پنجمین کنفرانس انجمن رمز ایران
۲۴ الی ۲۶ مهر ماه ۱۳۸۶ دانشگاه علم و صنعت ایران
انجمن رمز ایران
Iranian Society of Cryptology

نهان‌نگاری تصاویر دیجیتال بر اساس ثبت تصویر و مقاوم در مقابل حملات RST

مجتبی ابوالقاسمی
دانشکده مهندسی برق
دانشگاه صنعتی امیرکبیر
mo_abolghasemi@cic.aut.ac.ir

حسن آقائی‌نیا
دانشکده مهندسی برق
دانشگاه صنعتی امیرکبیر
aghaeini@aut.ac.ir

چکیده: امروزه به خاطر پیشرفت تکنولوژی چندرسانه‌ای روشهای مختلفی برای نهان‌نگاری به منظور حفاظت حق طبع ونشر ارائه شده است. در این مقاله یک آلگوریتم نهان‌نگاری دیجیتال بر اساس تبدیل موجک گسسته و ثبت تصویر، مقاوم در برابر حملات چرخش، مقیاس‌دهی و انتقال (RST) ارائه شده است. در این روش نهان‌نگاری از مدل سیستم بینایی انسان (HVS) جهت ایجاد شدت مناسب پیوند واترمارک به تصویر میزبان تا حد مطلوب استفاده می‌شود. به کار بردن ثبت تصویر بر اساس گشتاورهای زرنیک با استفاده از شبکهٔ عصبی، باعث شده است در مرحلهٔ آشکارسازی، آلگوریتم در مقابل حملات هندسی مقاومت خوبی داشته باشد. همچنین در مقابل حملات غیر هندسی از قبیل برش، فشرده سازی، فیلترنمودن و ... کارایی آلگوریتم مورد ارزیابی واقع شده و نشان می‌دهد روش پیشنهادی در مقابل این نوع حملات نیز مقاومت خوبی دارد.

واژه های کلیدی: نهان‌نگاری، تبدیل موجک گسسته (DWT)، ثبت تصویر، حملات هندسی (RST)، گشتاورهای زرنیک

۱- مقدمه

نهان‌نگاری[1] فرآیندی است که در طی آن اطلاعات (پیام) در دادهٔ دیجیتال مانند صوت، تصویر، فیلم، نرم‌افزار و... به منظور حفاظت حق‌مالکیت[2]، کنترل کپی، صحت‌سنجی[3] داده درج می‌گردد. این ایده برای اولین بار در سال ۱۹۹۰ پدید آمد و از آن به بعد تحقیقات در این زمینه به صورت نمایی رشد یافت.

اولین روش نهان‌نگاری برای تصاویر دیجیتال توسط کارونی[4] در سال ۱۹۹۳ ارائه گردید [1,2]. اگر چه مقالاتی نیز قبل از آن برای ایدهٔ برچسب زدن تصاویر با اطلاعات محرمانه چاپ گردید [3,4]. بعد از آن ایدهٔ استفاده از نهان‌نگاری در سایر داده‌های دیجیتال مانند صوت و فیلم توسعه یافت. اولین کنفرانس دانشگاهی در سال ۱۹۹۶ برگزار گردید [5]. طی سالهای گذشته روشهای نهان‌نگاری مختلفی ارائه گردیده است [6-10].

1 . Watermarking
2 . Copyright Protection
3. Authentication.
4 . Caronni

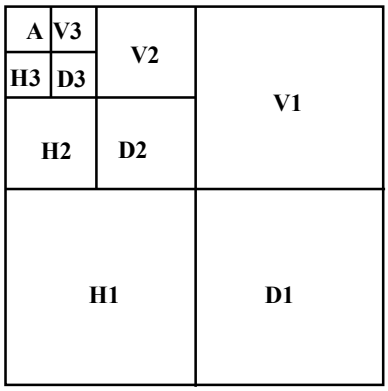
از یک دیدگاه کلی نهانگاری را می‌توان به دو نسل تقسیم نمود. نسل اول[5] روشهایی هستند که عمدتاً نهانگاری را روی کل حوزه رسانه انجام می‌دهند. در این روشها معمولاً در حوزه‌های مکانی و یا تبدیل (مانند DCT،DWT) عمل درج پیام صورت می‌گیرد. در روشهای نهانگاری در حوزه تبدیل، ضرایب تبدیل بر اساس قانون مشخصی تغییر می‌کنند. معمولاً نهانگاری در حوزه تبدیلها مقاومت بیشتری را در برابر حملات و پردازشهای رایج از خود نشان می‌دهد. این روشها در مقابل حملاتی از قبیل فشرده‌سازی JPEG، اضافه کردن نویز، فیلترنمودن و کلاً حملاتی که هندسهٔ رسانه را تحت تاثیر قرار نمی‌دهند مقاومت خوبی دارند ولی عمدتاً در مقابل حملات، خرابی‌ها و پردازشهای هندسی مانند چرخش، مقیاس کردن و انتقال به علت از دست رفتن سنکرونیزاسیون در زمان آشکارسازی واترمارک، کارایی خود را از دست می‌دهند. علاوه بر آن این روشها با تکنیکهای جدید فشرده‌سازی ویدئو و تصویر ساکن مانند استانداردهایJPEG2000 و MPEG4/3 که بر اساس شیء یا ناحیه کار می‌کنند تطابق کمتری دارند. بطور کلی آلگوریتمهای نسل اول (1GW) هنوز نتوانسته‌اند نیازمندیهای نهانگاری خوب با مشخصات زیر را به صورت کامل بر آورده نمایند: (۱) مقاومت: حذف واترمارک مشکل باشد و نسبت به حمله های مختلف و عملیاتهای پردازش تصویر استاندارد مانند، فشرده‌سازی، فیلتر کردن، چرخش، مقیاس‌دهی، برش، و غیره مقاومت نماید. (۲) شفافیت: واترمارک نباید برای بیننده قابل درک باشد و همچنین خرابی قابل ملاحظه ای روی تصویر ایجاد نکند. (۳) امنیت: کاربران غیرمجاز قادر نباشند با استفاده از تحلیلهای استاتیکی رایج یا حمله‌های همبستگی آنرا آشکار نمایند. (٤) عدم ابهام: کاربران مجاز باید اطلاعات درج خورده را بدون ابهام با یک واترمارک بازیافت شده مشخص نمایند.

نسل دوم نهان نگاری روشهایی است که به منظور افزایش مقاومت و نامرئی بودن و غلبه بر مشکلات نسل اول توسعه داده شدند. روشهای نسل دوم ویژگیهای ناحیه‌ای[6]، مرزها و شیء[7] را مورد نظر قرار داده و مزیتهای بیشتری بر حسب آشکارسازی و بازیافت در مقابل حملات هندسی در مقایسه با روشهای نسل اول بدست می‌دهند. این مزیتها با کشف (استخراج) ناحیه مطلوب یا ویژگیهای شئ و مشخصات از تصویر بدست می‌آید. همچنین روشهای نسل دوم طوری طراحی شده‌اند که مقاومتهای قابل انتخاب برای کلاسهای مختلف حمله بدست آید. در نتیجه قابلیت انعطاف نهانگاری بطور قابل ملاحظه بهبود خواهد یافت. در این مقاله ابتدا در بخشهای دوم و سوم مروری بر مباحث تبدلات موجک و گشتاورهای زرنیک خواهیم داشت. آلگوریتم پیشنهادی بر اساس ثبت تصویر در بخش چهارم شرح داده می‌شود و بخش پنجم نیز به آزمایشات و نتایج تجربی بدست آمده اختصاص داده شده است. در انتها نیز نتیجه‌گیری آورده شده است.

۲- تبدیلات موجک

چون DWT یک تبدیل جدائی‌پذیر است، یک DWT دو بعدی را می‌توان با اعمال دوبار متوالی DWT یک بعدی، که ابتدا بر روی سطرها و سپس بر روی ستونهای تصویر اعمال شود پیاده نمود. پیاده‌سازی بانک فیلتر شناخته شده را می‌توان برای استفاده جهت محاسبه DWT دو بعدی بکار برد، که ساختار هرمی زیر باند شکل ۱ را نتیجه می‌دهد. تجزیه سه سطحی نشان داده شده در شکل ۱، دارای ۱۰ زیرباند می‌باشد. که با D_j, H_j, V_j علامت‌گذاری شده است که در آن H، V و D به ترتیب افقی، عمودی و قطری را نشان می‌دهد و j مقیاس یا سطوح تجزیه را نشان می‌دهد. ضرایب تجزیه کنتراست در سمت بالا چپ نشان داده شده و با A علامت گذاری شده است (ضرایب تقریب[8]) [11].

[5]. First Generation Watermarking (1GW)
[6]. Region
[7]. Object
[8]. Approximation Coefficient



شکل ۱: سه سطح DWT از یک تصویر

۳- گشتاورهای زرنیک[9]

چند جمله‌ای‌های زرنیک، یک دنباله نامحدود از چند جمله‌ای هاست که روی دایره یکه متعامد هستند. این گشتاورها یک تصویر تابع دو بعدی روی چند جمله‌ای های مختلط متعامد می باشند [12]. مجموعه چند جمله ای های $\{V_{nm}(x,y)\}$ بصورت زیر تعریف می شود:

$$V_{n,m}(x,y)=R_{n,m}(x,y).\exp\left(j.m.\tan^{-1}(y/x)\right) \qquad (۱)$$

$$x^2+y^2\le 1$$

بطوریکه n و m بترتیب مرتبه و تکرار چند جمله ای بوده و دارای شرایط زیر است:

$$\begin{cases} n\ge 0 \\ |m|\le n \\ n-|m|=2k \end{cases} \qquad (۲)$$

چند جمله‌ای شعاعی $R_{nm}(x,y)$ بصورت زیر تعریف می‌شود:

$$R_{n,m}(x,y)=\sum_{s=0}^{\frac{n-|m|}{2}} B_{n,|m|,s}\cdot(x^2+y^2)^{n-2\cdot s/2} \qquad (۳)$$

$$B_{n,|m|,s}=(-1)^s\cdot\frac{(n-s)!}{s!\cdot(\frac{n+|m|}{2}-s)!\cdot(\frac{n-|m|}{2}-s)!} \qquad (٤)$$

گشتاور زرنیک از مرتبه n و تکرار m برای تابع دو بعدی گسسته $f(x,y)$ با رابطه زیر تعریف می شود:

$$A_{n,m}=\frac{n+1}{\pi}\cdot\sum_x\sum_y f(x,y)\cdot V^*_{n,m}(x,y) \qquad (۵)$$

$$x^2+y^2\le 1$$

گشتاورهای زرنیک را می‌توان توسط گشتاورهای هندسی نیز محاسبه کرد:

$$A_{n,m}=\frac{n+1}{\pi}\sum_{s=0}^{n-|m|/2}\sum_{a=0}^{b}\sum_{d=0}^{|m|} (-j)^d\cdot\binom{|m|}{d}\cdot\binom{b}{a}\cdot B_{n,|m|,s}\cdot G_{n-2.s-2.a-2\cdot d,2.a+d} \qquad (٦)$$

که در آن G_{pq} گشتاور هندسی مرکزی مقیاس شده بمیزان α بوده و بصورت زیر تعریف می‌شود:

$$G_{pq}=\frac{\mu_{pq}}{\alpha^{(p+q+2)/2}} \qquad (۷)$$

و μ_{pq} گشتاور هندسی مرکزی است.

۴- روش نهان‌نگاری پیشنهادی

حملات هندسی را می‌توان به شکلهای مختلف توصیف نمود. ترکیب چرخش، مقیاس‌دهی و انتقال (RST)[10] رایجترین آنهاست. این حملات را می‌توان با چهار پارامتر به صورت زیر نمایش داد:

$$\begin{bmatrix} x_n \\ y_n \end{bmatrix}=\begin{bmatrix} s & 0 \\ 0 & s \end{bmatrix}\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}\begin{bmatrix} x_0 \\ y_0 \end{bmatrix}+\begin{bmatrix} t_1 \\ t_2 \end{bmatrix} \qquad (۸)$$

[9]. Zernike Moments

[10]. Rotation, Scaling and Transform

که در آن (x_0, y_0) مختصات اصلی، (x_n, y_n) مختصات تبدیل یافته تصویر است و $\begin{bmatrix} s & 0 \\ 0 & s \end{bmatrix}$ و $\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$ به ترتیب ماتریسهای مقیاس‌دهی و چرخش و (t_1, t_2) بردار انتقال می‌باشد.

ایده اصلی این تحقیق استفاده از روشهای ثبت تصویر جهت مقابله با این حملات است. هدف ثبت تصویر یافتن تبدیلی است که بهترین تطبیق بین تصویر مرجع و تصویر دیگر را فراهم کند و در کاربردهای وسیعی از قبیل شناسایی الگو، بازسازی تصویر و غیره استفاده می‌شود. به طور کلی فرآیند ثبت تصویر، استخراج ویژگیهایی از هر تصویر و تخمین پارامترهای تبدیل هندسی است. در شکلهای ۲ و ۳ بلوک دیاگرام روش پیشنهادی به ترتیب برای درج و استخراج واترمارک آورده شده است.

۴-۱- مرحلهٔ درج واترمارک

مرحله ۱: ابتدا دنباله‌ای باینری شبه‌تصادفی با طول M1×M2 با یک کلید محرمانه K ایجاد شده توسط کاربر، به فضای دوبعدی S ترسیم می‌شود. قبل از درج واترمارک W با S رمزگذاری می‌شود. واترمارک رمز شده $WS = W \oplus S$ است. همچنین W برای ناپدید کردن رابطه خاص و افزایش عدم مرئی بودن می‌تواند براساس مشخصات اسکرامبل شده، جایگردان[11] شود.

مرحله ۲، برای روش نهان‌نگاری با استفاده از چهارچوب DWT، تصویر میزبان با اندازه $N \times N$ به بلوکهای $n \times n$ بصورت غیرهمپوشانی تقسیم شده و DWT سه سطحی برای هر یک بلوک دیتا بطور مستقل بدست می‌آید. برای تصویر پوششی I ، تعداد $\left(\frac{N}{n}\right)^2$ بلوک با اندازه $n \times n$ ایجاد می شود. برای حصول تعداد بلوکهای مساوی با تصویر I، واترمارک فرض شده WS به بلوکهای با اندازه مساوی با تعداد بلوکهای $\left(\frac{M}{n}\right)^2$ تجزیه می‌شود.

مرحله ۳: برای هر بلوک $n \times n$ تصویر پوششی، درج واترمارک فقط بر روی ضرایب تجزیه سطح سوم انجام می‌شود. برای درج واترمارک ، ضرایب سطح سوم در هر بلوک تصویر انتخاب شده و تغییر داده می‌شوند. فرمول درج بصورت زیر است:

$$C_D^*(u,v,b) = \begin{cases} C_D(u,v,b) + J(u,v,b).WS(u,v,b), & |C_D(u,v,b)| > J(u,v,b) \\ C_D(u,v,b) & otherwise \end{cases} \quad (۹)$$

که در آن $C_D(u,v,b)$ ضریب DWT امین بلوک (u,v) b تصویر پوششی I را نشان می‌دهد و $C_D^*(u,v,b)$ ضرایب اصلاح شده را نمایش می‌دهد و $WS(u,v,b)$ دنباله واترمارک رمز شده و $J(u,v,b)$ آستانه‌های JND محاسبه شده برای هر ضریب فرکانسی در هر بلوک است. در این تحقیق از مدل HVS بکار رفته در مرجع [13] استفاده شده است.

مرحله ۵: بعد از درج واترمارک در ضرایب تبدیل معکوس روی بلوکهای گرفته شده تا تصویر نهان نگاری شده IW ایجاد شود.

۴-۲- ثبت تصویر

روشهای مختلفی برای ثبت تصویر وجود دارد. در این تحقیق برای ثبت تصویر از آموزش یک شبکهٔ عصبی پیش‌سو جهت تخمین پارامترهای تبدیل مستوی[12] استفاده شده است. هر تصویر در مجموعهٔ آموزش با مقادیر رندوم چرخش، مقیاس کردن و انتقال در محدوده‌های مشخص بکار گرفته شد. سپس ۵۸ گشتاور زرنیک از هر تصویر به عنوان ورودی شبکهٔعصبی در نظر گرفته شد. در لایهٔ مخفی ۲۵ نرون و در لایهٔ خروجی نیز چهار نرون برای پارامترهای تبدیل مستوی در نظر گرفته شد. همچنین از توابع تبدیل سیگموید در لایهٔ مخفی و توابع خطی در لایهٔ خروجی استفاده گردید. ۲۰۰ تصویر مختلف در مرحلهٔ آموزش به کار گرفته شد. نتایج تست این شبکه که بر

[11] . Permute

[12] . Affine

روی تصویر لِنا انجام شده در جدول ۲ آورده شده است. ملاحظه می‌گردد با دقت مناسبی پارامترهای تبدیل مستوی تخمین زده شده‌اند.

جدول ۲: تخمین پارامترها برای ثبت تصویر

حمله	پارامتر حمله	پارامترهای ثبت شده		
		چرخش	مقیاس دهی	انتقال
بدون حمله		۰/۰۸۳	۰/۹۹۹۹	[-۰/۰۰۸۲ ۰/۰۲۳۲]
مقیاس‌دهی	۰/۷۵	-۰/۰۶۳۲	۰/۷۴۳۲	[-۰/۰۵۱ ۰/۰۰۸۱]
	۱/۱	۰/۰۹۶۵	۱/۱۰۵۴	[-۰/۲۴۳۲ ۰/۱۵۷۸]
چرخش	۵ °	۰/۰۵۴۶	۰/۹۹۹۹	[-۰/۱۵۴۳ ۰/۲۳۱۰]
	۴۵ °	۴۴/۹۹۲۳	۱/۰۰۴۳	[-۰/۰۱۳۶ ۰/۱۵۴۳]
انتقال	[۱ ۰]	-۰/۰۳۴۵	۱/۰۰۰۳	[۰/۲۳۴۱ -۱/۲۳۸۱]
	[۳- ۳]	-۰/۲۳۴۳	۰/۹۹۸۹	[-۳/۰۹۳۲ ۲/۹۱۲۳]
ترکیب حملات	(۱۰ °، ۰/۷۵، [۲ -۳])	۹/۹۵۴۳	۰/۷۵۰۳	[-۳/۱۲۰۶ ۱/۹۵۴۳]
	(۴۵ °، ۰/۹، [۱- ۲])	۴۵/۰۸۳۴	۰/۹۰۳۲	[۱/۸۳۴۲ -۱/۲۳۱۴]

۴-۳- استخراج واترمارک

فرآیند استخراج واترمارک مشابه با فرآیند درج است منتها بصورت معکوس. تنها تبدیل DWT معکوس لازم نیست.

مرحله ۱: ابتدا تصویر نهان‌نگاری شده تست IW و تصویر اصلی I به شبکهٔ عصبی داده شده تا میزان حملات هندسی وارد شده به آن مشخص گردد. با تعیین پارامترهای حمله معکوس تبدیل مستوی روی تصویر تست انجام شده و به ورودی آشکارساز واترمارک داده می‌شود.

مرحله ۳: تصویر نهان‌نگاری شده تست IW' و تصویر اصلی I به بلوکهای $n\times n$ تقسیم می‌شود و هر بلوک بصورت مستقل تبدیل DWT گرفته می‌شود.

مرحله ٤: ضرایب فرکانسی میانی بلوکها از IW,I بصورت مشابه روش درج انتخاب می‌شوند. رویه مورد نیاز دیگر محاسبه JND ضرایب مربوطه است.

مرحله ۵: استخراج اطلاعات واترمارک: اطلاعات واترمارک درج شده بصورت زیر قابل وصول است.

$$WS^*(u,v,b)= \quad (۱۰)$$
$$\begin{cases} 1 & \left|C_D^*(u,v,b)-C_D(u,v,b)\right| > 0.65J(u,v,b) \\ 0 & otherwise \end{cases}$$

مرحله ٦: با کلید محرمانه K دنباله شبه‌تصادفی مشابه با مرحله رمزگاری اطلاعات ایجاد کرده و واترمارک استخراج می‌گردد.

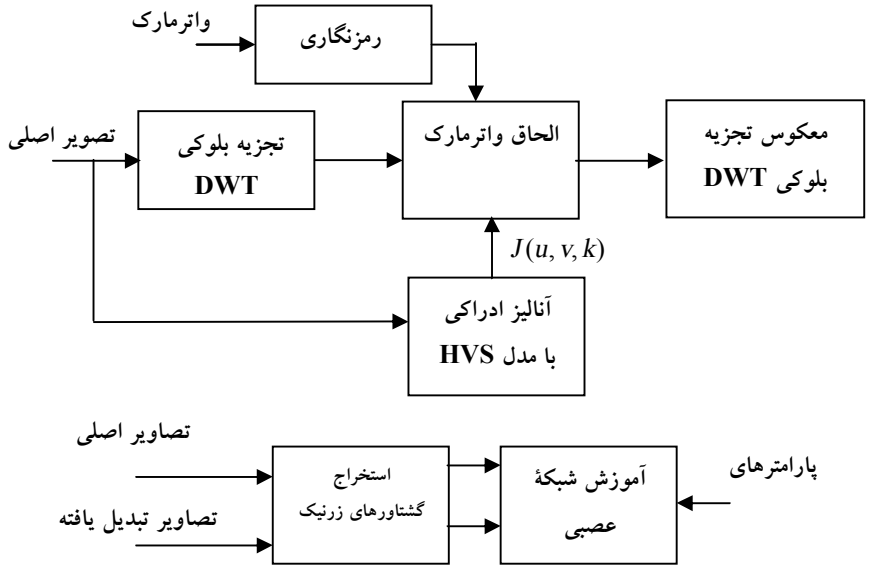
۵- نتایج تجربی

در آزمایشات، از تصاویر سطح خاکستری مختلفی (مانند لِنا، بابون و ...) با اندازه‌های ۵۱۲ × ۵۱۲ جهت تست آلگوریتم استفاده شد. شکل ۴ تصویر اصلی و نهان‌نگاری شده و همچنین واترمارک استخراج شده را نشان می‌دهد. ملاحظه می‌شود که آلگوریتم اعوجاج قابل ملاحظه‌ای روی تصویر نهان‌نگاری شده ایجاد نمی‌کند و تصویر واترمارک استخراج شده با تصویر اصلی آن یکی است.

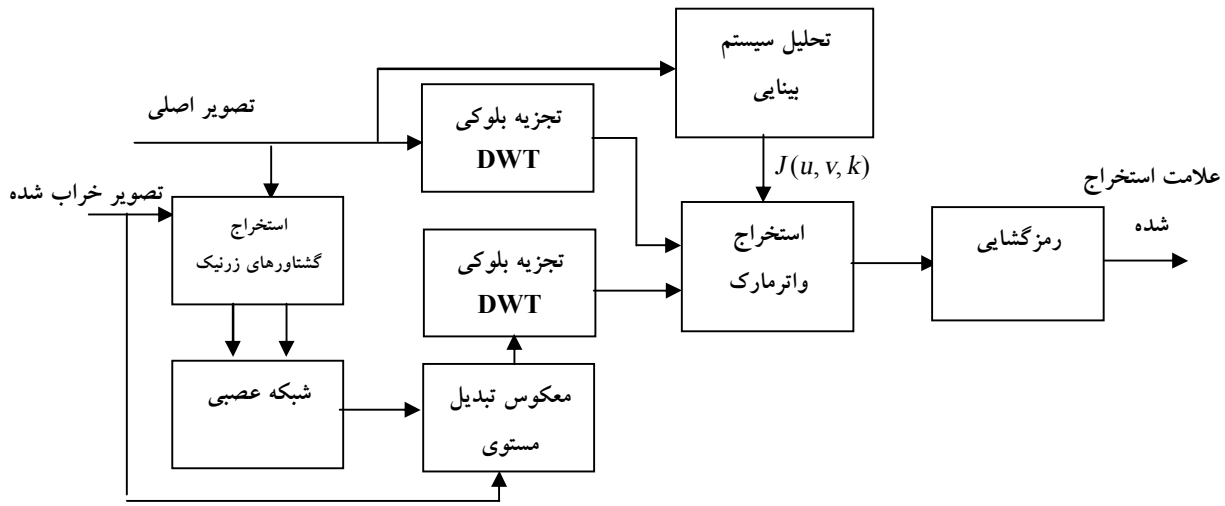
برای ارزیابی کیفیت تصویر نهان نگاری شده و واترمارک استخراج شده، از PSNR (پیک نسبت سیگنال به نویز) و (همبستگی نرمالیزه شده) NC معیار شباهت بین واترمارک درج شده W و واترمارک استخراج شده W^* استفاده شده است. PSNR بصورت زیر تعریف می‌شود:

$$PSNR = 10.\log\left(\frac{255^2}{\frac{1}{N1.N2}\sum_{i=0}^{i=N1-1}\sum_{j=0}^{j=N2-1}(I(i,j)-IW(i,j))^2}\right) dB \quad (۱۱)$$

که در آن $I(i,j)$ و $IW(i,j)$، (i,j)امین مقدار پیکسل در تصویر پوششی و تصویر نهان‌نگاری شده است.



شکل ۲: فرآیند درج واترمارک



شکل ۳: فرآیند آشکارسازی واترمارک

NC بصورت زیر تعریف می شود:

$$NC = \sum_{i=0}^{M1-1}\sum_{j=0}^{M2-1} W(i,j)W^*(i,j) / \sum_{i=0}^{M1-1}\sum_{j=0}^{M2-1}[W(i,j)]^2 \qquad (۱۳)$$

جدول ۱ : مقادیر PSNR (dB) تصاویر نهانگاری شده

تصویر	Baboon	Pepper	Jet	Lena
PSNR	۳۹/۰۷	۴۱/۴۸	۴۰/۲۷	۴۳/۳۰

مقدار PSNR، تصویر نهاننگاری شده ۴۳/۳dB است. در شکل ۴ نشان داده شده است که کیفیت تصویر نهانگاری شده خوب را بیان می‌کند و نیازمندیهای نهانگاری را برآورده می‌نماید. در کنار کیفیت تصویر خوب، واترمارک استخراج شده W^* مشابه تصویر اصلی است با NC برابر ۱، دارد. تصاویر دیگری نیز تست شدند و نتایج برای مقایسه در جدول ۱ آورده شده است.

۵-۱- ارزیابی در مقابل حملات غیر هندسی

ابتدا آلگوریتم برای حملات غیر هندسی مانند فشرده‌سازی JPEG، اضافه کردن نویز، فیلتر کردن، و ... مورد تست قرار گرفت. بعد از اینکه تصویر تحت حملات مختلف قرار گرفت واترمارک استخراج شده هنوز از نظر بصری قابل دریافت است. نتایج این آزمایشات در جدول ۲ جهت مقایسه، آورده شده است.

(الف)

(ب)

شکل ۴: نتایج پیوند و استخراج واترمارک (الف) تصویر و واترمارک اصلی، (ب) تصویر نهان‌نگاری شده و واترمارک استخراج شده

جدول ۱ : مقادیر PSNR (dB) تصاویر نهان‌نگاری شده

تصویر	Baboon	Pepper	Jet	Lena
PSNR	۳۹/۰۷	۴۱/۴۸	۴۰/۲۷	۴۳/۳۰

۵-۱- ارزیابی در مقابل حملات غیر هندسی

ابتدا آلگوریتم برای حملات غیر هندسی مانند فشرده‌سازی JPEG، اضافه کردن نویز، فیلتر کردن، و ... مورد تست قرار گرفت. بعد از اینکه تصویر تحت حملات مختلف قرار گرفت واترمارک استخراج شده هنوز از نظر بصری قابل دریافت است. نتایج این آزمایشات در جدول ۲ جهت مقایسه، آورده شده است.

۵-۲- ارزیابی در مقابل حملات هندسی

برای حملات هندسی چرخش، مقیاس کردن و انتقال نیز آزمایشات متفاوتی انجام شد. نتایج مربوط به حملات مختلف چرخش در جدول ۳ آورده شده است. با چرخش معکوس بر روی تصویر نهان‌نگاری شده واترمارک استخراج می‌گردد. نتایج نشان می‌دهد واترمارک استخراج شده مشابه واترمارک اصلی است. دلیل کمتر بودن مقدار NC از ۱، خطای تخمین زاویهٔ چرخش توسط بخش ثبت تصویر است

جدول ۲: مقاومت در مقابل حملات مختلف غیر هندسی

نوع حمله	PSNR	NC
برش	۱۰/۷۳	۰/۵۶
متعادل کردن هیستوگرام	۱۹/۲۴	۰/۸۷
مقیاس‌دهی	۲۶/۰۱	۰/۶۳
نویز گاووسی	۲۰/۰۵	۰/۳۸
فیلتر میانه	۲۶/۶۲	۰/۶۵
فیلتر پایین‌گذر	۲۵/۷۶	۰/۶۴
فشرده‌سازی JPEG ٪۱۰۰	۲۵/۷۹	۱
فشرده‌سازی JPEG ٪۹۰	۲۵/۶۸	۰/۹۴
فشرده‌سازی JPEG ٪۸۰	۲۵/۵۹	۰/۹۲
فشرده‌سازی JPEG ٪۷۰	۲۵/۵۴	۰/۹۰
فشرده‌سازی JPEG ٪۵۰	۲۵/۴۳	۰/۸۴
فشرده‌سازی JPEG ٪۳۰	۲۵/۲۳	۰/۷۳
فشرده‌سازی JPEG ٪۲۰	۲۵/۱۰	۰/۶۴
فشرده‌سازی JPEG ٪۱۵	۲۴/۹۳	۰/۵

جدول ۳: نتایج مربوط به حمله چرخش مختلف

درجه	۳۰ °	۴۵ °	۶۰ °	۱۲۰ °
NC	۰/۹۱۱	۰/۸۰۹	۰/۸۴۵	۰/۹۲۱
درجه	۱۵۰ °	۲۰۰ °	۲۴۰ °	۳۰۰ °
NC	۰/۸۹۸	۰/۹۳۷	۰/۹۰۱	۰/۸۲۳

در جداول ٤ و ٥ به ترتیب نتایج مربوط به حملات مقیاس دهی و انتقال ذکر شده‌اند. در اینجا نیز با مقیاس کردن و انتقال دوبارهٔ تصویر نهان‌نگاری شده واترمارک استخراج می‌گردد. ملاحظه می‌شود NC مقادیر قابل قبولی را برای آشکارسازی واترمارک فراهم نموده است.

جدول ۴: نتایج مربوط به حمله مقیاس‌دهی مختلف

فاکتور	NC	فاکتور	NC
۰/۹	۰/۹۸۷	۱/۵	۰/۹۹۰
۰/۷۵	۰/۹۸۵	۲	۰/۹۴۷
۰/۵	۰/۸۶۵	۳	۰/۹۲۵
۰/۴	۰/۸۰۲	۵	۰/۹۴۶
۰/۳	۰/۷۵۳	۱۰	۰/۹۴۱

جدول ۵: نتایج مربوط به حمله انتقال مختلف

فاکتور	۱	۳	۵	۱۰
NC	۰/۹۹۸	۰/۹۰۱	۰/۷۵۶	۰/۶۵۴
درجه	-۱	۳ -	-۵	-۱۰
NC	۰/۹۵۸	۰/۸۵۲	۰/۶۰۵	۰/۶۰۰

۶- نتیجه‌گیری

در این مقاله یک روش نهان‌نگاری بر اساس تبدیل موجک ارائه گردید که با به کار بردن ثبت تصویر آنرا در مقابل حملات هندسی مقاوم نمودیم. دقت روش ارائه شده به نوع آلگوریتم و روشی که برای ثبت تصویر بکار می‌رود بستگی دارد. در اینجا با استفاده از یک شبکهٔ عصبی پیش-سو دقت مناسبی را برای تخمین پارامترهای تبدیل مستوی بدست آوردیم و در نتیجه مقاومت خوبی در مقابل حملات چرخش، مقیاس کردن و انتقال حاصل گردید.

۷- مراجع

[1] G. Caronni. Ermitteln unauthorisierter verteiler von maschinenlesbaren daten. Technical report, ETH Z¨urich, Switzerland, August 1993.
[2] Germano Caronni. Assuring ownership rights for digital images. In H.H. Br¨uggermann and W. Gerhardt-H¨ackl,

editors, *Reliable IT Systems (VIS'95)*, pages 251{263. Vieweg Publishing Company, Germany, 1995.
[3] K. Tanaka, Y. Nakamura, and K. Matsui. Embedding secret information into a dithered multilevel image. In *Proceeding of the 1990 IEEE Military Communications Conference*, pages 216{220, September 1990.
[4] K. Tanaka, Y. Nakamura, and K. Matsui. Embedding the attribute information into a dithered image. *Systems and Computers in Japan*, 21(7), 1990.
[5]. Ross J. Anderson, editor. *Information hiding: _rst international workshop*, volume 1174 of *Lecture Notes in Computer Science*, Isaac Newton Institute, Cambridge, England, May 1996. Springer-Verlag, Berlin, Germany, ISBN 3-540-61996-8.
[6] David Aucsmith, editor. *Information Hiding: Second International Workshop*, volume 1525 of *Lecture Notes in Computer Science*, Portland, Oregon, USA, 1998. Springer-Verlag, Berlin, Germany, ISBN 3-540-65386-4.
[7]. Mitchell D. Swanson, Mei Kobayashi, and Ahmed H. Tew_k. Multimedia data-embedding and watermarking technologies. Proceedings of the IEEE, 86(6):1064{1087, June 1998.
[8] Michel Arnold, Martin Schmucker, Stephen D. Wlthusen, Techniques and Applications of Digital Watermarking and Content Protection, Artech House, 2003.
[9] Chun-Shien Lu, Multimedia Security: Steganography and Digital Watermarking Techniques for Intelectual Property, IDEA GROUP PUBLISHING 2004.
[10] Kutter, M., Bhattacharjee, S.K., & Ebarahimi, T., Towards second generation watermarking schemes. International Conference on Image Processing Proceeding, ICIP 99, (vol, 1, pp. 320-323).
[11] Sean B. Ziegeler, Hrishikesh Tamhankar, James E. Fowler, Lori Mann Bruce," Wavelet-Based Watermarking of Remotely Sensed Imagery Tailored to Classification Performance", IEEE 2004, pp. 259-262.
[12] Belkasim, S.O., Shridhar, M. , Ahmadi, M. : "Pattern recognition with moment invariants, a comparative study and new results. Pattern Recognition", 24(12), (1991) 1117-1138