

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

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

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

چکیده: امروزه به خاطر پیشرفت تکنولوژی چندرسانه‌ای روش‌های مختلفی برای نهان‌نگاری به منظور حفاظت حق طبع و نشر ارائه شده است. در این مقاله یک الگوریتم 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 شبکه عصبی، باعث شده است در مرحله آشکارسازی، الگوریتم در مقابل حملات هندسی مقاومت خوبی داشته باشد. همچنین در مقابل حملات غیر هندسی از قبیل برش، فشرده سازی، فیلتر نمودن و ... کارایی الگوریتم 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

اولین روش نهان‌نگاری برای تصاویر دیجیتال توسط کارونی^۴ در سال ۱۹۹۳ ارائه گردید [1,2]. اگر چه مقالاتی نیز قبل از آن برای ایده برچسب زدن تصاویر با اطلاعات محرمانه چاپ گردید [3,4]. بعد از آن ایده 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].

نهان‌نگاری^۱ فرآیندی است که در طی آن اطلاعات (پیام) در داده دیجیتال مانند صوت، تصویر، فیلم، نرم‌افزار و... به منظور حفاظت حق مالکیت^۲، کنترل کپی، صحت‌سنجی^۳ 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.

1. Watermarking
2. Copyright Protection
3. Authentication.

4. Caronni

شیء^۷ 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 شیء 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 نهان‌نگاری 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. الگوریتم 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^۸) [11].

از یک دیدگاه کلی نهان‌نگاری را می‌توان به دو نسل تقسیم نمود. نسل اول^۵ روشهایی هستند که عمدتاً نهان‌نگاری را روی کل حوزه رسانه انجام می‌دهند. در این روشها معمولاً در حوزه‌های مکانی و یا تبدیل (مانند DWT, DCT) عمل درج پیام صورت می‌گیرد. در روشهای نهان‌نگاری در حوزه تبدیل، ضرایب تبدیل بر اساس قانون مشخصی تغییر می‌کنند. معمولاً نهان‌نگاری در حوزه تبدیلهای 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 هندسه 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 استانداردهای JPEG2000 و MPEG4/3 که بر اساس شیء یا ناحیه کار می‌کنند تطابق کمتری دارند. بطور کلی الگوریتمهای نسل اول (IGW) هنوز نتوانسته‌اند نیازمندیهای نهان‌نگاری خوب با مشخصات زیر را به صورت کامل بر آورده نمایند: (۱) مقاومت: حذف واترمارک مشکل باشد و نسبت به حمله‌های مختلف و عملیتهای 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 ملاحظه‌ای روی تصویر ایجاد نکند. (۳) امنیت: کاربران غیرمجاز قادر نباشند با استفاده از تحلیلهای استاتیکی رایج یا حمله‌های همبستگی آنها آشکار نمایند. (۴) عدم ابهام: کاربران مجاز باید اطلاعات درج خورده را بدون ابهام با یک واترمارک بازیافت شده مشخص نمایند.

نسل دوم نهان‌نگاری روشهایی است که به منظور افزایش مقاومت و نامرئی بودن و غلبه بر مشکلات نسل اول توسعه داده شدند. روشهای نسل دوم ویژگیهای ناحیه‌ای^۶، مرزها و

⁷. Object
⁸. Approximation Coefficient

⁵. First Generation Watermarking (IGW)
⁶. Region

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:

$$C_D^*(u, v, b) = \begin{cases} C_D(u, v, b) + J(u, v, b) \cdot WS(u, v, b), & |C_D(u, v, b)| > J(u, v, b) \\ C_D(u, v, b) & otherwise \end{cases} \quad (9)$$

که در آن $C_D(u, v, b)$ ضریب DWT امین بلوک 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.

۲-۴- ثبت تصویر

روشهای مختلفی برای ثبت تصویر وجود دارد. در این تحقیق برای ثبت تصویر از آموزش یک شبکه عصبی پیش سو جهت تخمین پارامترهای تبدیل مستوی^{۱۲} استفاده شده است. هر تصویر در مجموعه 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 شبکه عصبی در نظر گرفته شد. در لایه مخفی ۲۵ نرون و در لایه خروجی نیز چهار نرون برای پارامترهای تبدیل مستوی در نظر گرفته شد. همچنین از توابع تبدیل سیگموئید در لایه مخفی و توابع خطی در لایه خروجی استفاده گردید. ۲۰۰ تصویر مختلف در مرحله آموزش به کار گرفته شد. نتایج تست این شبکه که بر

که در آن (x_0, y_0) مختصات اصلی، (x_n, y_n) مختصات تبدیل یافته تصویر است و $\begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix}$ و $\begin{bmatrix} s & 0 \\ 0 & s \end{bmatrix}$ به ترتیب ماتریسهای مقیاس دهی 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- مرحله درج واترمارک

مرحله ۱: ابتدا دنباله‌ای باینری شبه تصادفی با طول $M1 \times M2$ 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 اسکراملبل شده، جایگردان^{۱۱} شود.

مرحله ۲، برای روش نهان نگاری 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 می‌شود. 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.

¹² . Affine

¹¹ . Permute

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

$$WS^*(u, v, b) = \begin{cases} 1 & |C_D^*(u, v, b) - C_D(u, v, b)| > 0.65J(u, v, b) \\ 0 & otherwise \end{cases} \quad (10)$$

مرحله ۶: با کلید محرمانه K دنباله شبه تصادفی مشابه با مرحله رمزگاری اطلاعات ایجاد کرده و واترمارک استخراج می‌گردد.

۵- نتایج تجربی

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

برای ارزیابی کیفیت تصویر نهان‌نگاری 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:

$$PSNR = 10 \cdot \log \left(\frac{255^2}{\frac{1}{N1 \cdot N2} \sum_{i=0}^{N1-1} \sum_{j=0}^{N2-1} (I(i, j) - IW(i, j))^2} \right) \text{ dB} \quad (11)$$

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

روی تصویر لِنَا 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

انتقال	پارامترهای ثبت شده		پارامتر حمله	حمله
	مقیاس دهی	چرخش		
				بدون حمله
[-۰.۰۸۲ ۰.۰۲۳۲]	۰/۹۹۹۹	۰/۰۸۳	۰/۷۵	مقیاس دهی
[-۰.۰۵۱ ۰/۰۰۸۱]	۰/۷۴۳۲	-۰/۰۶۳۲	۱/۱	ی
[-۰.۲۴۳۲ ۰/۱۵۷۸]	۱/۱۰۵۴	۰/۰۹۶۵	۵°	چرخش
[-۰.۱۵۴۳ ۰/۲۳۱۰]	۰/۹۹۹۹	۰/۰۵۴۶	۴۵°	
[-۰.۱۳۶ ۰/۱۵۴۳]	۱/۰۰۴۳	۴۴/۹۹۲۳	[۱ ۰]	انتقال
[۰.۲۳۴۱ -۱/۲۳۸۱]	۱/۰۰۰۳	-۰/۰۳۴۵	-۳	
[-۰.۰۹۳۲ ۲/۹۱۲۳]	۰/۹۹۸۹	-۰/۲۳۴۳	[۳	
[-۰.۱۲۰۶ ۱/۹۵۴۳]	۰/۷۵۰۳	۹/۹۵۴۳	(۱۰°، ۰/۷۵	ترکیب حملات
			[۲ -۳]	
			(
[۱/۸۳۴۲ -۱/۲۳۱۴]	۰/۹۰۳۲	۴۵/۰۸۳۴	(۴۵°، ۰/۹	
			۲)	
			(-۱)	

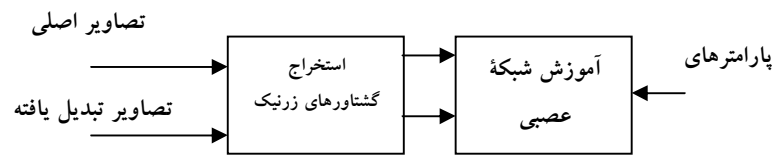
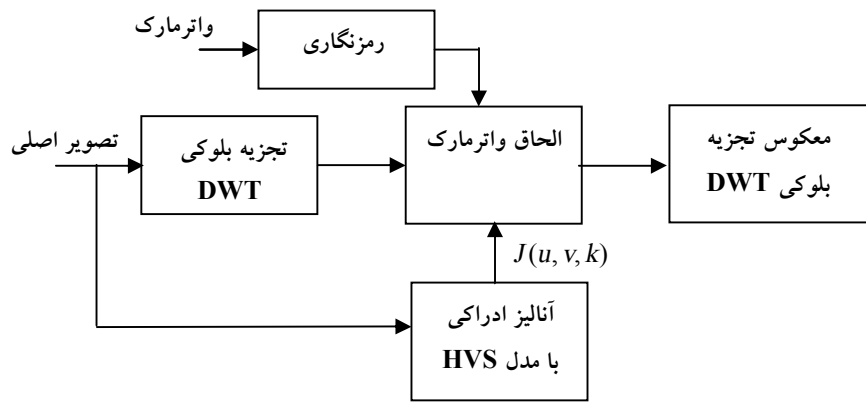
۳-۴- استخراج واترمارک

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

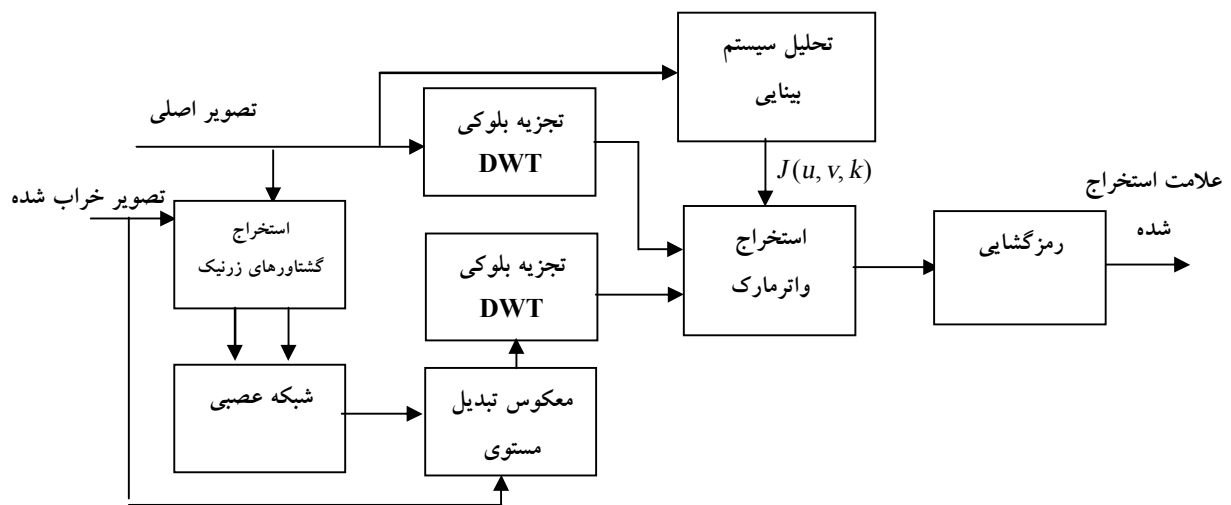
مرحله ۱: ابتدا تصویر نهان‌نگاری شده تست IW و تصویر اصلی I به شبکه عصبی داده شده تا میزان حملات هندسی وارد شده به آن مشخص گردد. با تعیین پارامترهای حمله معکوس تبدیل مستوی روی تصویر تست انجام شده و به ورودی آشکارساز واترمارک داده می‌شود.

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

مرحله ۴: ضرایب فرکانسی میانی بلوکها از IW, I بصورت مشابه روش درج انتخاب می‌شوند. رویه مورد نیاز دیگر محاسبه JND ضرایب مربوطه است.



شکل ۲: فرآیند درج واترمارک



شکل ۳: فرآیند آشکارسازی واترمارک

NC بصورت زیر تعریف می شود:

$$NC = \frac{\sum_{i=0}^{M1-1} \sum_{j=0}^{M2-1} W(i, j)W^*(i, j)}{\sum_{i=0}^{M1-1} \sum_{j=0}^{M2-1} [W(i, j)]^2} \quad (13)$$

جدول ۱: مقادیر PSNR (dB) تصاویر نهان‌نگاری شده

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

مقدار PSNR، تصویر نهان‌نگاری شده ۴۳/۳۰dB است. در شکل ۴ نشان داده شده است که کیفیت تصویر نهان‌نگاری شده خوب را بیان می‌کند و نیازمندیهای نهان‌نگاری 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 الگوریتم 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.

نشان می‌دهد واترمارک استخراج شده مشابه واترمارک اصلی است. دلیل کمتر بودن مقدار NC از ۱، خطای تخمین زاویه چرخش توسط بخش ثبت تصویر است

جدول ۲: مقاومت در مقابل حملات مختلف غیر هندسی

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

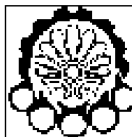
جدول ۳: نتایج مربوط به حمله چرخش مختلف

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

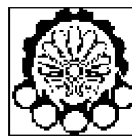
در جداول ۴ و ۵ به ترتیب نتایج مربوط به حملات مقیاس دهی و انتقال ذکر شده‌اند. در اینجا نیز با مقیاس کردن و انتقال دوباره تصویر نهان‌نگاری شده واترمارک استخراج می‌گردد. ملاحظه می‌شود NC مقادیر قابل قبولی را برای آشکارسازی واترمارک فراهم نموده است.



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

۱-۵- ارزیابی در مقابل حملات غیر هندسی

ابتدا الگوریتم 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.

۲-۵- 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

[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. Wlhusen, *Techniques and Applications of Digital Watermarking and Content Protection*, Artech House, 2003.

[9] Chun-Shien Lu, *Multimedia Security: Steganography and Digital Watermarking Techniques for Intellectual Property*, IDEA GROUP PUBLISHING 2004.

[10] Kutter, M., Bhattacharjee, S.K., & Ebrahimi, 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

جدول ۴: نتایج مربوط به حمله مقیاس دهی مختلف

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

جدول ۵: نتایج مربوط به حمله انتقال مختلف

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

۶- نتیجه گیری

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 الگوریتم و روشی که برای ثبت تصویر بکار می رود بستگی دارد. در اینجا با استفاده از یک شبکه 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 Zurich, Switzerland, August 1993.

[2] Germano Caronni. Assuring ownership rights for digital images. In H.H. Brüggermann and W. Gerhardt-Hackl,

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.