



# نهان نگاری دیجیتال تصویر به روش طیف گسترده

مریم سعیدمهر، ساجده نیک‌نداف و نسترن عشوری<sup>۱</sup>

<sup>۱</sup> دانشکده برق و کامپیوتر، دانشگاه صنعتی اصفهان، اصفهان، ایران

**چکیده:** گسترش سیستم‌های چندرسانه‌ای استفاده از شبکه‌های کامپیوتری و اینترنت، دسترسی به اطلاعات دیجیتال و کپی‌برداری از آن‌ها را به آسانی ممکن کرده است. بنابراین مسئله‌ی حفاظت از داده‌ها در مقابل کپی‌برداری و جعل، اهمیت فراوانی دارد. از بین روش‌های حفاظت از داده می‌توان به استفاده از نهان نگاری و روش‌های مختلف رمزنگاری اشاره کرد. به فرایند گنجاندن واترمارک در میان داده‌های دیجیتال معمولی، نهان نگاری دیجیتال گفته می‌شود. نهان نگاری دیجیتال در حوزه‌های مختلفی از جمله تبلیغات و تجاری سازی، حفاظت از حق نشر، حفاظت از داده در مقابل هکرها و ... کاربرد دارد. در نهان نگاری باید پارامترهایی همچون شفافیت، مقاومت و ظرفیت در نظر گرفته شود. ما در این مقاله به بررسی پنج مورد از روش‌های موجود برای نهان نگاری دیجیتال می‌پردازیم که هر کدام تلاش می‌کنند تهاوت بین این سه پارامتر را ارضا کنند و الگوریتم‌های قبلی را بهبود بخشند.

**کلمات کلیدی:** نهان نگاری دیجیتال، واترمارک، حق نشر، شفافیت، مقاومت

## ۱ مقدمه

ممکن توسط چشم انسان قابل مشاهده نباشد. مقاومت به معنای صدمه ندیدن اطلاعات پنهان شده در تصویر نهان نگاری شده و همچنین قابل بازیابی بودن آن پس از اعمال انواع حملات علیه تصویر است. این حمله‌ها شامل حملات ساده مثل چرخاندن، بریدن، تغییر سایز و ... و حملات افزودن نویز مانند نویز نمک-فلفل، نویز گوسی، نویز میانه و ... و همچنین حملات پیچیده حوزه فرکانس مثل فشرده سازی JPEG می‌باشد. معیار ظرفیت مشخص می‌کند اندازه تصویر نماد نسبت به اندازه تصویر پوشانه حداکثر چقدر می‌تواند باشد، به عبارت دیگر، در یک تصویر پوشانه با اندازه‌ی مشخص چند بیت داده می‌توان ذخیره کرد. واضح است که این ملزومات به یکدیگر مرتبط هستند و الگوریتم‌های نهان نگاری سعی در رعایت این ملزومات دارند. هر الگوریتم نهان نگاری دو مرحله دارد، درج سیگنال واترمارک و استخراج آن. برای درج سیگنال واترمارک می‌توان از حوزه مکان یا حوزه فرکانس استفاده کرد. استخراج آن نیز می‌تواند با استفاده از همبستگی با واترمارک اصلی (روش‌های آشکار و نیمه آشکار) یا مستقل از آن (روش‌های کور) صورت گیرد. واضح است انتخاب روش درج و نحوه استخراج واترمارک به هم وابسته است. یکی از راه‌های درج سیگنال واترمارک در حوزه مکان، اضافه کردن یک رشته‌ی شبه نویز معرف سیگنال واترمارک به سطح روشنایی پیکسل‌های تصویر پوشانه مورد نظر است.

امروزه به دلیل رونق استفاده از اینترنت و شبکه‌های اجتماعی، استفاده از داده دیجیتال چندرسانه‌ای رواج پیدا کرده است. گرچه داده دیجیتال مزایای زیادی نسبت به داده آنالوگ دارد ولی ارائه دهندگان سرویس‌های چند رسانه‌ای نگران پخش و انتشار بی رویه ناشی از کپی غیر مجاز داده‌های دیجیتال هستند که برخلاف داده آنالوگ کیفیتی مشابه داده اصلی دارند. برای محافظت از محصولات دیجیتال در مقابل کپی‌های غیرمجاز و حفظ حق نشر آثار، روش‌های زیادی به وجود آمده است. نهان نگاری یکی از رایج‌ترین روش‌های ذخیره سازی اطلاعاتی از قبیل امضا یا نماد صاحب اثر در محصول دیجیتال است. تاکنون روش‌های متفاوتی برای نهان نگاری معرفی شده است که کیفیت این روش‌ها با سه مشخصه‌ی (۱) شفافیت از نظر درک سیستم بینایی، (۲) مقاومت و (۳) ظرفیت، سنجیده و مقایسه می‌شود. شفافیت یعنی نهان نگاری تا حد ممکن به کیفیت تصویر پوشانه صدمه نزند. البته بدیهی است که نهان نگاری ذاتاً با ایجاد تغییرات در تصویر پوشانه، تصویر نماد را در آن ذخیره می‌کند. پس نمی‌توان انتظار داشت تصویر نهان نگاری شده با تصویر پوشانه تفاوتی نداشته باشد، بلکه در اینجا شفافیت به معنای به حداقل رساندن این تغییرات است تا به کیفیت تصویر لطمه نزند و تا حد

بخش کلی تبدیل میکند که ضرایب LL ضرایب باند پایین بوده و حاوی اطلاعات مهمی هستند که تغییرات در آن ها می تواند کیفیت تصویر را تحت تاثیر قرار دهد. ضرایب HH ضرایب باند پایین هستند که تغییرات آن ها کیفیت تصویر را خراب نمیکند اما این ضرایب مقاومت چندانی نسبت به حملات فرکانسی ندارند. [۲]

LL	HL
LH	HH

شکل ۱: بخش بندی تصویر توسط تبدیل DWT

### • تبدیل DHT

بر خلاف تبدیلهای دیگر که شامل محاسبات پیچیده هستند، این تبدیل محاسبات به مراتب آسان تر دارد. این تبدیل بر مبنای تابع والش است و فقط شامل عملیات باینری و ساده است. این ویژگی ها باعث می شود این تبدیل برای نهان نگاری مناسب باشد. برای انجام این تبدیل روی یک عکس  $2^n \times 2^n$  از یک ماتریس  $2^n \times 2^n$  استفاده می شود که آن را  $H_n$  می نامند. این ماتریس فقط شامل درایه های ۱ و -۱ است.  $H_n$  ها از طریق معادله ۲ و با ضرب کرانکر بدست می آیند:

$$H_n = H_{n-1} \otimes H_1, H_1 = 1 \quad (2)$$

تبدیل هادامارد هر ماتریس دلخواه U با استفاده از رابطه ۳ محاسبه می شود.

$$V = \frac{H_n \times U \times H_n}{N} \quad (3)$$

قانون شنون اثبات کرده است که این تبدیل نسبت به سایر تبدیلات تغییرات کمتری در اطلاعات تصویر اعمال می کند.

### • تبدیل CT

تبدیل کانتورلت، تبدیل دوبعدی جهت دار جدایی ناپذیری است که برای توصیف منحنی ها و جزئیات ظریف در تصاویر به کار می رود. بسط کانتورلت از توابع پایه ای که در جهات مختلف با اشکال و مقیاس های مختلف گرایش دارند تشکیل شده است. با این مجموعه از توابع پایه ای غنی، تبدیل کانتورلت به طور کارایی کانتورهای هموار که اجزای اصلی و مهم در تصاویر طبیعی می باشند را توصیف می کند. بر خلاف دیگر تبدیلهای که ابتدا در یک حوزه پیوسته ساخته می شوند و سپس برای نمونه برداری داده گسسته می شوند، تبدیل کانتورلت با کمک فیلتر بانک های جهت دار از یک حوزه ی گسسته شروع شده و سپس از طریق یک چارچوب تحلیلی مالتی رزولوشن به یک حوزه

امنیت این روش به کلید به کار رفته در تولید این رشته شبه تصادفی بستگی دارد و استخراج آن با توجه به میزان همبستگی بین تصویر نهان نگاری شده و سیگنال واترمارک میتواند با استفاده از روش های کور یا آشکار صورت گیرد. در حوزه فرکانس، تبدیلات متعددی از قبیل مدولاسیون دامنه یا فاز (DFT)، گسسته کسینوسی (DCT)، موجک (DWT)، هادامارد (DHT)، کانتورلت (CT) و ... وجود دارند. نهان نگاری به روش طیف گسترده (حوزه فرکانس) مقاومت زیادی در مقابل حملات مختلف ایجاد می کند همچنین ظرفیت بالایی برای پنهان کردن داده های ثانویه دارد ولی نهان نگاری حوزه مکان نسبت به حملات مختلفی که روی تصویر صورت می گیرد نظیر فشرده سازی و فیلترینگ، مقاومت چندانی ندارد در عین حال برخلاف روش های نهان نگاری حوزه فرکانس، ظرفیت بالایی هم برای پنهان کردن داده ندارد [۱].

## ۲ پیشینه نظری

این بخش به بررسی مفاهیم پایه در نهان نگاری می پردازد. زیربخش اول در مورد انواع تبدیلات فرکانسی است که برای نهان نگاری استفاده می شود و زیربخش دوم در مورد معیار های سنجش کیفیت تصویر نهان نگاری شده است.

### ۱-۲ تبدیلات متداول

#### • تبدیل DCT

این تبدیل کاربرد فراوانی در موضوعات مختلف پردازش تصویر و به خصوص نهان نگاری دارد. این تبدیل همان تبدیل DFT است که فقط ضرایب حقیقی یعنی ضرایب کسینوسی در آن بدست می آیند. ضرایب DCT به شکل زیر محاسبه میشوند:

$$F[u, v] = \frac{1}{N^2} \sum_{m=1}^{N-1} \sum_{n=1}^{N-1} f[m, n] \cos\left((2m+1)\frac{u\pi}{2N}\right) \cos\left((2n+1)\frac{v\pi}{2N}\right) \quad (1)$$

رابطه ۱ ضرایب DCT را برای یک بلوک N در N بدست می آورد که در آن ضرایب DCT و  $f[m, n]$  مقدار پیکسل های آن بلوک هستند. همانطور که مشخص است عملاً  $F[0, 0]$  میانگین پیکسل های تصویر است و به آن مقدار DC گفته میشود. به طور کلی در یک بلوک ضرایب بالا سمت راست یعنی ضرایب فرکانس پایین حاوی اطلاعات مهمی از تصویر هستند و دستکاری آن ها کاملاً میتواند تصویر را خراب کند. از طرفی ضرایب پایین سمت چپ یعنی ضرایب فرکانس بالا کم ارزش ترین اطلاعات را دارند و دستکاری آن ها مشکلی در کیفیت تصویر به وجود نمی آورد در عوض این ضرایب همان ضرایبی هستند که در حمله ی JPEG صفر می شوند و در نتیجه مقاومت پایینی دارند.

#### • تبدیل DWT

این تبدیل با استفاده از گذر دادن تصویر از یک فیلتر پایین گذر و یک فیلتر بالا گذر به وجود می آید و تصویر را مثل شکل ۱ به چهار

$$PSNR = 10 \times \log_{10} \left( \frac{MAX_I^2}{MSE} \right)$$

$$= 20 \times \log_{10} (MAX_I) - 10 \times \log_{10} (MSE) \quad (5)$$

#### • Bit Error Rate : BER

این معیار نسبت تعداد بیت‌های متفاوت از اصل را به تعداد کل بیت‌ها می‌گیرد. مثلاً دو رشته ی  $x = 0101010101$  و  $\hat{x} = 0101110101$  فقط در یک بیت اختلاف دارند پس  $BER = \frac{1}{10}$  است.

#### • Normalized Cross Correlation : NCC

این معیار برای اندازه‌گیری میزان شباهت دو سیگنال (چه گسسته و چه پیوسته) تعریف شده است که برابر کانولوشن سیگنال دوم در conjugate complex سیگنال اول است.

#### • Normalized Correlation : NC

اگر پیغام اولیه ای که می‌خواهیم در تصویر پوشانه پنهان کنیم و  $\hat{W}$  پیغام استخراج شده از تصویر نهان نگاری شده باشد و  $M$  طول پیغام مذکور باشد آنگاه NC طبق رابطه ۶ به دست می‌آید.

$$NC = 1 - \frac{\sum_{i=1}^M W_i - \hat{W}_i}{M} \quad (6)$$

#### • Structural SIMilarity : SSIM

برای محاسبه SSIM از رابطه ۷ استفاده می‌شود.

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \quad (7)$$

که در آن :

$x, y$  : تصویر پوشانه و تصویر نهان نگاری شده به ابعاد  $N \times N$

$\mu_x$  : میانگین  $x$

$\mu_y$  : میانگین  $y$

$\sigma_x^2$  : واریانس  $x$

$\sigma_y^2$  : واریانس  $y$

$\sigma_{xy}$  : کواریانس  $x$  و  $y$

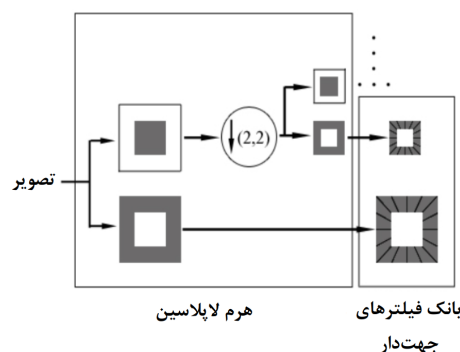
$c_1 = (k_1 L)^2, c_2 = (k_2 L)^2$  : دو متغیر برای تثبیت تقسیم با

مخرج ضعیف.

$L$  : دامنه دینامیکی مقادیر پیکسل و به صورت پیش فرض

$k_1 = 0.01, k_2 = 0.03$  است.

پیوسته همگرا می‌شود. این تبدیل نسبت به تغییر مقیاس، تغییر جهت و تغییر مکان تصویر انعطاف پذیر است. همانطور که در شکل ۲ می‌بینید، تبدیل کانتورلت یک ساختار درختی کارآمد را پیاده‌سازی می‌کند، که در واقع یک ترکیب تکرار شونده از هرم لاپلاسن (LP)، برای استخراج نقاط ناپیوستگی، و یک فیلتربانک جهت دار (DFB) می‌باشد. از آنجایی که DFB طراحی شده تا ویژگی‌های جهت دار عکس ورودی را در فرکانس‌های بالا استخراج کند و در استخراج محتویات پایین ضعیف است، آن را با LP ترکیب کردند، تا قبل از اعمال DFB در هر مرحله، فرکانس‌های پایین را از تصویر جدا کند.



شکل ۲: بانک فیلتر دوتایی تبدیل کانتور (برگرفته از [۳])

به طور خلاصه، در تبدیل کانتورلت در هر مرحله به وسیله تبدیل لاپلاس فرکانس‌های پایین عکس جدا شده و به مرحله بعد فرستاده می‌شوند، و لبه‌های باقیمانده عکس به وسیله فیلتربانک استخراج می‌شوند. در هر مرحله ضربایی از عکس استخراج می‌شود که از توابعی از این ضرایب مانند میانگین و انحراف معیار و غیره می‌توان به عنوان ویژگی توصیف‌گر بخشی که تبدیل روی آن انجام شده استفاده کرد. [۳]

## ۲-۲ معیارهای سنجش کیفیت

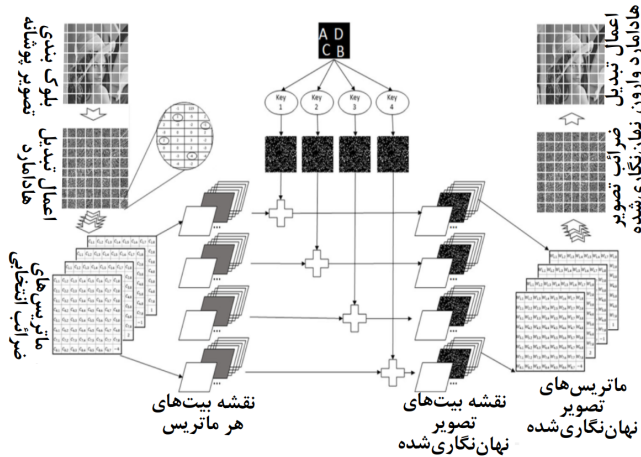
#### • Mean Square Error : MSE

اگر تصور پوشانه را با  $I$  و تصویر نهان نگاری شده را با  $K$  نشان دهیم و ابعاد تصویرها  $m \times n$  باشد آنگاه MSE این دو تصویر طبق رابطه ۴ محاسبه می‌شود.

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} (I(i, j) - K(i, j))^2 \quad (4)$$

#### • Peak Signal-to-Noise Ratio : PSNR

برای محاسبه PSNR هم باید از رابطه ۵ استفاده کرد.



شکل ۳: نمودار جعبه ای الگوریتم ارائه شده در [۵]. (برگرفته از [۵])

این الگوریتم برای درج یک لوگوی سیاه-سفید در یک تصویر خاکستری ارائه شده که از تبدیل هادامارد برای این منظور استفاده می‌کند. همانطور که در شکل ۳ هم پیداست، این روش، ابتدا تصویر پوشانه خاکستری را به منظور بهبود شفافیت تصویر نهان نگاری شده، به بلوک‌هایی غیر همپوشان تقسیم می‌کند، سپس از هر بلوک تبدیل هادامارد می‌گیرد و بیت‌های لوگو را در یکی از نقشه-بیت‌های ضرایب به دست آمده از تبدیل هادامارد، درج می‌کند. همچنین به منظور ارتقای امنیت و بهبود شفافیت، به جای استفاده مستقیم از بیت‌های لوگو از بیت‌های رمزنگاری شده آن برای تعبیه کردن در پوشانه استفاده می‌کند. به علاوه لوگو را در ضرایب دنباله متوسط که معادل فرکانس متوسط در حوزه تبدیلات DCT و DFT است، قرار می‌دهد تا نسبت به حملات فشرده سازی JPEG مقاومت بیشتری ایجاد کند و همزمان به شفافیت تصویر نهان نگاری شده لطمه نزنند. در انتها نیز با تبدیل وارون به تصویر نهان نگاری شده‌ی نهایی می‌رسد. برای استخراج واترمارک از تصویر نهان نگاری شده، تقریباً عکس همان مسیری که برای درج اطلاعات در پوشانه طی شده را می‌رود و در آخر با استفاده از مکانیزم رأی گیری، از بین افزونگی‌های موجود بیت‌های مناسب برای بازسازی پیغام مندرج در پوشانه را استخراج می‌کند. نویسندگان مقاله [۵] برای یافتن مناسب ترین نقشه-بیت تصویر پوشانه برای درج لوگو، معیار  $\rho = MSSIM \times NCC$  را تعریف می‌کنند که به خوبی تهاثر بین شفافیت و مقاومت را بیان می‌کند به این صورت که MSSIM تصویر پوشانه و تصویر نهان نگاری شده، عملکرد الگوریتم را از لحاظ شفافیت می‌سنجند و NCC لوگوی استخراج شده و لوگوی اولیه، برای محاسبه مقاومت مناسب است. در نهایت، نویسندگان مقاله [۵] با طراحی چندین آزمایش تجربی، به این نتیجه رسیدند که نقشه-بیت پنجم مناسب ترین نقشه-بیت از لحاظ رعایت شفافیت و مقاومت برای نهان نگاری با این الگوریتم است. در آخر، بعد از سنجش الگوریتم از جنبه های شفافیت و مقاومت طی آزمایشات متعدد، نتیجه حاصله، اثبات کننده ی عملکرد بسیار خوب این روش نسبت به پیشرفته ترین الگوریتم

روش استفاده شده برای نهان نگاری دیجیتال در این مقاله [۴]، روش ضربی در دامنه کانتورلت با استفاده از توزیع گاوسی معکوس نرمال است. در بین روش های نهان نگاری دیجیتال، روش های ضربی هم مقاومت بیشتری دارند و هم نامحسوس بودن بیشتری را نسبت به روش های جمعی، به وجود می آورند. امروزه نشان داده شده است که تکنیک های نهان نگاری دامنه ی کانتورلت، نسبت به سایر روش های نهان نگاری ضربی مقاومت بیشتری دارند. در ابتدا، تبدیل کانتورلت روی تصویر اعمال می شود و ویژگی های مهم عکس را به شکل ضرایبی به دست می آورد. برای مثال فرض کنیم  $x = \{x_1, \dots, x_N\}$  مجموعه ضرایب کانتورلت به دست آمده باشند. مجموعه  $w = \{w_1, \dots, w_N\}$  دنباله ای شبه تصادفی که مقادیرش بین -۱ تا ۱ است. با استفاده از این دو مجموعه، مجموعه ضرایب واترمارک با استفاده از رابطه ۸ محاسبه می شود.

$$y_i = (1 + \text{sign}(x_i) \xi w_i) x_i, \quad i = 1, \dots, N \quad (8)$$

که در آن  $\xi$  عامل وزنی مثبت است که برای ایجاد تهاثر بین مقاومت و شفافیت واترمارک استفاده می شود. برای استخراج واترمارک هم از رابطه ۹ استفاده می شود.

$$(9) \quad \sum_{n=1}^N \ln \frac{\sqrt{\delta^2 + \left(\frac{y_i}{1 - \text{sign}(y_i)\xi}\right)^2} K_1 \left( \alpha \sqrt{\delta^2 + \left(\frac{y_i}{1 + \text{sign}(y_i)\xi}\right)^2} \right)}{\sqrt{\delta^2 + \left(\frac{y_i}{1 + \text{sign}(y_i)\xi}\right)^2} K_1 \left( \alpha \sqrt{\delta^2 + \left(\frac{y_i}{1 - \text{sign}(y_i)\xi}\right)^2} \right)} > 1 - T$$

$$< 0$$

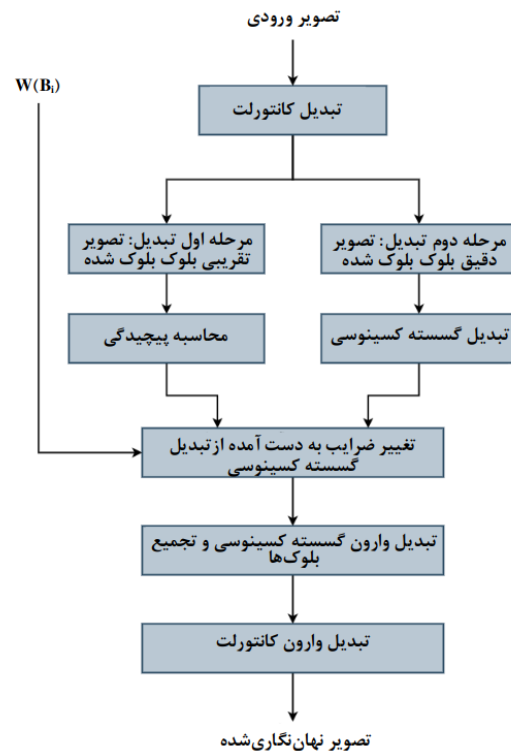
دو نوع فیلتر کانتورلت متفاوت در نظر گرفته شده: فیلترهای lad-der مثل pkva و فیلترهای ۹-۷ bi-orthogonal. با استفاده از این فیلترها مقادیر PSNR و BER اندازه گیری می شود و مشاهده می شود که فیلترهای ۹-۷ bi-orthogonal نسبت به بقیه PSNR بیشتر و BER کمتری ایجاد می کنند. برای ایجاد شرایط عادلانه در مقایسه کارایی رمزگشای پیشنهاد شده، PSNR و طول پیام ها برابر در نظر گرفته شده است. طبق نتایج، این روش، BER کمتری دارد در نتیجه این روش نسبت به سایر روش های موجود کارایی بهتری داشته و شفافیت و مقاومت بیشتری ایجاد می کند.

الگوریتم پیشنهادی در [۵]، برای نهان نگاری دیجیتال تصویر به روش طیف گسترده در حوزه DHT است که در شکل ۳ نشان داده شده است.

های وقت، در حفظ شفافیت می‌باشد. همچنین از جنبه مقاومت، علیرغم عملکرد ضعیف نسبت به حملاتی نظیر تغییر سطح روشنایی و تصحیح گاما، در مجموع می‌توان بیان کرد که این الگوریتم، کارکرد قابل قبولی داشته است.

### ۳-۳ روش

الگوریتم پیشنهادی در [۶]، برای نهان نگاری دیجیتال تصویر به روش طیف گسترده در حوزه CT و DCT است که در شکل ۴ نشان داده شده است.



شکل ۴: نمودار جعبه ای الگوریتم ارائه شده در [۶]. منظور از  $W(B_i)$  یک بیت از تصویر لوگو است. (برگرفته از [۶])

در این الگوریتم از دو مرحله تبدیل کانتورلت روی تصویر پوشانه استفاده می‌شود. در مرحله اول، خروجی یک تصویر تقریبی خواهد بود که در ادامه آن را به بلوک‌هایی تقسیم می‌کند. در همین حال مرحله دوم تبدیل کانتورلت را اعمال می‌کند که خروجی، تصویری همراه با جزئیات است که مشابه قبل آن را نیز به بلوک‌هایی تقسیم می‌کند به صورتی که بین بلوک‌های تصویر خروجی مرحله اول و دوم تبدیل کانتورلت، یک تناظر یک به یک برقرار باشد. این الگوریتم، اطلاعات ثانویه را در بلوک‌های تصویر همراه با جزئیات که خروجی مرحله دوم تبدیل کانتورلت است، پنهان می‌کند و به منظور حفظ مقاومت تصویر نهان نگاری شده، تکنیک‌هایی به کار می‌برد از جمله اینکه (۱) بیت‌های پیام مورد نظر را همراه با افزونگی در تصویر پوشانه مخفی می‌کند و (۲) اطلاعات را در ضرایب تبدیل DCT بلوک‌های مختلف پوشانه درج می‌کند. روش این الگوریتم برای کنترل شدت درج اطلاعات در

بلوک‌های مختلف پوشانه، استفاده از معیاری به نام پیچیدگی است. این معیار بر اساس میزان آنتروپی و تجمع لبه‌ها در بلوک‌های تصویر، میزان پیچیدگی هر بلوک را به صورت عددی مشخص می‌کند. پس طبق این الگوریتم پیشنهادی، در پیچیده ترین بلوک‌ها، شدیدترین میزان درج اطلاعات را داریم و هرچه پیچیدگی بلوک کمتر می‌شود، میزان اطلاعاتی که در آن بلوک درج می‌شود نیز کمتر می‌شود. بعد از انتخاب بلوک‌های مناسب، از هر کدام تبدیل گسسته کسینوسی گرفته می‌شود و اطلاعات در ضرایب به دست آمده پنهان می‌شوند. سپس با تبدیل وارون DCT و همچنین تبدیل وارون CT به تصویر نهان نگاری شده‌ی نهایی می‌رسد. برای استخراج واترمارک از تصویر نهان نگاری شده، تقریباً عکس همان عملیاتی که برای درج اطلاعات در پوشانه انجام شده است را بکار می‌برند و در آخر با استفاده از مکانیزم رأی گیری، از بین افزونگی‌های موجود، بیت‌های مناسب برای بازسازی پیام مندرج در پوشانه را استخراج می‌کند. نویسندگان مقاله [۶] برای مقایسه الگوریتم پیشنهادیشان با پیشرفته ترین الگوریتم‌های وقت، از Matlab R2013a استفاده کرده اند و الگوریتم را روی یک تصویر خاکستری  $512 \times 512$  به عنوان پوشانه و 128 بیت داده ثانویه برای درج در پوشانه امتحان کرده اند. با بررسی نتایج حاصل از آزمایشات متعددشان به این جمع بندی رسیده اند که (۱) الگوریتم معرفی شده در این مقاله [۶] تحت یک PSNR ثابت، SSIM خوبی نشان داده به این معنا که از نظر ارضای مشخصه‌ی شفافیت، عملکرد بسیار خوبی داشته است و (۲) این الگوریتم [۶] در مقابل حملات مختلف از قبیل برش، فشرده سازی JPEG، افزودن نویز گوسی و ... عملکرد خوبی داشته و به لحاظ مقاومت، نسبت به الگوریتم‌های مذکور، خیلی بهتر بوده است.

### ۴-۳ روش

مقاله [۲] روشی را مطرح می‌کند که در آن نهان نگاری فقط در مناطق خاصی از تصویر انجام شود که در آن سه ویژگی (۱) برجستگی کم (۲) شدت زیاد (۳) تجمع لبه وجود داشته باشد چون چشم انسان نسبت به این مکان‌ها حساسیت کمتری داشته و متوجه تغییرات رخ داده در این بخش‌ها نمی‌شود. پس از محاسبه این مشخصه‌ها در تصویر از یک سیستم فازی استفاده می‌کند تا بتواند این سه مشخصه را در کنار هم قرار داده و یک درجه عضویت به هر قسمت از تصویر اختصاص دهد که هرچه این درجه عضویت به یک نزدیکتر باشد یعنی مکان مناسب‌تری برای نهان نگاری است. مرحله ی نهان نگاری به این صورت انجام می‌شود که ابتدا دو مرحله از تصویر پوشانه DWT گرفته می‌شود و باند میانی آن برای نهان نگاری انتخاب می‌شود. پس از آن باند میانی به بلوک‌های  $8 \times 8$  تقسیم و از بلوک‌ها DCT گرفته می‌شود و سپس تصویر نماد به صورت تکرار شونده برای افزایش مقاومت، داخل ضرایب DCT و با استفاده از درجه عضویت محاسبه شده به عنوان strength factor نهان نگاری می‌شود. برای استخراج تصویر پس از استخراج باند میانی پس از دوبار تبدیل DWT و DCT گرفتن از آن، عملیات voting برای استخراج بیت‌های تصویر نماد انجام می‌شود. برای بررسی کارایی



## ۴ نتیجه گیری

در این مقاله ۵ روش برای نهان نگاری مطرح شد که هر کدام به نحوی سعی در افزایش سه مشخصه ی کیفیتی نهان نگاری داشتند. جنبه ی مشترک تمام این الگوریتم ها استفاده از حوزه ی فرکانس به جای حوزه ی مکان برای نهان نگاری و همچنین استخراج به صورت کور است. آن طور که به نظر می رسد استفاده از تبدیلات متوالی تاثیر مستقیم در کیفیت هرچه بیشتر تصویر نهان نگاری شده و مقاومت آن نسبت به حملات مختلف دارد. همچنین به طور کلی ذخیره سازی تصویر نماد به صورت تکراری و استفاده از تمام ظرفیت الگوریتم، احتمال خطا در مرحله ی استخراج را به شدت کاهش میدهد. یکی از متداول ترین روش های اخیر نیز استفاده از پیش پردازش هایی روی تصویر پوشانه برای افزایش شفافیت تصویر نهان نگاری شده است. تمام مقالات [۲، ۴، ۵، ۶، ۷] پس از مطرح کردن روش خود به بررسی عملکرد آن با معیار های مختلف سنجش کیفیت پرداخته اند و در همه ی موارد به نتایج بهتری نسبت به مقالات هم عصر خود رسیده اند.

## مراجع

- [1] A. Rashid, "Digital watermarking applications and techniques: A brief review," *International Journal of Computer Applications Technology and Research*, Jan. 2016.
- [2] S. R. S. N. K. S. S. K. N. S. S. Maedeh Jamali, Shima Rafiei, "Adaptive image watermarking using human perception based fuzzy inference system," *Journal of Intelligent and Fuzzy Systems*, 2018.
- [3] M. N. D. Arthur L. da Cunha, Jianping Zhou, "The nonsub-sampled contourlet transform: Theory, design, and applications," *IEEE TRANSACTIONS ON IMAGE PROCESSING*, Oct. 2006.
- [4] M. O. A. H. Sadreazami and M. N. S. Swamy, "Multiplicative watermark decoder in contourlet domain using the normal inverse gaussian distribution," *IEEE Transactions on Multimedia*, 2015.
- [5] S. M. R. S. N. K. M. E. S. S. K. N. Elham Etemad, Shadrokh Samavi, "Robust image watermarking scheme using bit-plane of hadamard coefficients," *Multimed Tools Appl*, Jan. 2017.
- [6] N. K. S. S. H. R. Fazlali, S. Samavi, "Adaptive blind image watermarking using edge pixel concentration," *Multimed Tools Appl*, Jan. 2016.
- [7] S. S. N. K. S. S. Mohrekesh M., Shekoofeh Azizi, "Hierarchical watermarking framework based on analysis of local complexity variations," 2018.

روش پیشنهادی از چندین تصویر استاندارد به عنوان پوشانه استفاده شده و معیار سنجش شفافیت را PSNR و MSSIM در نظر گرفته که در این معیار الگوریتم پیشنهادی [۲] بهتر از الگوریتم های پیشرفته ترین الگوریتم های وقت عمل کرده است. برای سنجش مقاومت از معیار NC بعد از حمله های بریدن و فیلتر گوسی در اندازه های مختلف استفاده شده که در اکثر موارد توانسته به مقدار یک برسد (تصویر نماد بعد از بازیابی مشابه اصل نماد است). برای مقایسه بین این الگوریتم و الگوریتم های state of art از نظر مقاومت نسبت به حملات JPEG، نویز نمک و فلفل، بریدن، فیلتر میانگین، فیلتر گوسی و نویز سفید از معیار BER استفاده کرده که در اکثر موارد نتیجه بهتری گرفته است. البته یکی از معایب این روش مصرف حافظه و زمان زیاد در بخش استخراج ویژگی هاست.

## ۳-۵ روش ۵

در این مقاله [۷] هم فریمورکی ارائه شده که با توجه به مشخصات محلی تصویر و به صورت سلسله مراتبی به هر بخش تصویر یک strength factor اختصاص می دهد. برای این کار ابتدا تصویر پوشانه با یک دیتاست از تصاویری که به طور تجربی  $\alpha$  مناسب آن ها تعیین شده مقایسه میشود و یک  $\alpha_i$  به آن اختصاص داده میشود. سپس پیچیدگی هر پیکسل به صورت جمع اختلاف آن با پیکسل های همسایگی ۸ محاسبه میشود و پیچیدگی هر بلوک برابر میانگین پیچیدگی پیکسل های آن است. سپس طبق پیچیدگی هر بلوک به آن یک  $a$  اختصاصی در بازه ی  $\alpha - m$  تا  $\alpha + m$  داده می شود که این آستانه برای جلوگیری از اختلاف بیش از حد بلوک ها و در نتیجه پدیده ی blockiness شدن تصویر است. این فریمورک برای هر الگوریتم نهان نگاری میتواند استفاده شود ولی نویسندگان مقاله [۷] به طور خاص پیشنهاد میکنند که برای نهان نگاری ابتدا از تصویر تبدیل CT گرفته شود و سپس از آن DCT گرفته شود و بیت های نماد به صورت تکرار شونده با strength factor محاسبه شده و در ضرایب DCT از باند approximate تبدیل CT نهان نگاری شوند. برای استخراج نیز پس از محاسبه ی CT و DCT عملیات voting انجام شود. با اندازه گیری PSNR مشخص شده این الگوریتم از نظر شفافیت بهتر از الگوریتم های non-adaptive عمل میکند. همچنین با اندازه گیری NC مشخص شده از نظر مقاومت به حمله های بریدن، JPEG، نویز نمک و فلفل و نویز گوسی عملکرد بهتری نسبت به الگوریتم های non-adaptive دارد. همچنین به طور میانگین پس از حملات بریدن، تغییر سایز، نویز گوسی، نمک و فلفل، JPEG، فیلتر میانگین، Histogram Equalization و Gamma-Correction مقدار NC بیشتر و BER کمتر نسبت به سایر روش های non-adaptive داشته است. در آخر، الگوریتم پیشنهادی [۷] نسبت به روش های state of art گاهی بهتر و گاهی ضعیف تر بوده است اما در مجموع میتوان گفت عملکردی مشابه یا بهتر داشته است.