

نهان نگاری دیجیتال تصویر به روش طیف گسترده در حوزه تبدیل گسسته کسینوسی

لیلی احسان*، فاطمه ادیسی*

احسان اله کبیر[□]، سعید نادر اصفهانی^{□□}

*دانشکده صدا و سیما، گروه فنی l_ehsan@hotmail.com, fateme_edrisi@yahoo.com

[□]دانشگاه تربیت مدرس، بخش مهندسی برق kabir@modares.ac.ir و ^{□□}دانشگاه تهران، گروه مهندسی برق nader@ut.ac.ir

چکیده

در این مقاله الگوریتمی برای درج سیگنال واترمارک در یک تصویر خاکستری، به روش طیف گسترده در حوزه تبدیل گسسته کسینوسی ارائه می شود. تصویر واترمارک شده در برابر حملات عمدی و غیر عمدی، به ویژه در برابر فشردن سازی JPEG مقاوم است. برای گسترش سیگنال واترمارک، از رشته های گلد ۱۰۲۳ بیتی استفاده می شود. تبدیل گسسته کسینوسی بر روی بلوکهای ۸×۸ تصویر انجام می شود. در هر بلوک، مهمترین ضریب AC در جدول کوانتیزه JPEG برای درج هر ضریبی از سیگنال طیف گسترده واترمارک، انتخاب شده است. مقاومت تصویر نهان نگاری شده با ضریب بهره های مختلف، در برابر حملات عمدی و غیر عمدی، برای چند تصویر نمونه که خواص فرکانسی متفاوتی دارند، بررسی و مقایسه شده است.

کلمات کلیدی: نهان نگاری دیجیتال، واترمارک، تبدیل گسسته کسینوسی، طیف گسترده

۱. مقدمه

در دهه اخیر، به علت اتصال تعداد بیشماری از کامپیوترهای شخصی به شبکه جهانی اینترنت، انفجاری در توزیع و استفاده آسان از داده دیجیتال چند رسانه ای به وقوع پیوسته است. گرچه داده دیجیتال مزایای بسیاری نسبت به داده آنالوگ دارد، ولی ارائه دهندگان سرویس های چند رسانه ای نگران پخش و انتشار بی رویه ناشی از کپی غیر مجاز داده های دیجیتال هستند، که بر خلاف حالت آنالوگ کیفیتی مشابه داده اصلی دارند.

برای حفاظت از محصولات دیجیتال چند رسانه ای در برابر کپی های غیر مجاز^(۱) و حفظ حق انتشار^(۲) برای داده های صوتی، تصویری و ویدئویی از دو تکنیک رمز نگاری^(۳) و نهان نگاری^(۴) استفاده می شود. تکنیک های رمز نگاری برای حفاظت داده دیجیتال به هنگام انتقال از فرستنده به گیرنده به کار می روند. داده ها در فرستنده رمز می شوند و پس از دریافت در گیرنده رمز گشایی می شوند. از این پس دیگر هیچگونه حفاظتی از داده صورت نمی گیرد. ولی در تکنیک های نهان نگاری، یک سیگنال پنهانی به نام واترمارک، مستقیماً در داخل داده حک^(۵) می شود و همواره در آن باقی می ماند. برای استفاده از داده نهان نگاری شده، نیازی به برداشتن سیگنال واترمارک نیست زیرا این سیگنال طوری در داده میزبان درج می شود که هیچ تأثیر نامطلوبی بر داده اصلی نمی گذارد. به عنوان مثال در نهان نگاری داده در تصویر، چشم انسان نباید تفاوت بین تصویر اصلی و تصویر واترمارک شده را حس کند. در صورت هر گونه استفاده غیر مجاز از تصویر واترمارک شده، مانند کپی غیر مجاز از آن و یا هر گونه تحریف و تغییر تصویر توسط افراد غیر مجاز، صاحب اصلی داده می تواند با استخراج سیگنال واترمارک، که تنها توسط او امکان پذیر است، مالکیت خود را به اثبات برساند و یا محل تغییرات صورت گرفته بر روی تصویر را مشخص کند.

۱-۱. اهداف و ملزومات نهان نگاری

نهان نگاری کاربردهای مختلفی دارد که برخی از آنها عبارتند از: الف) اثبات حق مالکیت^(۶) و یا حفظ حق نشر (ب) نهان کردن داده های مختلف با امکان رد گیری^(۷) (ج) کنترل عمل کپی برداری (د) نظارت بر پخش^(۸) (ه) تصدیق صحت داده^(۹) (و) برچسب زدن به تصاویر^(۱۰) (ز) ارتباطات مخفیانه و پنهان سازی داده^(۱۱).

(۱) Copy protection (۲) copyright protection (۳) encryption (۴) watermarking (۵) embedding (۶) owner identification (۷) transactional watermarks (fingerprinting) (۸) Broadcast (۹) data (۱۰) Indexing (۱۱) Data Authentication Monitoring hiding

گرچه هر کاربردی از نهان نگاری تصویر نیازهای خاص خود را دارد ، با این همه تمام روش های نهان نگاری باید ملزومات مشترکی را رعایت کنند که عبارتند از :

۱) شفافیت از نظر درک سیستم بینایی ، ۲) امنیت ، ۳) رعایت ظرفیت سیگنال و اتر مارک .

واضح است که این ملزومات به یکدیگر مربوطند. آلوگوریتم های نهان نگاری ، به منظور درج اطلاعات سیگنال پیام در داخل داده میزبان، تغییرات کوچکی را بر اساس سیگنال پیام در داده میزبان ، ایجاد می کنند ، به نحوی که با چشم انسان قابل مشاهده نباشد.

۲-۱. پیشینه کار

هر آلوگوریتم نهان نگاری ۲ مرحله دارد : درج سیگنال و اتر مارک و استخراج آن . برای درج سیگنال و اتر مارک می توان از حوزه مکان یا حوزه فرکانس استفاده کرد . استخراج آن می تواند با استفاده از همبستگی با و اتر مارک اصلی و یا مستقل از آن صورت گیرد . واضح است انتخاب روش درج و نحوه استخراج و اتر مارک به هم وابسته اند .

یکی از راهها برای افزودن یک سیگنال و اتر مارک در حوزه مکان ، اضافه کردن یک رشته شبه نویز معرف سیگنال و اتر مارک به مقادیر روشنایی پیکسل های تصویر مورد نظر است . امنیت این روش به کلید به کار رفته در تولید رشته شبه تصادفی بستگی دارد و استخراج آن با استفاده از مقدار همبستگی بین تصویر و اتر مارک شده و سیگنال اصلی و اتر مارک صورت می گیرد [۱ و ۲] . برای درج تعداد زیادی بیت در تصویر میزبان ، می توان تصویر اصلی را به تعدادی زیر تصویر تقسیم کرد و هر بیت را به یکی از این زیر تصویر ها اضافه کرد . از دیگر روش های نهان نگاری در حوزه مکان می توان از روش LSB^۱ نام برد [۱] .

در حوزه فرکانس ، بسیاری از روشها ، از مدولاسیون دامنه یا فاز DFT استفاده می کنند [۲] . حوزه متداول دیگر برای درج سیگنال و اتر مارک ، حوزه تبدیل گسسته کسینوسی است [۳] . با استفاده از تبدیل گسسته کسینوسی می توان یک تصویر را به باند های شبه فرکانسی تقسیم کرد و و اتر مارک را در مناسبترین باند درج کرد . مقایسه مناسبی بین حوزه های مختلف تبدیل برای درج سیگنال و اتر مارک در حضور فشرده سازی JPEG در مقاله [۴] صورت گرفته است . تبدیلات مقایسه شده شامل تبدیل گسسته کسینوسی ، موجک ، هادامارد ، سینوسی گسسته و KLT هستند . روش های دیگر نهان نگاری بر مبنای فشرده سازی فرکانس پیشنهاد شده اند [۵] . در این روش ها بلوکهایی از تصویر که حاوی الگوهای تکراری هستند ، انتخاب می شوند . گرچه این روشها در برابر JPEG مقاوم اند ولی بیشتر برای تصاویری که حاوی مناظر و اجسام طبیعی هستند ، مناسب می باشند .

^۱ Least Significant Bit

نهان نگاری به روش طیف گسترده از یک مفهوم مخابرات طیف گسترده استفاده می کند که در آن یک سیگنال باند باریک در داخل یک سیگنال شبه نویز منتقل می شود . توانایی این روش در تحمل تداخلات ناخواسته بسیار بالاست . این روش همچنین دارای مزایای امنیت حاصل از رمز نگاری است که بر مبنای کلید های استفاده شده در تولید رشته های شبه تصادفی متعامد مانند رشته های گلد یا کاسامی حاصل می شود [۶] .

این مقاله در باره نهان نگاری دیجیتال تصاویر ثابت به روش طیف گسترده ، در حوزه تبدیل گسسته کسینوسی است . از میان روشهای مختلف در این زمینه ، [۷ الی ۱۳] ، روش پیشنهادی کاکس مبنای کار این تحقیق قرار گرفت [۱۳] . این روش سیگنال و اتر مارک را در مهمترین مؤلفه های تصویر از نظر بینایی انسان ، قرار می دهد . ابتدا تبدیل گسسته کسینوسی کل تصویر گرفته می شود و سپس سیگنال پیام طیف گسترده در مهمترین مؤلفه های طیفی تصویر ، از نظر قابلیت درک و مشاهده ، درج می شود .

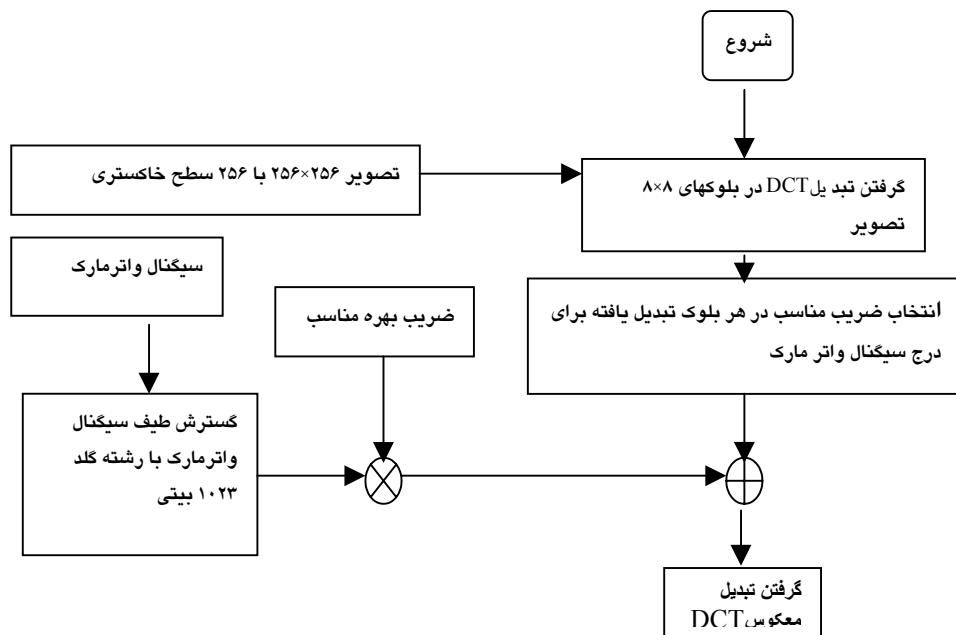
در روش پیشنهادی ما ، بر خلاف روش کاکس ، به منظور ایجاد مقاومت بیشتر در برابر فشرده سازی JPEG ، همانند روش JPEG ، از بلوکهای ۸×۸ تصویر ، تبدیل گسسته کسینوسی گرفته می شود . سپس در هر بلوک ۸×۸ که به طور تصادفی انتخاب می شود ، ضریب مورد نظر از سیگنال و اتر مارک ، درج می شود . مقاومت این روش نهان نگاری در برابر انواع تغییرات در تصویر به خصوص فشرده سازی JPEG با ضریب کیفیت های مختلف ، اضافه شدن نویز های ناشی از انتقال در یک کانال مخابراتی ، تغییرات هندسی مانند تغییر مقیاس و اندازه شکل و نیز بریده شدن بخشی از تصویر بررسی می شود.

۲. طراحی آلوگوریتم نهان نگاری و بررسی مقاومت آن

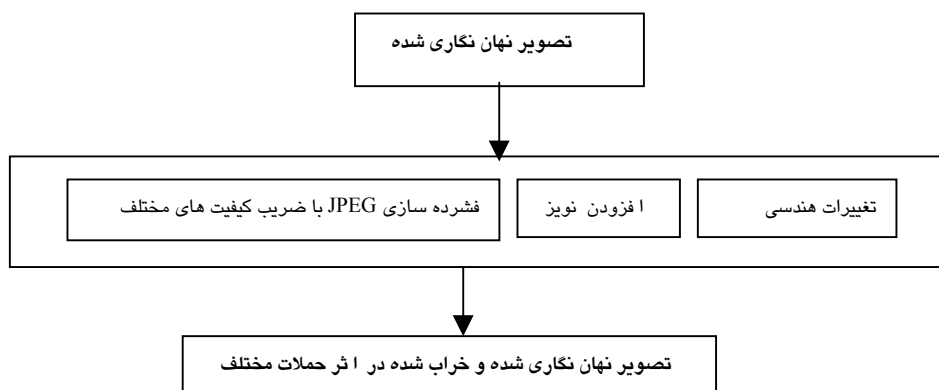
آلوگوریتم پیشنهادی در این مقاله ، برای نهان نگاری دیجیتال تصویر ثابت به روش طیف گسترده در حوزه DCT ، در شکل های ۱ و ۲ و ۳ نشان داده شده است . [۱۴]

۲-۱. درج و اتر مارک

برای درج و اتر مارک ، ابتدا سیگنال پیام به یک سیگنال ۲ قطبی تبدیل شده و هر بیت آن در یک رشته ۱۰۲۴ بیتی گلد ضرب می شود . سیگنال طیف گسترده و اتر مارک از حاصل جمع این بیتها بر روی تمام سیگنال پیام ، حاصل می شود [۱۴] . برای جلوگیری از حذف سیگنال و اتر مارک در اثر فشرده سازی با اتلاف ، هر یک از مؤلفه های این سیگنال در مهمترین ضریب AC از تبدیل DCT هر بلوک با توجه به جدول کوانتیزه JPEG درج می شود . انتخاب هر بلوک برای وارد کردن سیگنال و اتر مارک ، به طور اتفاقی انجام میشود . پس از



شکل ۱ روند نمای درج سیگنال واترمارک در تصویر



شکل ۲ روند نمای تغییرات عمدی و غیر عمدی تصویر نهان نگاری شده به هنگام انتقال

$$Sim(X, X^*) = \frac{X \cdot X^*}{\sqrt{X^* \cdot X^*}}$$

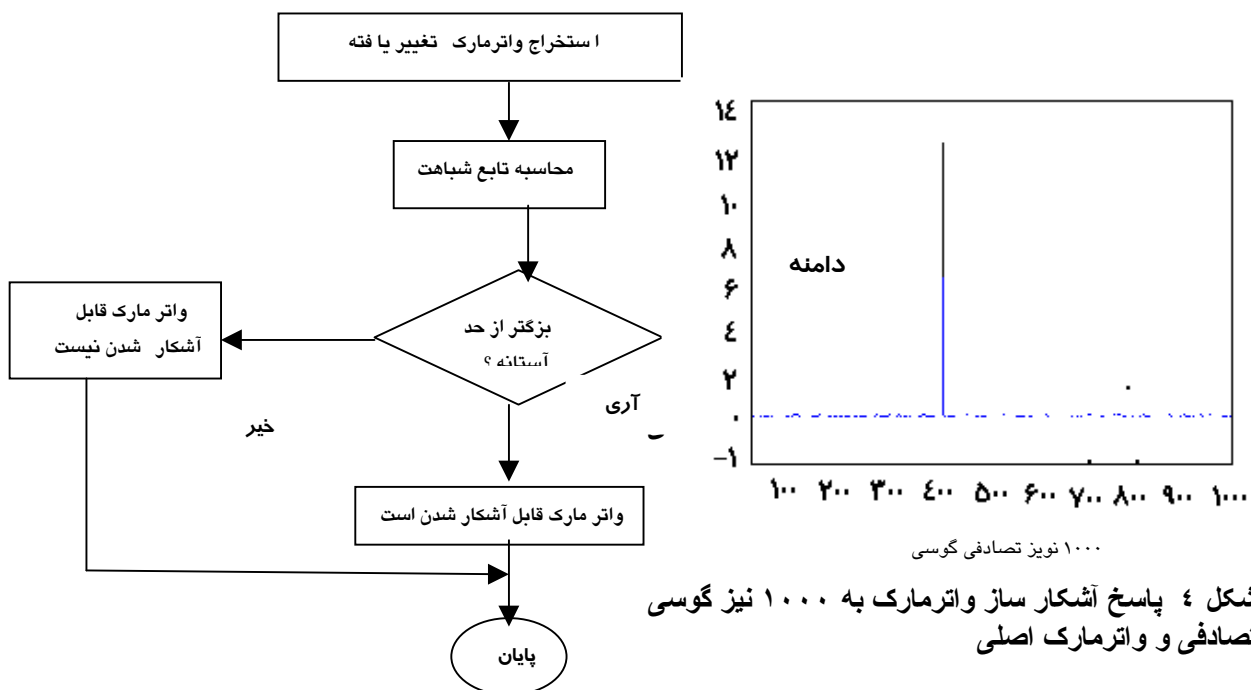
آن، تصویر واترمارک شده همان طور که در شکل ۲ نشان داده شده، تحت تأثیر انواع حملات قرار می گیرد.

۲-۲. آشکارسازی واترمارک از تصویر خراب شده

نحوه آشکارسازی سیگنال واترمارک در شکل ۳ نشان داده شده است. باید توجه داشت که امکان اینکه سیگنال اصلی پیام، X ، که در تصویر درج شده است، درست همان سیگنال واترمارک استخراج شده، X^* ، باشد بسیار کم است. در نتیجه شباهت بین X و X^* را با استفاده از رابطه زیر اندازه می گیریم:

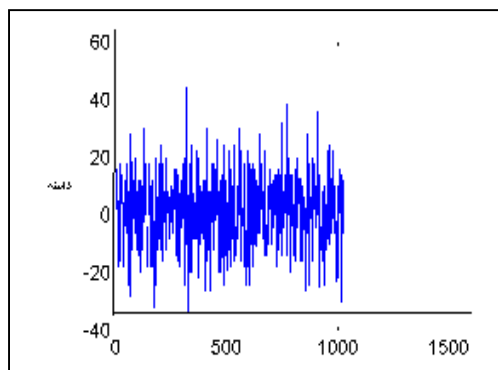
رابطه فوق یک رابطه معمول برای اندازه گیری شباهت بین سیگنال اصلی واترمارک و سیگنال استخراج شده است [۱۳].

برای بدست آوردن حد آستانه، همانطور که در شکل ۴ نشان داده شده است، مقادیر تابع شباهت بین ۱۰۰۰ نویز گوسی تصادفی تولید شده توسط یک مولد نویز گوسی، با سیگنال پیام طیف گسترده، محاسبه شده و از بیشینه این مقادیر بعلاوه قدر مطلق مقدار متوسط آنها، به عنوان حد آستانهء سنجش برای مقادیر تابع شباهت بدست آمده در آزمایشهای مختلف، استفاده شده است.



شکل ۳ روند نمای استخراج واترمارک از تصویر نهان نگاری شده

۳. نتایج آزمایش ها



شکل ۵ سیگنال طیف گسترده پیام

کیفیت های مختلف است. این موضوع به خصوص وقتی فشردن سازی ها به همراه افزودن نویز و عبور تصویر نهان نگاری شده از فیلتر مناسب صورت می گیرد، خود را بیشتر نمایان می سازد. به طور مثال در نمودار ۱، حملات $j15+2N2F$, $j50+2N2F$, $j35+2N2F$, $j75+2N2F$ ، همگی مقدار تقریباً مشابهی از تابع شباهت را بدست می دهند. این نتیجه جالب، نمایانگر

در این تحقیق از جمله "This is a watermark" به عنوان سیگنال پیام استفاده شده است که در ۳ تصویر استاندارد 256×256 ، با 256 سطح خاکستری به نام های فلفله^۱، بابون^۲ و زیلدا^۳، به ترتیب به عنوان مثالهایی از تصاویر با نواحی یکنواخت و در عین حال دارای لبه های برجسته، فرکانس بالا و تصاویر هموار، درج می شود (تصاویر اصلی و واترمارک شده در انتهای مقاله آورده شده اند).

برای گسترش طیف سیگنال پیام، از رشته های گلد که خواص آماری مناسبی از نظر همبستگی متقابل پایین دارند، استفاده شده است. سیگنال ۱۵۲ بیتی پیام $\{152 = 19 \times 8 \text{ بیت}\}$ ، با استفاده از رشته های گلد ۱۰۲۴ بیتی، گسترده شده است، شکل ۵ سیگنال حاصل از این گسترش را نشان می دهد. بنابراین در هر یک از ۱۰۲۴ بلوک تصویر، یکی از ۱۰۲۴ مقدار سیگنال گسترش یافته درج می شود، ترتیب انتخاب بلوکها تصادفی است.

برای بررسی عملکرد الگوریتم پیشنهادی، تصویر نهان نگاری شده تحت تأثیر حملات مختلفی مطابق جدول (۱) قرار داده شده و نتایج حاصله در نمودار های ۱ و ۲ نشان داده شده است. از نتایج بسیار جالبی که در نمودار ۱ مشخص است، تغییر بسیار کم اندازه تابع شباهت در فشردن سازی JPEG با ضریب

^(۳) Zelda

^(۲) Baboon

^(۱) Pappers

مقاومت بسیار خوب سیگنال و اتر مارک در برابر فشرده سازی های مختلف است. به عبارت دیگر، تغییر مقدار شباهت، تابعی از نویز اضافه شده و فیلتر استفاده شده برای بهبود آن بوده و با وجود آنکه در اثر فشرده سازی با ضریب کیفیت ۱۵٪، مقدار بسیار زیادی از اطلاعات تصویر از بین رفته است، ولی مقاومت و اتر مارک نسبت به حالت مشابه ولی با فشرده سازی تحت ضریب کیفیت ۷۵٪، تغییر چندانی نکرده است. از این نتایج چنین بر می آید که درج هر بیت از سیگنال طیف گسترده و اتر مارک در ضریبی از تبدیل DCT هر بلوک که از نظر JPEG ارزش بیشتری دارد، سبب مقاوم شدن بسیار زیاد سیگنال نهان شده در تصویر، در برابر فشرده سازی های J PEG می شود.

نکته قابل توجه دیگر این است که سیگنال و اتر مارک در تصویر بابون نسبت به نویز فلفل - نمکی و عبور از فیلتر میانه مقاومت کمتری نسبت به نویز گوسی از خود نشان می دهد و این برخلاف چیزی است که در نهان نگاری بر روی تصاویر فلفل ها و زیلدا که فرکانس مکانی کمتری دارند، مشاهده می شود. علت آن هم تأثیر زیادتر فیلتر میانه بر روی تصویر بابون است که دارای فرکانس مکانی زیادتری نسبت به دو تصویر دیگر است و در اثر هموار شدن توسط این فیلتر، دچار تغییرات زیادی می شود. در نتیجه اطلاعات سیگنال و اتر مارک هم متحمل تغییرات زیادی می شود که به نوبه خود سبب کم شدن مقدار تابع شباهت و پایین آمدن مقاومت و اتر مارک در برابر این حمله می شود.

توضیحات		
ردیف	علائم مختصر	
1	j75	Q= % JPEG
2	j50	Q= % JPEG
3	j35	Q= % JPEG
4	j15	Q= % JPEG
5	G+WF	(m=0,v=.005)
6	S&P+MF	
7	G+S&P+2F	
8	j75+2N2F	Q= %
9	j75S&P+MF	Q= %
10	j75G+WF	Q= %
11	j50+2N2F	Q= %
12	j50S&P+MF	Q= %
13	j50G+WF	Q= %
14	j35+2N2F	Q= %
15	j35S&P+MF	Q= %
16	j35G+WF	Q= %
17	j15+2N2F	Q= %
18	j15S&P+MF	Q= %
19	j15G+WF	Q= %
20	Resize	× ×
21	C 1/2	/
22	C 1/3	/
23	C 1/4	/
24	C 1/5	/
25	C 1/6	/

- 5) P.Davvern , M.Scott , "Fractal based image steganography" , in PrePro. Information Hiding, Univ.of Cambridge , U.K. , May 1996 , pp. 245-256.
- 6) J.G.Proakis, M.Salehi , " Contemporary Communication Systems using MATLAB" , 2000 by Brooks/Cole Publishing Company, pp. 392-422
- 7) T.Kaller , G.Depovere , M.Macs , " A video watermarking system for broadcast monitoring " , in Proc.SPIE Electronic Imaging , jan. 1999 , pp. 103-112 .
- 8) Y.L.Guan, J.Jinjing , "An Objective Compression between Spatial & DCT Watermarking Schemes for MPEG Video" , IEEE International Conf.Information technology coding and computers (ITCC01) , April 2001 , pp.211-297.
- 9) R. B. Wolfgang , C. I. Podilchuk and E. J. Delp. , "Perceptual Watermarks for Digital Images and Video " , Proceedings of the IEEE , Vol. 87,NO. 7, July 1999 , pp.1108-1126 .
- 10) LM. Marvel , C. G. Boncelet , and C. T. Retter , " Spread Spectrum Steganography" , IEEE Transactions on Image Processing , Vol. 8 , No. 8 , August 1999 , pp.1078-1083.
- 11) I.J.Cox , M. L. Miller and A. L. Mckellips , "Watermarking as communications with side information " , Proceedings of the IEEE , vol. 87,no.7,IEEE 1999 , pp.1127-1141.
- 12) M. D. Swanson , M. Kobayashi and A. H. Tewfik , " Multimedia Data -Embedding and Watermarking Technologies " , Proceedings of the IEEE , Vol. 86 , No. 6, June 1998 , pp. 1064-1087 .
- 13) I.J.Cox , J.Kilant , T.Leighton and T.Shamoon , " Secure Spread Spectrum Watermarking for Multimedia " , IEEE Trans.Image Processing , vol.6 , Dec.1997 , pp. 1673-1687 .

۱۴ ف. ادریسی ، ل. احسان ، " نهان نگاری دیجیتال تصویر به روش طیف گسترده در حوزه DCT " ، پایان نامه کارشناسی ارشد مخابرات گرایش سیستم ، دانشکده صداوسیما ، تابستان ۱۳۸۱

در حالت کلی می توان از نمودار ۱ نتیجه گرفت که تصاویر هموار (مانند تصویر زیلدا) ، در برابر حملات فشرده سازی به همراه اضافه شدن نویز و فیلتر شدن ، مقاومت بیشتری را از خود نشان می دهد .
در این آزمایشها ، مقادیر مختلف ضریب بهره a از ۰/۵ تا ۲ ، از نظر تأثیری که در مقاومت سیگنال واترمارک به حملات مختلف دارد ، نیز مقایسه شده اند . این مقایسات در نمودار ۲ بر روی تصویر بابون نشان داده شده اند. ملاحظه می شود که گرچه افزایش ضریب بهره ، مقاوت واترمارک را در برابر اکثر حملات به خصوص آنهایی که با افزودن نویز و عبور از فیلترهای مختلف همراهند ، به نحو قابل ملاحظه ای افزایش می دهد ، ولی در حملات مربوط به بریدن بخشی از تصویر ، تأثیر چندانی در بالا بردن مقاومت سیگنال واترمارک ندارد . علت هم این است که در این حمله ، با کمبود نواحی دارای سیگنال واترمارک مواجه هستیم و بالا بردن ضریب بهره کمکی به افزایش مقاومت سیگنال واترمارک نمی کند [۱۴].

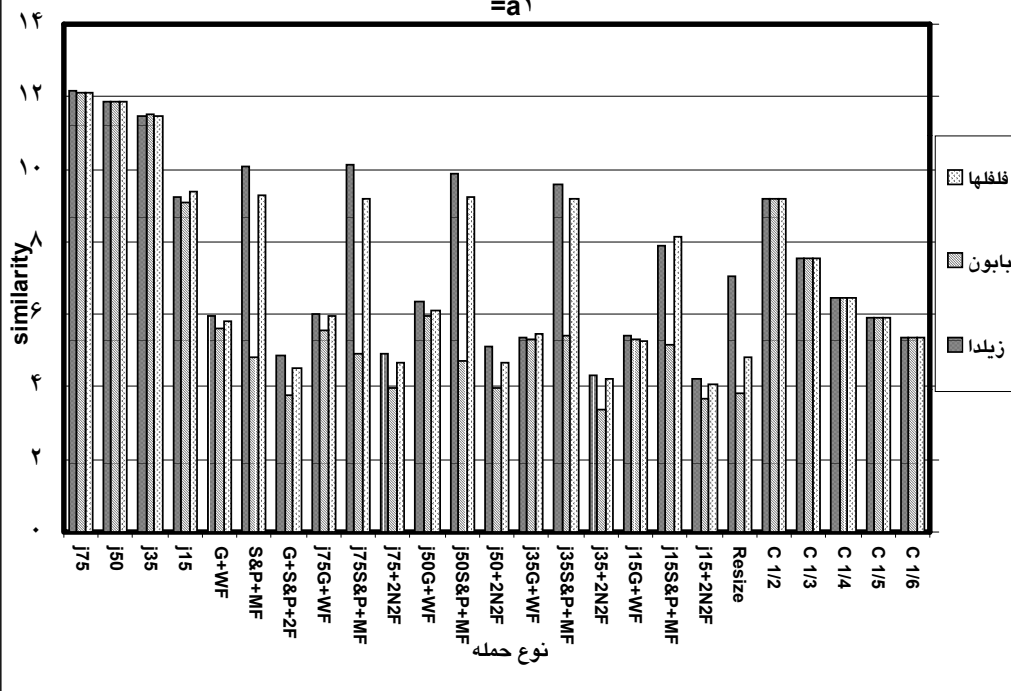
۴. نتیجه گیری

از آنجا که سیگنال واترمارک در طی تمام حملات صورت گرفته به خوبی آشکار شده ، امکان بروز خطای مثبت یا منفی با روش نهان نگاری پیشنهادی بسیار کم است . همچنین مقاومت بسیار خوب سیگنال واترمارک در برابر فشرده سازی JPEG نشان دهنده انتخاب مناسب ضرایب درج سیگنال واترمارک است . افزایش ضریب بهره تا میزان $a=2$ ، گرچه هیچ تأثیر کیفی جدی بر روی تصویر ندارد ولی مقاومت سیگنال را به طور مؤثری در برابر حملات افزایش می دهد .

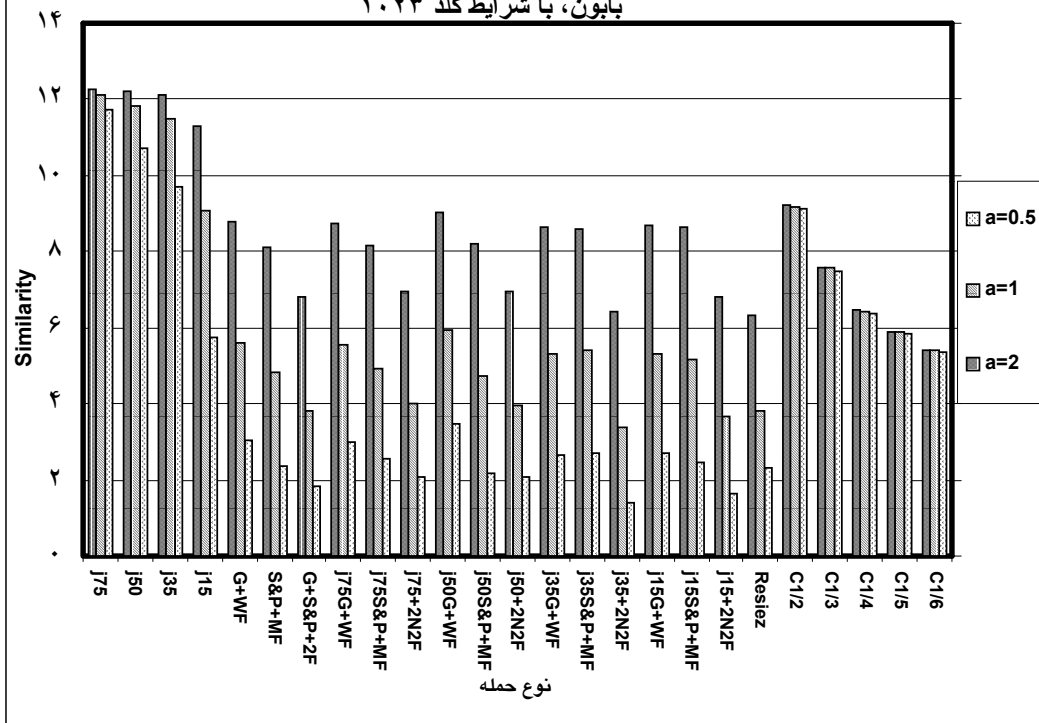
مراجع

- 1) G.C.Langelaar , I. Setyawan and R. L. Lagendijk , " Watermarking Digital Image and Video Data " in IEEE Signal Processing Magazine , Sept. 2000 , pp.1053-1058.
- 2) J.K. O Ruanaidh , T.Pun, " Rotation , Scale and Translation Invariant Spread Spectrum Digital Image Watermarking" , IEEE Signal Processing , vol. 66 , No.3 , may 1998 , pp. 303-317
- 3) S.Jeong , K.Hong Dual , "Detection of A Watermark Embedded in the DCT Domain" , EE368Aproject Report , Image Systems Eng.Program,Stanford University, 31 May,2001.
www.Iseo.stanford.edu/class/ee368a_Proj01/dropbox/Project06.
- 4) C. Fei , D.Kundur and R. Kwong " The Choice of Watermark Domain in the Presence of Compression " , Proceeding of the IEEE ,Int Conf. 2001,pp. 79-86 .

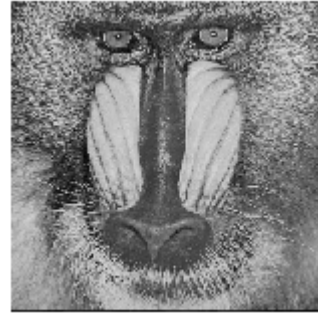
نمودار ۱: مقایسه بین سه تصویر، به روش اتفاقی، با شرایط گلد ۱۰۲۳ و ضریب بهره $a=1$



نمودار ۲: مقایسه بین ۳ ضریب ($a=0.5, a=1, a=2$) به روش اتفاقی، روی تصویر بابون، با شرایط گلد ۱۰۲۳



تصویر اصلی بابون



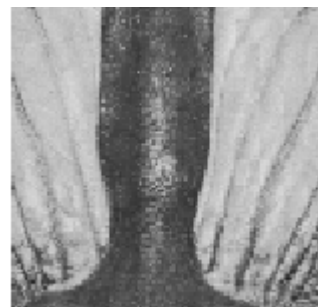
تصویر واتر مارک شده بابون



افزودن دو نویز و عبور از فیلتر وینر و میانه و JPEG با $Q=35\%$ به تصویر واتر مارک شده



بریدن $1/6$ تصویر واتر مارک شده



افزودن دو نویز و عبور از فیلتر وینر و میانه و JPEG با $Q=15\%$ به تصویر واتر مارک شده



تصویر اصلی زیلدا



تصویر واتر مارک شده زیلدا



افزودن نویزهای گوسی و فلفل نمکی و JPEG با $Q=35\%$ به تصویر واتر مارک شده



بریدن $1/3$ تصویر واتر مارک شده



افزودن نویز فلفل نمکی و گوسی و JPEG با $Q=15\%$ به تصویر واتر مارک شده



تصویر اصلی فلفلها



تصویر واتر مارک شده فلفلها



افزودن نویز فلفل نمکی به تصویر واتر مارک شده



تغییر درجه تفکیک تصویر واتر مارک شده



تصویر واتر مارک شده به همراه JPEG با $Q=15\%$

