفته است. در تشابه پیکسل‌ها هر چه نقاط نمودار به قطر اصلی نزدیک‌تر باشند نشان دهنده تشابه بیشتر دو پیکسل مجاور به هم است. شکل‌های زیر شباهت پیکسل‌ها را نشان می‌دهند. به وضوح مشخص است که تصویر واترمارک شده و تصویر اصلی از تشابه پیکسل بسیار نزدیکی برخوردار هستند.



شکل ۲: تشابه پیکسل‌ها تصویر واترمارک شده(سمت راست) و تصویر اصلی(سمت‌چپ)

۴-۲ تحلیل ضریب همبستگی

می‌توان برای هر تصویر از رابطه زیر ضریب همبستگی محاسبه کرد. هر چه عدد فوق الذکر بزرگتر باشد نشان از همبستگی بالای پیکسل‌های یک تصویر به یکدیگر دارد.

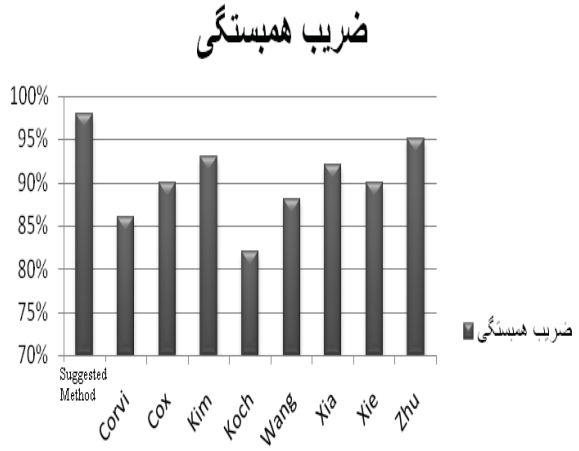
(۱۱)

$$C_r = \frac{N\sum_{j=1}^{N}(x_i \times y_{i)} - \sum_{j=1}^{N}x_j \times \sum_{j=1}^{N}y_j}{\sqrt{\left(N\sum_{j=1}^{N}{x_j}^2 - \left(\sum_{j=1}^{N}x_j\right)^2\right) \times \left(N\sum_{j=1}^{N}{y_j}^2 - \left(\sum_{j=1}^{N}y_j\right)^2\right)}}$$

در تصاویر معمولی این ضریب، عددی نزدیک به یک می‌باشد. در تصاویر واترمارک شده نیز باید این مقدار تا حد زیادی به ضریب همبستگی تصویر اصلی نزدیک باشد یا به عبارتی دیگر نزدیک یک باشد و مانند یک تصویر بدون واترمارک به نظر رسد. جهت ارزیابی توانایی الگوریتم در این زمینه، ضریب همبستگی برای پیکسل‌های مجاور مورب (قطری)، افقی و عمودی در صفحات قرمز، سبز و آبی محاسبه شده است. [۹]

جدول ۵: ضرایب همبستگی تصویر اصلی و واترمارک شده

	تصویر اصلی	تصویر واترمارک شده
همبستگی مورب	۰.۷۵۴۱	۰.۷۴۴۸
همبستگی افقی	۰.۸۲۱۴	۰.۸۲۹۵
همبستگی عمودی	۰.۸۳۷۱	۰.۸۳۰۵

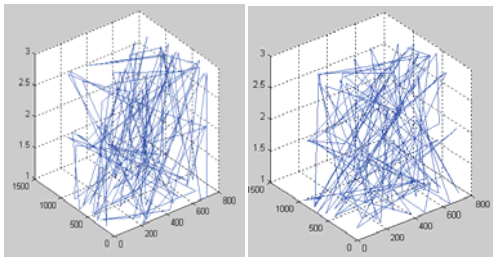


شکل ۳: نمودار مقایسه روش‌های واترمارکینگ بر اساس ضریب همبستگی[۹]

۳-۴ حساسیت به کلید اصلی

یک روش موفق واترمارکینگ، باید حساسیت بسیار زیادی به کلید واترمارک داشته باشد. این حساسیت ایجاب می‌کند که کلیدهای بسیار مشابه (که فقط در یک بیت اختلاف دارند) نگاشت‌های بسیار متفاوت از یکدیگر تولید کنند. به عبارت دیگر هر گونه تغییر حتی به اندازه یک بیت در کلید اصلی باید نگاشت جدید و کاملا متفاوت با نگاشت حاصل از کلید قبلی ایجاد کند. در طی فرایند آشکارسازی واترمارک در صورتی که تصویر با یک کلید بسیار نزدیک به کلید اصلی(که فقط در یک بیت با کلید اصلی متفاوت است) استخراج گردد، باید واترمارک حاصل از این عمل کوچک‌ترین شباهتی به واترمارک اصلی نداشته باشد تا بر اساس شباهت‌ها، واترمارک کشف گردد. از این رو در این بخش آزمایشاتی برای مشخص نمودن حساسیت روش به تصویر و کلید اصلی ارائه می‌شود. [۱۰]

برای تشخیص حساسیت روش به کلید اصلی نگاشت حاصل از دو کلید بسیار مشابه که تنها در یک بیت اختلاف دارند مشخص می‌کنیم. نتایج این آزمون نشان دهنده این است که کلیدهای بسیار مشابه هم که تنها در یک بیت اختلاف دارند پس از اعمال بر روی یک تصویر ، نگاشت‌های بسیار متفاوتی ایجاد کرده اند.



شکل ۴: نمودار نگاشت واترمارک در تصویر با دو کلید مشابه

۴-۴ فضای حالت کلید

تمامی الگوریتم‌های امنیتی در برابر روش تحلیل رمز brute-force یعنی روشی که تمامی حالات کلید اصلی را بر روی رسانه امتحان می‌نماید ، آسیب پذیر هستند. درحالی که تنها راه حل موجود برای مقابله با این روش تحلیل رمز بوجود آوردن یک فضای بسیار زیاد برای حالات ممکن کلید اصلی است. به عبارت دیگر بایستی آنقدر تعداد حالات ممکنِ کلید اصلی(فضای کلید) زیاد باشد که امتحان کردن تمامی آنها با استفاده از قویترین رایانه‌های امروزی جهان مقدور نباشد. برای بررسی فضای کلید روش پیشنهادی لازم است که به رابطه ایجاد سیستم فوق آشوب لورنز دقت کنیم. در این رابطه چهار مقادیر اولیه وجود دارد و در هر مرحله این چهار پارامتر مورد استفاده قرار می‌گیرند. سه پارامتر سطوح پیکسل را مشخص می‌کند و پارامتر چهارم ترتیب استفاده سه پارامتر قبلی در سطوح پیکسل را مشخص می‌کند. با فرض اینکه در بازه اعداد تعریف شده برای تصاویر یک عدد دو رقمی با چهار رقم دقت اعشار داشته باشیم، نتایج زیر حاصل می‌شود:

$(۱۰^{۴})^{۶} = ۱۰^{۲۴}$

در تعیین پیکسل سه سطح داریم : x y z که می‌تواند به ۶ حالت نمایش داده شود.

$(۱۰^{۲۴})^{۶} = ۱۰^{۱۴۴}$

الگوریتم پیشنهادی تا ($۱۰^{۱۴۴}$) حالت ممکن برای کلید اصلی فضا ایجاد کرده است که عددی بسیار مناسب برای جلوگیری از حمله brute-force می‌باشد. به بیانی دیگر، شخصی که قصد دارد با روش brute-force به تصویر حمله نماید باید($۱۰^{۱۴۴}$) حالت ممکن را برای کلید اصلی امتحان نماید که عملاً غیر قابل انجام است. پس در این الگوریتم اندازه کلید اصلی بیش از ($۱۰^{۱۲۰}$) می‌باشد.

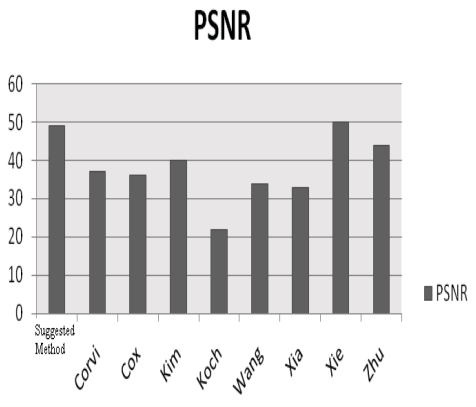
۵-۴ PSNR[1]

از PSNR به عنوان یک مقیاس برای کیفیت تصویر واترمارک شده استفاده کردیم که PSNR برای تصاویر از فرمول زیر به دست خواهد آمد[۱۱]:

$$PSNR = 10 * \log_{10}\left(\frac{255^2}{\frac{1}{W*H}\sum_{i=1}^{W}\sum_{j=1}^{H}(O_{ij} - D_{ij})^2}\right)$$

جدول ۶: PSNR بر اساس سایزهای مختلف واترمارک

سایز واترمارک	PSNR
(سایز تصویر) * ۱/۸	**۴۲.۱۱**
(سایز تصویر) * ۱/۴	**۴۲.۰۹**
(سایز تصویر) * ۱/۲	**۴۲.۰۶**
برابر با سایز تصویر	**۴۲.۰۳**



شکل ۵ : نمودار مقایسه روش‌های واترمارکینگ بر اساس PSNR[۹]

[1] Peak Signal to Noise Ratio

۵- نتیجه‌گیری

در این مقاله الگو واترمارکینگ نوینی ارائه شده است که در تصاویر رنگی و بر پایه سیستم فوق آشوب می‌باشد. در این روش رشته اعداد شبه تصادفی تولید شده توسط سیستم فوق آشوب مشخص کننده موقعیت واترمارک در تصویر می‌باشد. به منظور بالابردن امنیت، پارامتر چهارم سیستم فوق آشوب هر تکرار به عنوان عامل تعیین کننده ترتیب ورودی‌ها در تکرار بعد استفاده شده است. نتایج تجربی نشان می‌دهد روش پیشنهادی تغییرات اعمال شده در تصویر و واترمارک را مشخص می‌کند و این در حالی است که در مقابل حملات آماری و تفاضلی کاملا مقاوم است و حساسیت زیاد سیستم فوق آشوب به شرایط اولیه امنیت سیستم را به نحو قابل توجهی بهبود داده است و موجب افزایش مقاومت، طول و فضای کلید شده است. در این الگو استخراج واترمارک بدون تصویر اصلی امکان‌پذیر می‌باشد. بنابراین الگو پیشنهادی، روشی مناسب جهت واترمارکینگ تصاویر رنگی می‌باشد.

۶- پیشنهادات و کار آینده

کاربرد واترمارکینگ در تصاویر بسیار گسترده شده است. کاربردهای تجاری واترمارک در قالب واترمارک‌ها و اثرانگشت‌های دیجیتال برای ردیابی کپی‌رایت و مالکیت رسانه‌های دیجیتالی بسیار گسترده شده‌اند و الگوریتم‌ها و ابزارهای مختلفی بدین منظور تهیه شده است. فهم نقاط ضعف این سیستم‌ها منجر به ایجاد سیستم‌های مستحکم‌تری می‌شود و زمینه علمی واترمارکینگ را پیشرفت می‌دهد. این کار باعث می‌شود به منظور حمایت از تولید کنندگان از حق کپی و انتشار بهتری استفاده کرد و تکنیک‌های مطمئن‌تری را برای مقاومت در برابر مهاجمان بدست آورد.

تئوری آشوب به دلیل داشتن ویژگی‌های مطلوب پتانسیل استفاده در سیستم‌های واترمارکینگ را دارد. در واترمارکینگ مبتنی بر آشوب، تصویر واترمارک شده کمترین وابستگی آماری را به تصویر اصلی دارد. لذا تنها حمله قابل انجام حمله brute-force است که آن هم به دلیل ثابت نبودن کلید و طول زیاد آن به سختی امکان‌پذیر است. توابع مورد استفاده در الگوریتم‌های واترمارکینگ مبتنی بر آشوب عموماً توابع دارای فیدبک هستند و واترمارک هر بخش از تصویر نه تنها به کلید، بلکه به تصویر واترمارک شده بخش قبلی نیز وابسته است. نکته مهم دیگری که باید عنوان شود این است که با توجه به مقاومت واترمارکینگ مبتنی بر آشوب در برابر الگوریتم‌های تحلیل امروزی، نمی‌توان سطح امنیتی این نوع واترمارک را اندازه گرفت. لذا باید به طریقی مطمئن شویم واترمارکینگ مبتنی بر آشوب فاقد نقطه ضعف است و از سوی دیگر باید بر روی توسعه الگوریتم‌های تحلیل فعالیت نمود و با ارائه الگوریتم‌های تحلیل قوی‌تر و کارآمدتر، نشان داد که آیا الگوریتم‌های واترمارکینگ مبتنی بر آشوب واقعاً فاقد ضعف هستند و در صورت وجود نقاط ضعف در آن‌ها، چگونه می‌توان آن‌ها را بهبود بخشید.

مراجع

[1] Fei Chuhong,Kundur D,Kwong RH.Analysis and design of secure watermark-based authentication systems.IEEE Trans Inf Forensics Security 2006;1(1):43 .55.

[2] Yuan-Liang, Tang,Ching-Ting, Chen,Image authentication using relation measures of wavelet coe .cients.In:Proc Int Conf e- Technology,e-Commerce e-Service;2004.p.541 .5.

[3] Maeno K,Sun Qibin,Chang Shih-Fu,Suto M.New semi-fragile image authentication watermarking techniques using random bias and nonuniform quantization.IEEE Trans Multimedia 2006;8(1):32 .45.

[4] Rinaldi Munir, Bambang Riyanto, Sarwono Sutikno, Wiseto P. Agung, "Secure Spread Spectrum Watermarking Algorithm Based on Chaotic Map for Still Images", International Conference on Electrical Engineering and Informatics, 2007

[5] Zhao Dawei, Chen Guanrong, "A Chaos-Based Robust Wavelet-Domain Watermarking Algorithm ", Chaos, Solitions and Fractals22(2004) 47-54

[6] Deyun Peng, Jiazhen Wang, Peixin Yan, Sumin Yang, Jianli Hu, "A secure dual digital watermarking technique based on wavelet transform and chaos system", International Society for Optical Engineering, 2005

[7] Zhu Congxu, Liao Xuefeng, Li Zhihua, "Chaos-based multipurpose image watermarking algorithm", Wuhan University Journal of Natural Sciences, 2006

[8] Goa T, Chen Z, Gu Q, Yuan Z. "A new hyper-chaos generated from generalized Lorenz system via nonlinear feedback", Chaos, Solitons and Fractals, 2008

[9] E.Marini, F.Autrussea, "Evaluation of Standard Watermarking Technique", Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents, Feb 2008

[10] Belkacem, S. Dibi, Z. Bouridane, "Color Image Watermarking based on Chaotic Map", 14th IEEE International Conference of Electronics, Circuits and Systems, 2007.

[11] Zhenni Peng, Wenbo Liu, "Color image authentication based on spatiotemporal chaos and SVD", Chaos,Solitons and Fractals 36 (2008) 946 .952.