فصلنامه سیستم‌های پردازشی و ارتباطی چندرسانه‌ای هوشمند
Intelligent Multimedia Processing and Communication Systems (IMPCS)

**Spring, 2022, 3 (1), 47-56**
**DOR: 20.1001.1.27832570.1400.2.2.3.6**

**Received: 26 Sep 2021**
**Accepted: 11 Nov 2021**

# Improving the Security of Image Watermarking Based on the Combination of Discrete Wavelet Transform, Singular Value Decomposition and Discrete Cosine Conversion Methods

**Hosein Nematizade[1], Mohammad Tahghighi Sharabyan[2]***

1.Msc. Student, Faculty of Computer Engineering, Raja University of Qazvin, Qazvin Iran. nematizadh@gmail.com
2. Assistant Professor, Faculty of Electrical and Computer Engineering, Zanjan Branch, Islamic Azad University, Zanjan, Iran.*(Corresponding Author)* mntahghighi@gmail.com

## Abstract

**Introduction**: One of the methods of ensuring information security is the use of encryption methods, but these methods are not able to hide the existence of information. In order to hide information, algorithms called Steganography have been created. Steganography is the method of hiding important data in a file or ordinary message, in order to prevent detection by others. This secret information is extracted to the original state at the destination. The use of Steganography can be combined with encryption as an additional step to hide or protect data. Steganography can be used to hide almost any type of digital content, including text, images, video, or audio content. Often the content to be hidden is encrypted before the Steganography process to provide an extra layer of protection. Steganography is more focused on keeping information hidden, while cryptography is more involved with the issue of ensuring access to information. According to the type of cover signal and also the insertion algorithm, different steganography methods have been presented, which in terms of hiding capacity and security are different. This issue has also led to reproduction, redistribution, and illegal digital media. Since copying and changing digital data has become easy and undetectable, its investigation is also of great importance.

**Method**: In this article, a new method for non-blind image hiding that is resistant to affine transformation and normal image manipulation is used. The proposed Steganography method is based on additive discrete wavelet transform and singular value decomposition. After using RWDT for overlay and hidden images, we use SVD for their LL subbands. Then we modify the singular values of the overlay image using the singular values of the visual masker.

**Result**: Analytical studies on the extracted watermarked image show that the Steganography method is capable and resistant against Salt & Pepper attacks with a scale of 0.1 out of 1.0 and Gaussian attack with a rate of 0.01 and the watermarked image is well recovered.

**Discussion**: One of the most common cryptography techniques in the field of transformation is the modification of the coefficients obtained from the Singular Value Decomposition (SVD) of the image mask. The proposed algorithm has a good performance against rotation and cutting attacks, also the Steganography based on multiple SVD has performed poorly against these two attacks.

**Keywords:** Cloud computing, anomaly detection, normal behavior, behavioral parameters, biased behavior.

فصلنامه سیستم‌های پردازشی و ارتباطی چندرسانه‌ای هوشمند
Intelligent Multimedia Processing and Communication Systems (IMPCS)
انجمن علمی تجارت الکترونیکی ایران

# ارتقا امنیت نهان‌نگاری تصاویر مبتنی‌بر ترکیب روش‌های تبدیل موجک گسسته، تجزیه مقدار تکین و تبدیل کوسینوسی گسسته

تاریخ دریافت: ۱۴۰۰/۰۷/۰۴
تاریخ پذیرش: ۱۴۰۰/۰۸/۱۱
سال سوم، بهار ۱۴۰۱
شمارهٔ اول، صص: ۴۷ – ۵۶

**حسین نعمتی‌زاده[۱]، محمد تحقیقی شربیان[۲*]**

۱. دانشجوی کارشناسی ارشد، دانشکده مهندسی کامپیوتر، دانشگاه رجا، قزوین، ایران nematizadh@gmail.com
۲. استادیار، گروه کامپیوتر، دانشکده مهندسی کامپیوتر، واحد زنجان، دانشگاه آزاد اسلامی، زنجان، ایران. mntahghighi@gmail.com

**چکیده:** امروزه اطلاعات بسیار ارزشمندند و باید از دسترسی افراد غیرمجاز به اطلاعات طبقه‌بندی‌شده جلوگیری‌کرد. یکی از روش‌های تأمین امنیت اطلاعات، بهره‌گیری از روش‌های رمزنگاری است، اما این روش‌ها قادر نیستند وجود اطلاعات را مخفی‌کنند. برای مخفی‌کردن اطلاعات الگوریتم‌هایی با عنوان نهان‌نگاری به‌وجودآمده‌اند که معمولاً برای مخفی‌کردن اطلاعات از یک سیگنال پوشش استفاده‌می‌کنند. با توجه به نوع سیگنال پوشش و همچنین الگوریتم درج، روش‌های نهان‌نگاری متفاوتی ارائه‌شده که از نظر ظرفیت نهان‌نگاری و امنیّت متفاوت‌اند. این مسأله همچنین منجر به بازتولید، توزیع مجدد و غیرقانونی رسانه‌های دیجیتال‌شده‌است. ازآنجاکه کپی‌برداری و تغییر در داده‌های دیجیتال به امری آسان و غیرقابل‌کشف تبدیل‌شده، بررسی آن نیز از اهمیت بالایی برخوردار است. از این رو با توجه به رشد بسیار زیاد شبکه‌های کامپیوتری که انتقال سریع و بدون خطا در هر گونه کپی‌برداری را فراهم‌می‌کند و احتمالاً دستکاری غیرمجاز اطلاعات چندرسانه‌ای را افزایش‌می‌دهد، خطر نقض قانون کپی‌رایتِ داده‌های چندرسانه‌ای به‌طور جدی احساس‌می‌شود. روش‌های حوزه فضایی چندان پیچیده نیست ولی به‌اندازه روش‌های حوزه تبدیل، در برابر حملات گوناگون مقاومت ندارد. یکی از رایج‌ترین تکنیک‌ها در نهان‌نگاری حوزه تبدیل،اصلاح ضرایب به‌دست‌آمده از تجزیه مقدار تکین (SVD) تصویر پوشانه است.

**واژه‌های کلیدی:** نهان‌نگاری، رمزنگاری، موجک گسسته، مقدار تکین.

## ۱. مقدمه

پیشرفت روزافزون فن‌آوری دیجیتال سهولت دسترسی به اطلاعات دیجیتال را بهبود بخشیده‌است. دیجیتالی‌شدن داده‌های چندرسانه‌ای سبب‌شده تا عملیات ذخیره‌سازی سریع‌تر، قابل اعتمادتر و کارآمدتر باشد، فرآیندی که به نوبه خود عملیات انتقال و پردازش داده‌های دیجیتال را فعال‌تر کرده‌است. این مسأله همچنین منجر به بازتولید، توزیع مجدد و غیرقانونی رسانه‌های دیجیتال شده‌است. کپی‌برداری و تغییر در داده‌های دیجیتال به امری بسیار آسان و غیرقابل‌کشف تبدیل-شده‌است. از این رو، باتوجه‌به رشد روزافزون شبکه‌های کامپیوتری که انتقال سریع و بدون خطا در هر گونه کپی‌برداری را فراهم‌می‌کند و احتمالاً دستکاری غیرمجاز اطلاعات چندرسانه‌ای را نیز افزایش‌می‌دهد، خطر نقض قانون کپی‌رایت[۱] داده‌های چندرسانه‌ای به‌طور جدّی احساس‌می‌شود[۱]. نهان‌نگاری دیجیتال به پنهان‌سازی اطلاعات به-صورت غیرقابل‌رؤیت در یک رسانه دیجیتال همچون فیلم، صوت و تصویر به‌منظور اثبات مالکیت و یا انتقال اطلاعات به‌صورت مخفیانه اطلاق‌می-شود[۲]. این روش بخشی از فرآیند کلی‌تری به‌نام استگانوگرافی[۲] است. نهان‌نگاری دیجیتال رابطه نزدیکی با پنهان‌نگاری و پنهان‌سازی داده دارد. ولی با این‌همه، بسته به کاربردهای آن، تفاوت‌هایی نیز مشاهده-می‌شود. در تکنیک‌های نهان‌نگاری[۳]، یک سیگنال پنهانی به‌نام نهان‌نگار، مستقیماً درون داده جاگذاری[۴] می‌شود و همواره در آن باقی‌می‌ماند. برای استفاده از دادهٔ نهان‌نگاری‌شده، نیازی به برداشتن سیگنال نهان‌نگار نیست، زیرا این سیگنال طوری در داده میزبان درج‌می‌شود که هیچ تأثیر نامطلوبی بر داده اصلی نمی‌گذارد. به‌عنوان مثال در نهان‌نگاری داده برای تصاویر، چشم انسان نباید تفاوت بین تصویر اصلی و تصویر نهان‌نگاری-شده را حس‌کند. دو مسأله اساسی در نهان‌نگاری مقاومت[۵]، جداناپذیری نهان‌نگار از تصویر و مشاهده‌ناپذیری نهان‌نگار است؛ درواقع بده‌بستانی بین دو ویژگی مقاومت و غیرقابل‌مشاهده‌بودن در نهان‌نگاری وجوددارد به‌طوری‌که هرچه مقاومت روش نهان‌نگاری بیشتر باشد، مشاهده‌پذیری آن بیشتر است و بالعکس.

## ۲. پیشینه پژوهش

مقاله‌ای با عنوان "ذخیره و بازیابی دو سیگنال دیجیتال مجزای صوت در تصاویر به کمک کدهای دوبعدی مبتنی‌بر نهان‌نگاری" عملیات ذخیره و بازیابی دو سیگنال صوتی مجزا در بیت‌های کم‌ارزش تصویر دیجیتال با استفاده از کدهای دوبعدی را بررسی‌کرده‌است که در آن به کمک الگوریتم تولید کدهای دوبعدی از یک کلمه رمز منحصربه‌فرد، یک تصویر کد دوبعدی تهیه و توسط الگوریتم نهان‌نگاری، اطلاعات دو سیگنال صوتی مجزا در پیکسل‌های تعیین‌شده به کمک کدهای دوبعدی از تصویر میزبان، ذخیره و یک تصویر نهان‌نگاری‌شده تولیدمی‌شود. روش ارائه‌شده را می‌توان به‌عنوان یک روش نهان‌نگاری در بیت‌های کم‌ارزش از پیکسل‌های خاص تصویر و کاربردهای استراتژیک دیگر به‌کاربرد[۳].

یک طرح علامت‌گذاری ترکیبی استوار و محور براساس تبدیل موجک گسسته (DWT) و تجزیه ارزش مفرد نیز پیشنهاد و شبیه‌سازی شد. در ابتدا ، تصویر رنگی RGB به فضای رنگی YCbCr تبدیل‌می‌شود که از آن تنها جزء آکروماتیک Y برای درج داده‌های علامت درنظرگرفته‌می-شود. در مرحله بعد ، مؤلفه Y مدل رنگی YCbCr در بلوک‌های بدون همپوشانی تجزیه‌می‌شود و متعاقباً DWT برای هر بلوک اعمال‌می‌شود. در این کار ، بلوک‌های تصویری خاکستری تجزیه‌نشده که با هم تداخل-دارند به مقادیر منحصر به فرد بلوک‌های تصویر جلد با DWT تبدیل-می‌شوند. نتیجه شبیه‌سازی تکنیک پیشنهادی با استخراج داده‌های علامت کافی از تصویر روی جلد بازسازی‌شده، پس از اعمال حملات دگرگونی هندسی معمول(مانند چرخش، عملکرد تلنگر، برداشت، پوسته‌پوسته شدن، برش‌دادن و حذف خطوط یا عملکرد ستون)، استحکام ایجادمی‌کند[۲].

در مطالعهٔ دیگری باعنوان "یک الگوریتم علامت‌گذاری دیجیتال قوی با استفاده از DWT و SVD، یک روش تصویربرداری قوی دیجیتالی با استفاده از روش Wavelet Transform (DWT) و تجزیه ارزش انحصاری (SVD) ارائه‌کرده‌است. در این روش ابتدا تصویر اصلی ۲۵۶ × ۲۵۶ اندازه DWT به سطح سوم با استفاده از موج ویروس Haar تجزیه‌می‌شود که چهار زیربست LL3، LH3، HL3 و HH3 را فراهم‌می‌کند. پس از آن، SVD در این زیر باندها اعمال‌می‌شود تا ماتریس‌های مورّب از مقادیر منحصربه‌فرد به‌دست‌آیند. سپس علامت نهان‌نگاری در این مقادیر منحصربه‌فرد از چهار زیر باند جاسازی‌می‌شود. نتایج نشان‌می‌دهد ارزش PSNR برای کار جاری به‌دست‌آمده در مقایسه با رویکردهای قبلی بهتر است. علاوه‌بر این، نتایج به‌دست‌آمده نشان‌می‌دهد که با استفاده از روش فعلی می‌توان تصویر علامت‌گذاری‌شده را به‌درستی استخراج‌کرد حتی زمانی که تصویر علامت‌گذاری‌شده تحت حملات مختلف مانند چرخش، تاری حرکت، نویز گاوسی، اصلاح گاما، بازتابی، برداشت، مقیاس هیستوگرام و غیره است[۳]. مطالعه موجود دیگری به ذخیره و بازیابی دو سیگنال دیجیتال مجزای صوت در تصاویر به کمک کدهای دوبعدی مبتنی‌بر نهان‌نگار امن‌سازی اطلاعات کاربران در سیستم پردازش ابری پرداخته‌است. در این پژوهش برای افزایش مسائل امنیتی و حفظ حریم خصوصی به‌نحوی که تبادل اطلاعات برای دیگران محسوس و مشخص نباشد، با تلفیق رمزنگاری و نهان‌نگاری به تبادل اطلاعات در محیط ابر

پرداخته‌شده و هدف، رسیدن به یک سطح امنیتی مطلوب در تبادل اطلاعات محرمانه و بالابردن فاکتور امنیت در محاسبات ابری می‌باشد[۴]. در پژوهش یادشده تکنیک کارایی علامت‌گذاری برای بهبود عملکرد رویکرد مبتنی‌بر DWT-SVD ارائه‌شده‌است. در این روش از کد شناخته‌شده تصحیح خطا (ECC) و رمزگذاری آشوب استفاده‌شده‌است تا به‌ترتیب اعوجاج نویز کانال را کاهش‌داده و امنیت تکنیک را بهبود-بخشد. در روش پیشنهادی، تصویر کاور توسط DWT تبدیل‌می‌شود و زیر باندها برای تعبیه علامت‌های سفید انتخاب‌می‌شوند. پس از آن ، زیرباندهای انتخابی توسط SVD تبدیل‌می‌شوند. استفاده از تکنیک‌های دامنه تبدیل به‌همراه کد هامینگ اطمینان‌می‌دهد که این رویکرد استحکام و قابلیت اطمینان بیشتری دارد. گنجاندن رمزگذاری مبتنی‌بر آشوب دارای مزایای دو چندان مانند پنهان‌کردن محتوای علامت گذاری‌شده و تقویت امنیت کلی طرح پیش‌بینی‌شده است. روش ارائه-شده مقدار قابل‌توجهی از نسبت اوج سیگنال به نویز (PSNR)، همبستگی نرمال (NC)، میزان خطای بیت (BER)، تعداد تغییر پیکسل (NPCR) و میانگین تغییر شدت یک‌پارچه (UCAI) را در اختیار می-گذارد[۵]. یک طرح علامت‌گذاری ترکیبی استوار و محور براساس تبدیل موجک گسسته (DWT) و تجزیه ارزش مفرد پیشنهاد و شبیه‌سازی-کردند. درابتدا، تصویر رنگی RGB به فضای رنگی YCbCr تبدیل‌می‌شود که از آن تنها جزء آکروماتیک Y برای درج داده‌های علامت در نظر گرفته‌می‌شود. در مرحله بعد، مؤلفه Y مدل رنگی YCbCr در بلوک‌های بدون همپوشانی تجزیه‌می‌شود و متعاقباً DWT برای هر بلوک اعمال-می‌شود. در این کار، بلوک‌های تصویری خاکستری تجزیه‌نشده با هم تداخل‌دارند و به مقادیر منحصربه‌فرد بلوک‌های تصویر جلد با DWT تبدیل‌شده‌اند. نتیجه شبیه‌سازی تکنیک پیشنهادی با استخراج داده‌های علامت کافی از تصویر روی جلد بازسازی‌شده، پس از اعمال حملات دگرگونی هندسی معمول (مانند چرخش، عملکرد تلنگر، برداشت، پوسته‌پوسته شدن، برش‌دادن و حذف خطوط یا عملکرد ستون)، استحکام را ایجادمی‌کند[۶].

## ۳. روش پیشنهادی

روش جدید برای نهان‌نگاری تصویر غیرکور که در برابر تبدیل همگر(آفین) مقاوم است و دستکاری تصویر معمولی ارائه‌می‌شود. روش ارائه‌شده نهان‌نگاری مبتنی‌بر تبدیل موجک گسسته افزونه و تجزیه مقدار تکین را مطرح‌می‌کند. پس از به‌کارگیری RWDT برای تصاویر پوشانه و نهان‌نگار، SVD را برای زیرباندهای LL آن‌ها به‌کارمی‌گیریم. سپس مقادیر تکین تصویر پوشانه را با استفاده از مقادیر تکین نهان‌نگار دیداری اصلاح‌می‌کنیم.

نهان‌نگاری ( پنهان‌سازی داده‌ها) فرایند جاسازی داده‌ها در گروه چندرسانه‌ای از قبیل تصویر، صوت یا ویدئو و برای اهداف امنیتی یا محافظت از حق نشر است. این داده جاسازی‌شده را می‌توان بعدها از چندرسانه استخراج‌کرد یا در آن تشخیص‌داد. الگوریتم نهان‌نگاری شامل الگوریتم جاسازی و الگوریتم استخراج یا تشخیص است. نوع اطلاعات مورد نیاز توسط آشکارساز، معیار مهمی در طبقه‌بندی طرح‌های نهان-نگاری به‌شمارمی‌رود:

- طرح‌های غیرکور مستلزم تصویر اصلی و کلید(های) سرّی برای جاسازی نهان‌نگار می‌باشند.
- طرح‌های نیمه‌کور مستلزم کلید (های) سرّی و خود نهان‌نگارند.
- طرح‌های کور صرفاً مستلزم کلید (های) سرّی‌اند.

نهان‌نگاری را می‌توان در حوزه فضایی یا تبدیل انجام‌داد. روش‌های حوزه فضایی چندان پیچیده نیستند ولی درعین‌حال، به اندازه روش‌های حوزه تبدیل در برابر حملات گوناگون مقاومت ندارند. یکی از رایج‌ترین تکنیک‌ها در نهان‌نگاری حوزه تبدیل، اصلاح ضرایب به‌دست‌آمده از تجزیه مقدار تکین (SVD) تصویر پوشانه است. الگوریتم نهان‌نگاری مبتنی‌بر SVD نخستین بار توسط لیو و همکاران مطرح‌شد. در این الگوریتم، نویسندگان پس از به‌کارگیری تجزیه مقدار تکین برای تصویر پوشانه این ضرایب را با افزودن نهان‌نگار اصلاح‌می‌کنند. آن‌ها تبدیل SVD را دوباره در ماتریس به‌دست‌آمده به‌کار می‌گیرند تا مقادیر تکین اصلاح‌شده را بیابند. این مقادیر تکین با مؤلفه شناخته‌شده‌ای ترکیب-شده‌اند تا به تصویر نهان‌شده دست‌یابند. در اثر مشابه دیگر، چاندرا و همکاران مقادیر تکین نهان‌نگار را در مقادیر تکین تمام تصویر میزبان جاسازی‌کردند. مهم‌ترین نقص الگوریتم‌های مبتنی‌بر SVD ، تنزیل کیفیت تصویر نهان‌نگاری‌شده است. افزون بر آن، نهان‌نگار استخراج‌شده در برابر حملات رایج در الگوریتم‌های مبتنی‌بر SVD به‌اندازه کافی مقاوم نیست. بنابراین، پژوهشگران معمولاً SVD را با سایر الگوریتم‌ها از قبیل DCT و DWT ترکیب‌می‌کنند. در [۷]، نویسندگان DWT را با تکنیک SVD ترکیب‌کردند. در مقاله یادشده، پس از تجزیه تصویر میزبان به چهار زیرباند، SVD را برای هر زیرباند به‌کار بردند و مقادیر تکین نهان-نگاری‌شده را در زیرباندها جاسازی‌کردند. در [۸]، DWT با تکنیک SVD ترکیب می‌شود تا مقادیر تکین نهان‌نگار را در باند فرکانس بالای (HH) تصویر پنهان‌سازد. هنگامی که DWT با تکنیک SVD ترکیب‌می‌شود، الگوریتم نهان‌نگاری درخصوص مقاومت در برابر نویز گاوسی، حملات فشرده‌سازی و قیچی‌کردن عملکرد بهتری از الگوریتم قراردادی DWT دارد.

### ۱،۳. نهان‌نگاری مبتنی‌بر RDWT-DCT-SVD

$$I^{*1} := U^{*1}S^{*1}V^{*1} \quad (۵)$$

#### ۱،۱،۳. جاسازی نهان‌نگار

مراحل الگوریتم جاسازی نهان‌نگار الگوریتم ترکیبی RDWT-DCT-SVD به شرح زیرند:

مرحله ۱: RDWT را برای تصویر پوشانه به‌کاربگیرید تا آن را به زیرباندهای LL، HL، LH و HH تجزیه‌کند.

مرحله۲: DCT را برای زیرباندهای LL، HL، LH و HH تصویر پوشانه به‌کاربرید:

مرحله۳: SVD را برای زیرباند فرکانس پایین LL تصویر پوشانه به‌کاربرید:

$$I^1 = U^1\Sigma^1V^1 \quad (۱)$$

مرحله۴: RDWT را برای نهان نگار دیداری به‌کاربرید.

مرحله۵: SVDرا برای زیرباند فرکانس پایین نهان‌نگار به‌کاربرید:

$$w = U^w\Sigma^wV^w \quad (۲)$$

مرحله۶: مقادیر تکین تصویر پوشانه را با مقادیر تکین تصویر نهان‌نگار اصلاح‌کنید.

$$S^{*1} := S^1 + \alpha S^w \quad (۳)$$

مرحله۷: SVD معکوس را در تصویر پوشانه تبدیل‌شده با مقادیر تکین اصلاح‌شده به‌کارگیرید.

$$I^{*1} := U^1S^{*1}V^1 \quad (۴)$$

مرحله۸: DCT معکوس را در تصویر پوشانه تبدیل‌شده به‌کارگیرید.

مرحله۹: RDWT معکوس را با استفاده از ضرایب اصلاح‌شده باندهای فرکانس پایین به‌کارگیرید تا تصویر نهان‌نگاری‌شده به‌دست‌آید.

#### ۲،۱،۳. استخراج نهان‌نگار

الگوریتم ارائه‌شده استخراج نهان‌نگار به‌شرح زیر است:

مرحله۱: با استفاده از RDWT، تصویر نهان‌نگارشده I* را به ۴ زیرباند: LL، HL، LH و HH تجزیه‌کنید.

مرحله۲: DCT را برای زیرباند فرکانس‌های LL، HL، LH و HH به‌کار-



مرحله۳: SVD را برای زیرباند فرکانس پایین LL به‌کار ببرید:

مرحله۴: مقادیر تکین از زیرباند فرکانس پایین تصویر نهان‌نگاری‌شده و پوشانه استخراج‌کنید:

$$sw' = (S^{*1} - s^1)/\alpha \quad (۶)$$

مرحله۵: SVD معکوس را به‌کارگیرید تا ضرایب فرکانس پایین تصویر نهان‌نگار تبدیل‌شده را به‌دستآورید.

مرحله۶: RDWT معکوس را با استفاده از ضرایب زیرباند فرکانس پایین به‌کار بگیرید تا تصویر نهان‌نگار به‌دست‌آید.

#### ۳،۱،۳. فرآیند جاسازی تصویر نهان‌نگاری

الگوریتم جاسازی‌کردن تصویر نهان‌نگاری در تصویر میزبان به‌شرح زیر می‌باشد:

تصویر میزبان I را به سه ماتریس IR , IG , IB تقسیم‌کنید.

در ماتریس $Ii\ ;\ i = R,G,B$ ، DWT را اجراکنید و آن را به بلوک‌های $Ii\_LL\ ,Ii\_LH\ ,Ii\_HL\ ,Ii\_HH\ ;\ i = R,G,B$ تقسیم‌کنید.

دربلوک $Ii\_LL\ ;\ i =$

$R,G,B$ ،$SVD\ [Ii\_LL\_u, Ii\_LL\_s\ , Ii\_LL\_v] =$

$svd(Ii\_LL)\ ;\ i = R,G,B$ را اجراکنید.

ابعاد تصویر نهان‌نگاری W را به ابعاد بلوک LL از تصویر میزبان تغییردهید.

تصویر نهان‌نگاری W را به سه ماتریس WR , WG , WB تبدیل-کنید.

تصویر نهان‌نگاری را در مقیاس فاکتور T=0.05 ضرب‌کرده ، آنگاه با مقادیر منفرد (S) مجموعه LL از تصویر میزبان جمع‌کنید:

$$Ii\_LL\_s2 = Ii\_LL\_s + T * Wi\ ;\ i = R,G,B$$

در ماتریس i=R,G,B ; Ii_LL_s2 ، SVD را اجراکنید.

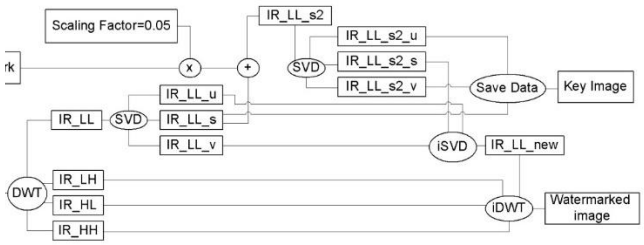
$$[Ii\_LL\_s2\_u, Ii\_LL\_s2\_s\ , Ii\_LL\_s2\_v] = svd(Ii\_LL)\ ;\ i = R,G,B$$

معکوس SVD را به‌شکل زیر اجراکنید. $Ii\_LL\_new = Ii\_LL\_u * Ii\_LL\_s2\_s * Ii\_LL\_vT$

ماتریس ۴ $Ii\_LL\_new, Ii\_LH, Ii\_HL,$ Ii_HH; i=R,G,B را برای $DWT$ اجراکنید و $Ii\ ;\ i = R,G,B$ را به‌دست‌آورید.

سه ماتریس IR , IG , IB را ادغام‌کنید و تصویر نهان‌نگاری‌شده $Iw$ را ایجادکنید.

سه ماتریس Ii_LL_s2_v ,Ii_LL_s ,Ii_LL_s2_u (کلید برای بازیابی تصویر واترمارک) را ذخیره‌نمایید.




**شکل ۱: الگوریتم جاسازی واترمارک در تصویر**

در این الگوریتم، مقدار نهان‌نگاری در ماتریس S تصویر میزبان قرارمی-گیرد.

#### ۴،۱،۳. فرآیند استخراج تصویر نهان‌نگاری

الگوریتم استخراج تصویر نهان‌نگاری از تصویر به‌شرح زیر می‌باشد:

تصویر واترمارک‌شده IW را به سه ماتریس IW R , IW G , IW B تقسیم‌کنید.

در ماتریس $DWT$ ، $IW\ i\ ;\ i = R, G, B$ را اجراکنید و آن را به بلوک‌های

$IW\ i_LL_new\ ,IW\ i_LH\ ,IW\ i_HL\ ,IW\ i_HH\ ;\ i = R, G, B$تقسیم‌کنید.

دربلوک$Ii_{LL_{new}};\ i =$

$R, G, B$ ، $SV\ .\ [IW\ i\_LL\_u, IW\ i\_LL\_s2\_s\ , IW\ i\_LL\_v] =$ $svd(IW\ i\_LL\_new)\ ;\ i = R, G, B$ اجراکنید.

ماتریس‌های $Ii\_LL\_s2\_u\ , Ii\_LL\_s\ , Ii\_LL\_s2\_v$ که در الگوریتم جاسازی واترمارک ذخیره کرده‌بودید را فراخوانی‌کنید.

معکوس SVD را به‌شکل زیر اجراکنید.

$$Ii\_LL\ = Ii\_LL\_u * Ii\_LL\_s * Ii\_LL\_vT$$

معکوس DWT را برای ۴ ماتریس $Ii\_LL, Ii\_LH, Ii\_HL,$ Ii_HH; i=R,G,B اجراکنید و $Ii\ ;\ i = R, G, B$را به‌دست‌آورید.

سه ماتریس IR , IG , IB را ادغام‌کنید تا تصویر میزبان استخراج‌شده ایجادشود.

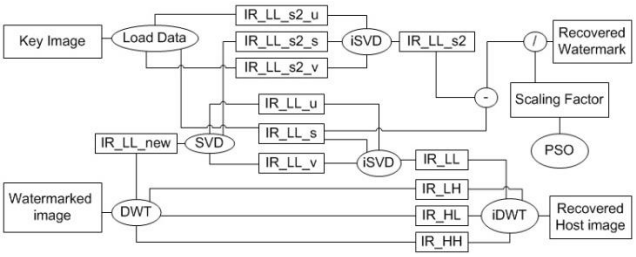
معکوس SVD را به‌شکل زیر اجراکنید.

Ii_LL_s2 =Ii_LL_s2_u*Ii_LL_s2_s*Ii_LL_s2_vT

ماتریس Ii_LL_s2 را از Ii_LL_s کم‌کرده سپس بر مقیاس فاکتور T (مقدار بهینه آن از طریق الگوریتم PSO به‌دست‌می‌آید) تقسیم‌کنید

Wi =(Ii_LL_s2-Ii_LL_s)/T ; i=R,G,B :

سه ماتریس WR , WG , WB را ادغام‌کنید تا تصویر واترمارک استخراج‌شده ایجاد گردد.




**شکل ۲: الگوریتم استخراج واترمارک از تصویر**

فلوچارت الگوریتم پیشنهادی به همراه الگوریتم پیشنهادی جهت استخراج‌کردن واترمارک بر روی تصویر مورد حمله قرارگرفته به‌صورت شکل ۳ می‌باشد.

در این تحقیق یک روش ارتقاء امنیت پنهان نگاری غیرقابل‌تشخیص و مبتنی بر DWT-SVD -DCT پیشنهادمی‌گردد. در این روش چند نکته مورد توجه قرارگرفته‌است که در ادامه به آن می‌پردازیم. نکته اول غیرقابل شخیص بودن است. بیشتر در پنهان‌نگاری از امنیت درازمدت و غیرقابل‌تشخیص بودن استفاده‌می‌شود. به عبارت دیگر، یک طرح استگانوگرافیک امن یک طرح آماری غیرقابل‌کشف است. نکته دوم استفاده از روش DWT به‌همراه تکنیک SVD و DCT است. با توجه به مطالب ارائه‌شده، الگوریتم‌های مبتنی‌بر SVD به دو نوع خالص و ترکیبی دسته‌بندی‌می‌شوند. در مورد الگوریتم‌های مبتنی‌بر SVD خالص، علامت نهان‌نگاری تنها در دامنه SVD جاسازی‌می‌شود، درحالی‌که، الگوریتم‌های مبتنی‌بر SVD ترکیبی، علامت نهان‌نگاری در دامنه SVD و یکی از الگوریتم‌های دامنه تبدیل جاسازی‌می‌شود. این مسأله بر پیچیدگی روش نهان‌نگاری افزوده‌است و آن را برای حمله-کنندگان غیرقابل‌کشف می‌سازد. با توجه به اینکه در روش ما از تکنیک SVD به‌همراه DWT استفاده‌شده‌است، روش پیشنهادی در گروه الگوریتم‌های ترکیبی مبتنی‌بر DCT قرارگیرد. از حیث ریاضی طرح استگانوگرافیک این‌گونه تعریف‌می‌شود: Ks اشاره به کلید استگ برگرفته از از یک مجموعه K، از تمام کلیدهای مخفی استگ دارد، S مجموعه‌ای از تمام پیام‌های مخفی، C مجموعه‌ای از تمام کارهای پوشش است. A طرح استگانوگرافیک تشکیل‌شده توسط دو نقشه: نقشه تعبیه EMB و نقشه استخراج EXT است.

$$Emb : C \times K \times S \rightarrow A$$
$$Ext : A \rightarrow S$$

رابطه $Ext\ (Emb(c, K_s, s)) = A$ برای تمام $A = Emb(c, k_s, s)$ همواره برقراراست و $s \epsilon S$ و $k_s \epsilon K$ ، $c \epsilon C$ کار استگ نامیده‌می‌شود و در روش پیشنهادی برروی تصاویر رنگی اعمال‌می‌شود. اندازه تصویر پوشش و مخفی نامحدود است. روش پیشنهادی تصویر پوششی را به چهار بلوک تقسیم و مقادیر منفرد از تصویر نهان‌نگاری را در بلوک گوشه جنوب‌شرقی از تصویر پوشش درج-می‌کند. برای استخراج تصویر مخفی باید کلید در دسترس باشد.

الگوریتم استخراج نهان‌نگاری تصویر نهان‌نگاری‌شده:

a را به سه ماتریس $aR\ , aG\ , aB$ تقسیم کنید.

در ماتریس DWT ، ai ; i=R,G,B را اجرا کنید و آن را به بلوک‌های $ai\_LL\ , ai\_LH\ , ai\_HL\ , ai\_HH;\ i = R, G, B$ تقسیم‌کنید.

در بلوک $SV$ ، $ai\_HH\ ;\ i = R, G, B$ را اجراکنید.

$$[ai\_HH\_u, ai\_HH\_s\ , ai\_HH\_v] = svd(ai\_HH)\ ;\ i = R, G, B$$ ماتریس‌های

$$ci\_HH\_s\ , si\_HH\_v, si\_HH\_u, si\_LL, si\_LH, si\_HL, Ms\ , Ns$$

که در الگوریتم جاسازی پنهان‌نگاری ذخیره‌کرده‌بودید را فراخوانی‌کنید.

ماتریس $ai\_HH\_s2$ را از $ci\_HH\_s$ کم‌کرده سپس بر مقیاس فاکتور تقسیم‌کنید:

$$si\_HH\_s\_new\ = (ai\_HH\_s - ci\_HH\_s)/T\ ;\ i = R, G, B$$

معکوس SVD را به‌شکل زیر اجراکنید.

$$si\_HH\_new\ =\ si\_HH\_u\ *\ si\_HH\_s\_new\ *\ si\_HH\_v\ T$$

معکوس DWT را برای ۴ ماتریس

$$si\_LL, si\_LH, si\_HL, si\_HH\_new\ =;\ i = R, G, B$$

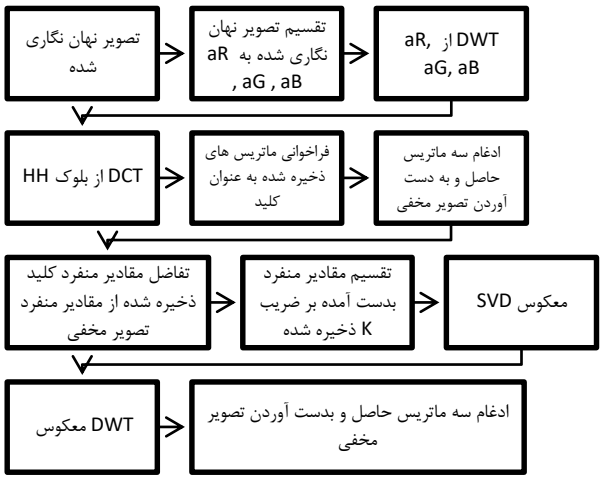
اجراکنید و

$$si\ ;\ i = R, G, B$$

را به‌دست‌آورید.

سه ماتریس $sR\ , sG\ , sB$ را ادغام‌کنید تا تصویر مخفی استخراج‌شده ایجادشود.

فلوچارت پیشنهادی:




**شکل ۳: الگوریتم استخراج پیشنهادی به روش DCT-DWT-SVD**

### ۵،۱،۳. نتایج پیاده‌سازی

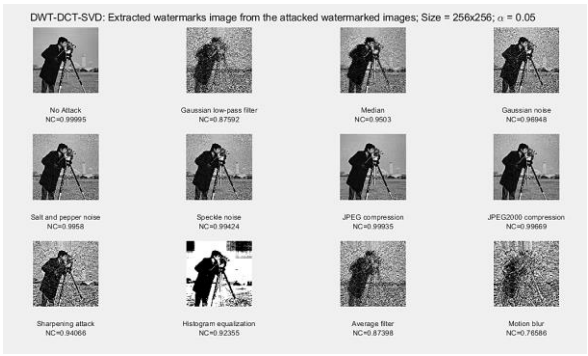
در این قسمت نتایج اجرای برنامه را به‌طور کامل بررسی‌می‌کنیم. نتایج شامل تصویر نهان‌نگاری‌شده و تصویر نهان‌نگاری استخراج‌شده‌است. روی تصویر نهان‌نگاری‌شده، شش نوع حمله صورت‌گرفته‌است: شامل Salt & Pepper، Rotation، Gaussian و Cropping. بعد از اعمال هر حمله روی تصویر نهان‌نگاری‌شده، تصویر نهان‌نگاری را استخراج‌کردیم و اوج نسبت سیگنال به نویز و میانگین مربع خطاها را برای هریک از تصاویر نهان‌نگاری استخراج‌شده به‌دست‌آوردیم. تصاویر و نتایج آزمایش-ها چنین است:

شکل (۵) و شکل (۶) نتایج آزمایش نهان‌نگاری توسط الگوریتم DWT-DCT SVD پیشنهادشده الگوریتم نهان‌نگاری مبتنی‌بر SVD چندگانه را نمایش‌می‌دهد. (a) تصویر نهان‌نگاری‌شده، (b) تصویر نهان‌نگاری استخراج‌شده می‌باشند. نتیجه مربوط به PSNR و MSE در جدول (۱) و جدول (۲) آمده‌است.



**شکل ۴: تصویر نهان‌نگاری‌شده توسط الگوریتم پیشنهادی DWT-DCT SVD**


**شکل ۵- تصویر نهان‌نگاری‌شده توسط الگوریتم پیشنهادی**

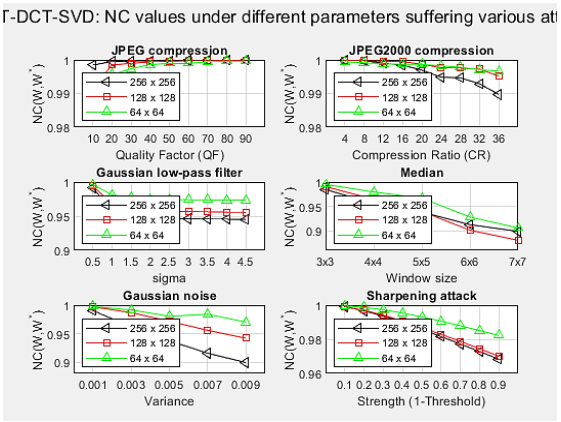



**شکل ۶: حمله Salt & pepper بر روی الگوریتم پیشنهادی**

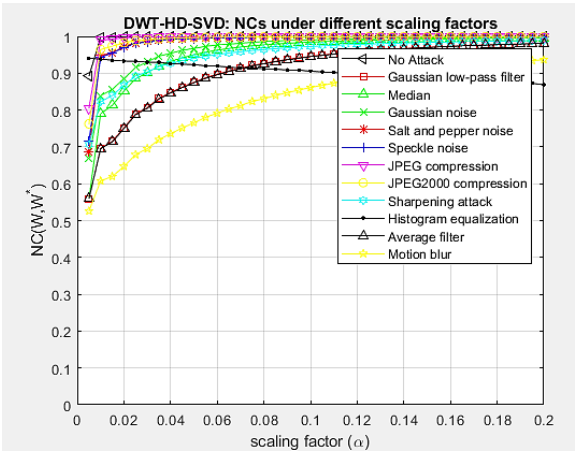
شکل (۶) و شکل (۷) نتایج آزمایش حمله Salt & pepper به تصویر نهان‌نگاری‌شده توسط الگوریتم پیشنهادی DWT-SVD و تصویر نهان-نگاری‌شده توسط الگوریتم نهان‌نگاری مبتنی‌بر SVD چندگانه زارعی (۲۰۱۴) را نمایش‌می‌دهد. در این حمله Salt & Pepper نویزهایی با مقیاس ۰,۱ از ۱,۰ به تصویر نهان‌نگاری‌شده اضافه‌شد. تصویر (a) تصویر نهان‌نگاری‌شده مورد حمله و (b) تصویر نهان‌نگاری استخراج‌شده می-باشند. نتیجه مربوط به PSNR و MSE در جدول (۱) و جدول (۲) آمده‌است.

**شکل ۷: حمله Salt & pepper بر روی الگوریتم پیشنهادی**

شکل (۸) و شکل (۹) نتایج آزمایش حمله Rotation (دوران) به تصویر نهان‌نگاری‌شده توسط الگوریتم پیشنهادی DWT-SVD و تصویر نهان‌نگاری‌شده توسط الگوریتم نهان‌نگاری مبتنی‌بر SVD چندگانه زارعی (۲۰۱۴) را نمایش‌می‌دهد. در این حمله Rotation، تصویر نهان‌نگاری‌شده به اندازه ۲۵ درجه دوران‌داده‌شده‌است. تصویر (a) تصویر نهان‌نگاری‌شده موردحمله و (b) تصویر نهان‌نگاری استخراج‌شده می‌باشند. نتیجه مربوط به PSNR و MSE در جدول (۱) و جدول (۲) آمده‌است.

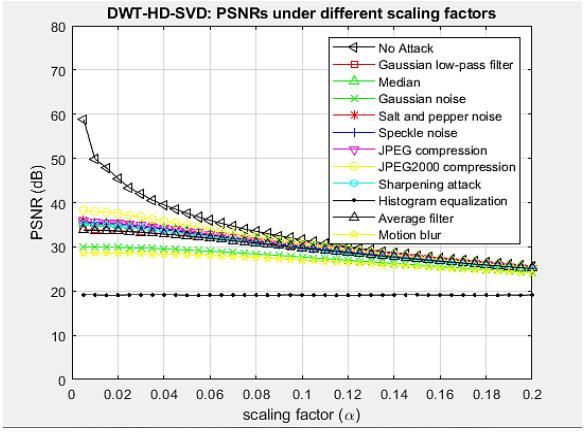



**شکل ۸: حمله Rotation روی الگوریتم پیشنهادی DCT DWT-SVD**

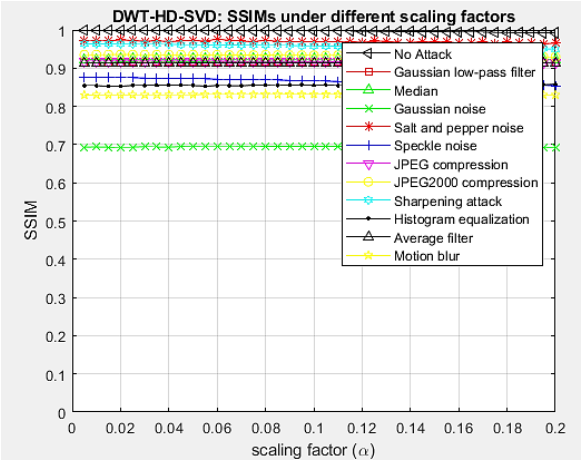



**شکل ۹: حمله Rotation روی الگوریتم پیشنهادی**

شکل (۱۰) و شکل (۱۱) نتایج آزمایش حمله Gaussian (گاوسی) به تصویر نهان‌نگاری‌شده توسط الگوریتم DWT-SVD و تصویر نهان‌نگاری‌شده توسط الگوریتم نهان‌نگاری مبتنی‌بر SVD را نمایش‌می‌دهد. تصویر (a) تصویر نهان‌نگاری‌شده مورد حمله و (b) تصویر نهان‌نگاری استخراج‌شده می‌باشند. نتیجه مربوط به PSNR و MSE در جدول (۱) و جدول (۲) آمده‌است.

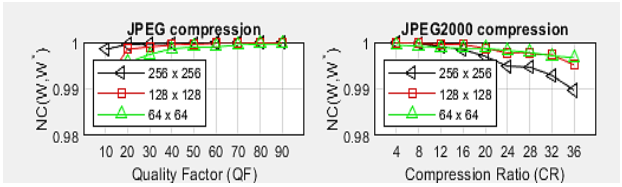



**شکل ۱۰: حمله Gaussian روی الگوریتم پیشنهادی DCT DWT-SVD**

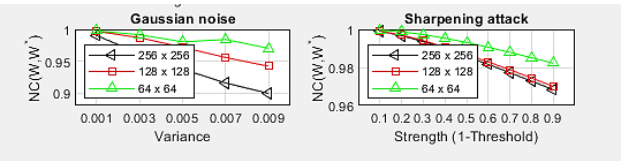



**شکل ۱۱: حمله Gaussian روی الگوریتم یشنهادی**

شکل (۱۱) و شکل (۱۲) نتایج آزمایش حمله Cropping (برش) به تصویر نهان‌نگاری‌شده توسط الگوریتم DWT-SVD و تصویر نهان‌نگاری‌شده توسط الگوریتم نهان‌نگاری مبتنی‌بر SVD چندگانه زارعی (۲۰۱۴) را نمایش‌می‌دهد. در حمله Cropping، تصویر نهان‌نگاری‌شده به اندازه ۵۰٪ برش‌خورده‌است. تصویر (a) تصویر نهان‌نگاری‌شده مورد حمله و (b) تصویر نهان‌نگاری استخراج‌شده‌اند. نتیجه مربوط به PSNR و MSE در جدول (۱) و جدول (۲) آمده‌است.




**شکل ۱۲: حمله Cropping روی الگوریتم پیشنهادی DCT DWT-SVD**




**شکل ۱۳:حمله Cropping روی الگوریتم بیشنهادی**

**جدول ۱: MSE و PSNR با استفاده از روش نهان‌نگاری پیشنهادی**

**DCT DWT-SVD**

| نوع حمله | PSNR | MSE |
|---|---|---|
| بدون حمله | 33.6102 | 28.5404 |
| Salt & Pepper (0.1) | 28.9174 | 84.0898 |
| Rotation (25deg) | 33.5010 | 29.2672 |
| Gaussian | 26.0719 | 161.9161 |
| Cropping | 33.0430 | 32.5219 |

**جدول ۲: MSE و PSNR با استفاده از روش نهان نگاری**

| نوع حمله | PSNR | MSE |
|---|---|---|
| بدون حمله | 34.8234 | 21.5846 |
| Salt & Pepper (0.1) | 33.7142 | 27.8650 |
| Rotation (25deg) | 32.7372 | 34.8950 |
| Gaussian | 34.1051 | 25.4668 |
| Cropping | 31.6102 | 46.5836 |

## ۴. نتیجه‌گیری

نهان نگاری یا استگانوگرافی هنر برقراری ارتباط پنهانی است و هدف آن پنهان‌کردن ارتباط با قراردادن پیام در یک رسانه پوششی است به گونه‌ای که کمترین تغییر قابل‌کشف را در آن ایجادنماید و نتوان موجودیت پیام پنهان شده در رسانه را حتی به‌صورت احتمالی آشکار-ساخت. در نهان‌نگاری تصویر، سیگنال نهان‌نگاری‌شده در حوزه مکانی یا یکی از حوزه‌های فرکانسی مثل تبدیل کسینوس گسسته، فوریه، و موجک و ... می‌تواند پنهان‌شود. تکنیک‌های نهان‌نگاری درحوزه تبدیل -در مقایسه با تکنیک‌های حوزه مکان - مقاومت بیشتری در مقابل حملات گوناگون از خود نشان‌می‌دهند، چون وقتی از تصویری تبدیل معکوس گرفته‌می‌شود، نهان‌نگاره به‌طور بی‌قاعده‌ای در طول تصویر پخش‌می‌شود، بنابراین خواندن و اصلاح آن برای نفوذگرها بسیار مشکل خواهدبود. با توجه به کارهای پیشین در این زمینه، در پژوهش حاضر قصدداشتیم الگوریتم‌های نهان‌نگاری در تصاویر دیجیتالی با استفاده از تجزیه مقدار منفرد را توسعه‌دهیم. برای این منظور از روش‌های نهان-نگاری ترکیبی شامل تجزیه مقدار منفرد و تبدیل موجک گسسته استفاده‌کرده‌ایم. هدف از این الگوریتم مخفی‌کردن پیام است. روش پیشنهادی با ترکیب تکنیک SVDوDCT و DWT باعث بهبود نهان-نگاری مبتنی‌بر DWT می‌شود. این الگوریتم از روش اعداد تصادفی در تصویر نهان‌نگاری و یک تصویر با متن معنی‌دار استفاده‌می‌کند. بنابراین کیفیت تصویر نهان‌نگاری استخراج‌شده عملکرد الگوریتم را تضمین‌می-کند. در روش پیشنهادی حمله‌کننده برای استخراج تصویر نهان‌نگاری، از نوع الگوریتم به‌کاررفته در فرآیند استگانوگرافی اطلاعی‌ندارد. الگوریتم‌های نهان‌نگاری و استخراج آن با استفاده از نرم‌افزار MATLAB 2016 پیاده‌سازی‌شدند. برای بررسی و ارزیابی روش پیشنهادشده، کیفیت بصری تصاویر نهان‌نگاری استخراج‌شده با اندازه‌گیری اوج نسبت سیگنال به نویز و میانگین مربع خطاها بررسی‌شده‌است. برای سنجش کارایی الگوریتم پیشنهادی با الگوریتم‌های قبلی مقایسه‌شده‌است. مقاومت تصویر نهان‌نگاری‌شده توسط این الگوریتم در مقایسه با سایر الگوریتم‌ها در برابر رایج‌ترین حملات مانند Salt & Pepper، Rotation، Gaussian و Cropping موردمطالعه‌قرارگرفته و برای مقایسه، از پارامترهایی مثل اوج نسبت سیگنال به نویز و میانگین مربع خطاها استفاده‌شده‌است. بررسی‌های تحلیلی روی تصویر نهان‌نگاری استخراج-شده، نشان‌می‌دهد که روش نهان‌نگاری در مقابل حملات Salt & Pepper با مقیاس ۰٫۱ از ۱٫۰ و در حمله گاوسی، به میزان ۰٫۰۱ توانمند و مقاوم و رایج بوده، تصویر نهان‌نگاری را به‌خوبی بازیابی می‌نماید؛ اما الگوریتم پیشنهادی ما در برابر این حملات ناتوان و ضعیف است. در مقابل الگوریتم پیشنهادی در برابر حملات دوران و برش عملکرد رضایت‌بخشی دارد ولی نهان‌نگاری مبتنی‌بر SVD چندگانه در برابر این دو حمله کمی ضعیف عمل‌کرده‌است.

## مراجع


[۱] شکرآمیز, خلیل و علیرضا نقش، ۱۳۹۶، *ذخیره و بازیابی دو سیگنال دیجیتال مجزای صوت در تصاویر به کمک کدهای دوبعدی مبتنی‌بر نهان‌نگاری*، سومین کنفرانس بین‌المللی بازشناسی الگو و تحلیل تصویر ایران، شهرکرد، دانشگاه شهرکرد- انجمن ماشین بینایی و پردازش تصویر ایران.

[۲] فرزادپور, فروغ و ابوالفضل اسفندی، ۱۳۹۶، *امن‌سازی اطلاعات کاربران در سیستم پردازش ابری*، کنفرانس بین‌المللی مهندسی و فن‌آوری اطلاعات، امارات- دبی، پژوهشکده فرهنگ و فن‌آوری پژوهشگاه فرهنگ و هنر.

[۳] عرب‌زاده, افسانه و علیرضا نقش، ۱۳۹۶، *مقاوم‌سازی تصویر دیجیتال قرآن نسبت به حمله برش با استفاده از تبدیل موجک گسسته مبتنی‌بر نهان‌نگاری*، سومین کنفرانس بین‌المللی بازشناسی الگو و تحلیل تصویر ایران، شهرکرد، دانشگاه شهرکرد- انجمن ماشین بینایی و پردازش تصویر ایران.

[۴] جلالی, آرش، ۱۳۹۶، *شناسایی الگو و نهان‌کاوی تصاویر با استفاده از نمایش تنک سریع در تصاویر حاوی اطلاعات به روش-S*

*UNIWARD*، سومین کنفرانس سالانه ملی مهندسی مکانیک و راهکارهای صنعتی، مشهد، مرکز علمی آموزشی و پژوهشی ارگ.
[۵] شکرآمیز, خلیل و علیرضا نقش، ۱۳۹۶، *ذخیره و بازیابی دو سیگنال دیجیتال مجزای صوت در تصاویر دیجیتال به کمک جدول سودوکو مبتنی‌بر نهان‌نگاری*، کنفرانس بین‌المللی تحقیقات بنیادین در مهندسی برق، تهران، دانشگاه ابرار.
[۶] وحیدی, ندا، ۱۳۹۶، *نهان‌نگاری مقاوم تصاویر دیجیتال مبتنی‌بر الگوریتم تبرید و جنگل تصادفی در دامنه تبدیل موجک گسسته*، دومین کنفرانس بین‌المللی پژوهش‌های دانش‌بنیان در مهندسی کامپیوتر و فن‌آوری اطلاعات، تهران، دانشگاه مجلسی.
[7] Q. Li, C. Yuan, Y.Z. Zong, (2007) "*Adaptive DWT-SVD domain image watermarking using human visual model*", 9th International Conference on Advanced Communication Technology (ICACT), pp. 1947–1951.,
[8] L. Liang, S. Qi, (2006) "*A new SVD-DWT composite watermarking*", Proceedings of IEEE International Conference on Signal Processing (ICSP).

## پی‌نوشت

1. Copyright
۲. Steganography
۳. watermark
4. Embedding
5. Robustness