مجله علمی پژوهشی «علوم و فناوری‌های پدافند نوین»
سال هشتم، شماره ۳، پاییز ۱۳۹۶؛ ص ۲۲۱-۲۱۳

تعیین سطح امنیت تصویر پوشانه نهان‌نگاری مبتنی بر منطق فازی

رضا اصفهانی[1*]، زین‌العابدین نوروزی[2]
۱- دانشجوی دکتری، ۲- استادیار، دانشگاه جامع امام حسین (ع)
(دریافت: ۹۵/۰۸/۰۷، پذیرش: ۹۵/۱۱/۲۴)

چکیده

یکی از مسائل مهم در سامانه‌های نهان‌نگاری، انتخاب پوشانه مناسب برای درج پیام محرمانه در آن است. از دیدگاه پدافند غیرعامل، قبل از عملیات نهان‌نگاری (اجرای درج پیام)، یک انتخاب مناسب پوشانه می‌تواند باعث افزایش کارایی عملکرد و کاهش خطا در این سامانه‌ها شود. در این مقاله یک روش برای آماده‌سازی پوشانه‌های تصویر با امنیت مناسب ارائه می‌شود. برای این منظور، برخی ویژگی‌های مهم تصویر مانند کنتراست و انرژی و نیز کاربرد منطق فازی با انتخاب سطح آستانه هریس در نظر گرفته می‌شود. ابتدا با استفاده از هر تصویر پوشانه، تصاویری با کنتراست‌های متفاوت و البته یک سطح آستانه هریس ثابت به‌دست می‌آید که برای استخراج ویژگی‌های ذکر شده از ماتریس‌های هم‌رخدادی سطوح خاکستری (GLCM) استفاده می‌شود. سپس با استفاده از منطق فازی، سطوح مختلف امنیتی برای تصاویر ارائه می‌شود. تصاویر با سطوح امنیتی مختلف را می‌توان در بانک‌های تصویر متفاوت ذخیره کرد. با توجه به شبیه‌سازی انجام شده، تصاویری که بر اساس روش پیشنهادی برای نهان‌نگاری انتخاب می‌شوند، دارای مقدار مناسب SSIM و PSNR هستند.

کلیدواژه‌ها: ماتریس‌های هم‌رخدادی، منطق فازی، آستانه هَریس، سطح امنیت تصویر، پوشانه نهان‌نگاری

Security Level Determination of Cover Image in Steganography Based on the Fuzzy Logic

R. Esfahani*, Z. Norozi
Imam Hossein University
(Received: 28/10/2016; Accepted: 12/02/2017)

Abstract

The selection of an appropriate cover to embedding a secret message is one of the main issues in the steganography. This leads to increasing the performance and decreasing the error from the point of view of passive defence. In this paper, preparation of a cover image with the suitable security level is described. For this porpose, some important features such as contrast, energy and the use of fuzzy logic with a selection threshold for Harris corners have been considered. Firstly, some images with different contrast were obtained but a fixed threshold for Harris corners from each cover image which extracting the features is done using Gray Levels Co-Occurrence Matrix (GLCM). Then, the security of images was graded using fuzzy logic. The images with different security levels can be stored in the different bank of images. According to the simulation which is done, selected images based on the proposed method, have an appropriate SSIM and PSNR in the steganography.

Keywords: Co-occurrence Matrix, Fuzzy Logic, Harris Threshold, Image Security Level, Cover of Steganography

*Corresponding Author E-mail: resfahani@ihu.ac.ir

۱. مقدمه

امنیت نهان‌نگاری تحت تأثیر مواردی چون نوع تصویر پوشانه، روش انتخاب محلی از پوشانه جهت اعمال تغییرات، نحوه درج پیام و تعداد تغییرات ناشی از درج است. نوع تصویر با بافت[1] پیچیده و انتخاب محلی از پوشانه مانند لبه‌های تصویر و یا حتی نقاط خاص[2] نزدیک لبه‌ها و گوشه‌ها جهت اعمال تغییرات، از معیارهایی است که بر روی ماتریس‌های هم‌رخدادی تعریف می‌شوند و تغییرات ناشی از درج پیام را حداقل می‌کنند و از این معیارها در این مقاله بهره گرفته شده است. در نهان‌نگاری موضوع انتخاب پوشانه مناسب، از این جهت از اهمیت ویژه‌ای برخوردار است که قبل از نهان‌نگاری، فرستنده پیام اطمینان حاصل کند که انتخاب پوشانه توسط خود فرستنده می‌تواند با سطح امنیتی مورد نظرش صورت گیرد. در پوشانه مناسب بین پارامترهای نرخ درج (ظرفیت)، امنیت و مقاومت تعادل مناسبی وجود دارد. موضوع مقالات برای انتخاب پوشانه مناسب در فرستنده، بیشتر از دیدگاه بافت تصویر (از جمله آنتروپی و همبستگی) و بصری ارائه شده است [۱ و ۲]. ولی در این مقاله روشی ارائه شده است که علاوه بر موارد فوق، معیارهای آماری نیز مورد نظر قرار گرفته است. بالاترین ظرفیت ممکن به شرط برقراری موازنه با امنیت در نهان‌نگاری، جزء اهداف طراحی الگوریتم است که در برخی گزارش‌ها مشهود است [۳]. ولی هیچ مقاله‌ای به موضوع سطح‌بندی امنیت پوشانه‌ها قبل از درج اطلاعات نپرداخته است. سطح‌بندی امنیت پوشانه‌ها، بر اساس بعضی ویژگی‌های پوشانه در این مقاله بیان شده که به کمک منطق فازی انجام شده است. استفاده از منطق فازی در نهان‌نگاری، در مقالات زیادی قابل مشاهده است مانند گزارشی که در خروجی سامانه استنتاج فازی، حساسیت لبه تصویر جهت درج اطلاعات نهان‌نگاری مطرح است [۴].

فضای عدم قطعیت منطق فازی بازه‌ای جهت تعریف شرایط و قوانین بیشتر را ایجاد می‌کند که در این مقاله تعریف سطوح مختلف امنیت پوشانه به کمک منطق فازی حاصل شده است. در بخش دوم، مفاهیم شامل منطق فازی، معیارهای سنجش، طبقه‌بند، آشکارساز هریس ارائه می‌شود. در بخش سوم روش پیشنهادی و در بخش چهارم نیز نتایج تجربی و شبیه‌سازی ارائه شده است. در ادامه، مفاهیم و تعاریفی که در این مقاله از آن‌ها بهره گرفته شده است، هر یک به طور خلاصه ارائه می‌شود.

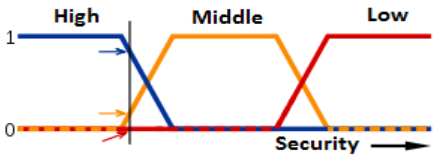
۱-۱. منطق فازی

با توجه به پیشرفت فناوری و انقلابی که در صنعت امنیت فضای تبادل اطلاعات رخ داده است، اهمیت تخمین اطلاعات یکی از مواردی است که در پیشگیری از حوادث و یا سرعت تصمیم‌گیری و بالطبع در کاهش یا افزایش پارامترهایی مانند امنیت نقش به سزایی دارد. در نهان‌نگاری، امنیت یکی از پارامترهای مهم به شمار می‌رود. در این مقاله روشی بر مبنای کنترل فازی پیشنهاد شده است که نه تنها امنیت پوشانه قبل از نهان‌نگاری تخمین زده می‌شود، بلکه سطح امنیت آن نیز بر اساس طبقه‌بندی که پیشنهاد شده، برآورد می‌گردد.

با توجه به بهره‌گیری از کنترل فازی در این مقاله لازم است تا گذری اجمالی به مقدمات و مفاهیم آن ارائه گردد. منطق فازی از منطق ارزش‌های "صفر و یک" نرم‌افزارهای کلاسیک فراتر رفته و درگاهی جدید برای دنیای علوم نرم‌افزاری و رایانه‌ها می‌گشاید، زیرا فضای شناور و نامحدود بین اعداد صفر و یک را نیز در منطق و استدلال‌های خود به‌کار می‌گیرد [۱ و ۴]. منطق فازی از جمله منطق‌های چند ارزشی بوده و بر نظریه مجموعه‌های عدم قطعیتی یا همان مجموعه‌های فازی تکیه می‌کند. مجموعه‌های فازی خود از تعمیم و گسترش مجموعه‌های قطعیتی به صورتی طبیعی حاصل می‌آیند. در حالت مجموعه‌های قطعی[3]، تابع عضویت[4] فقط دو مقدار یک و صفر در بُرد خود دارد. بنابراین:

$$\mu_A(x)=\begin{cases}1 & \text{اگر} \quad x\in A\\ 0 & \text{اگر} \quad x\notin A\end{cases} \qquad (۱)$$

که در اینجا، $\mu_A(x)$ تابع عضویت عنصر x در مجموعه قطعی A است. یک تابع عضویت یک منحنی است که نشان می‌دهد هر نقطه از فضای ورودی چگونه به یک مقدار عضویت (درجه عضویت) بین ۰ و ۱ نگاشته می‌شود. برد تابع عضویت از $[-۱,۱]$ در مورد مجموعه‌های قطعیتی به بازه بسته $\{۰,۱\}$ برای مجموعه‌های فازی تبدیل می‌شود. درجه عضویت $\mu_A(x)$ بیانگر میزان عضویت عنصر x به مجموعه فازی $\tilde{A}$ است. توابع عضویتی که در مجموعه‌های فازی استفاده می‌شود عبارتند از: تابع مثلثی، تابع ذوزنقه‌ای، تابع سیگما، تابع زنگوله‌ای، تابع S-شکل، تابع گوسی، تابع سیگموید و تابع چپ-راست. در این مقاله از تابع گوسی استفاده شده است. به عنوان مثال: می‌توان همانند شکل (۱) توابع عضویت برای توصیف سطح امنیت یک طرح نهان‌نگاری فرضی را در نظر گرفت.



شکل ۱. سطح امنیت یک طرح نهان‌نگاری فرضی

[1] Texture
[2] Feature-Points
[3] Crisp Sets
[4] Member Function

درستی هر چیزی در منطق فازی با یک مقدار به عنوان درجه برگردانده می‌شود که به آن قوانین فازی[1] اطلاق می‌شود و به کمک عملگرهای منطقی اجرا می‌شود. OR در نظریه مجموعه‌ها معادل اجتماع[2] مجموعه‌ها و در منطق فازی بیشینه[3] عضویت مجموعه‌ها است. AND در نظریه مجموعه‌ها معادل اشتراک[4] مجموعه‌ها و در منطق فازی کمینه[5] عضویت مجموعه‌ها است. NOT در نظریه مجموعه‌ها معادل متمم[6] یک مجموعه و در منطق فازی اختلاف عضویت از مقدار یک است.

و اما کنترل فازی[7]؛ کنترل از دیدگاه مهندسی به معنی حفظ پایداری[8] یک سامانه و تضمین عملکرد[9] مطلوب آن است. کنترل فازی روشی است که بر اساس منطق فازی، سعی می‌کند دو عامل پایداری و عملکرد مطلوب سامانه را تأمین می‌کند. نکته مهم آن است که سامانه‌هایی که طراحی می‌شوند، ورودی و خروجی قطعیتی دارند. این در حالی است که منطق فازی با متغیرهای فازی سر و کار دارد. برای کنترل فازی یک سامانه با پارامترهای قطعی با منطق فازی ابتدا ورودی‌های سامانه از حالت قطعیت تبدیل به حالت عدم قطعیت و یا به عبارتی متغیرهای فازی می‌شوند. این عمل فازی کردن[10] نام دارد. سپس می‌توان روی مجموعه‌های حاصل از فازی کردن قوانین فازی را اعمال کرد که خروجی باز هم فازی شده است. حال باید این خروجی‌های فازی را به خروجی‌های قطعیتی تبدیل کرد که این عمل را غیر فازی کردن[11] می‌گویند. الگوریتم‌های مختلفی برای اعمال قوانین فازی جهت کنترل یک سامانه وجود دارند که سامانه استنتاج فازی (FIS) [12] نامیده می‌شوند. دو سامانه استنتاج فازی معروف عبارتند از:

ممدانی[13]: در این روش برای غیر فازی کردن، باید تابع عضویت برای خروجی را داشته باشید.

ساگنو[14]: در این روش برای غیر فازی کردن به جای تابع عضویت، از یک تابع چندجمله‌ای جبری استفاده می‌شود که متغیرهای این تابع، ورودی‌های مسئله هستند.

روش ممدانی تعریف بهتری از خروجی ارائه می‌دهد ولی محاسبه مرکز ثقل نمودار کار دشواری است که باعث می‌شود بازدهی محاسباتی آن نسبت به روش ساگنو کاهش یابد. در مواردی که سرعت بر دقت ارجحیت دارد، الگوریتم ساگنو مناسب‌تر است. در این مقاله از سامانه استنتاج فازی ممدانی استفاده شده است. پنج مرحله جهت تحلیل فرایند استنتاج فازی مورد نیاز هستند. مراحل به ترتیب عبارتند از: ۱) فازی‌سازی متغیرهای ورودی‌ها؛ ۲) اعمال عملگرهای فازی؛ ۳) محاسبه خروجی از ورودی؛ ۴) اجتماع تمام خروجی‌ها؛ ۵) غیر فازی کردن.

۱-۲. پارامترها و معیارهای سنجش

در این قسمت مفاهیم پارامترها و معیارهای مورد نیاز برای روش پیشنهادی مورد استفاده در نهان‌نگاری مطرح شده است.

• شفافیت، تمایزناپذیری و امنیت: شفافیت سامانه، بیان کننده عدم تفاوت محسوس قبل و بعد از درج پیام در پوشانه است و هدف آن نامحسوس کردن پیام است. در حقیقت امنیت یک سامانه، در مخفی‌سازی شفافیت، نهفته است و هر چقدر که شباهت پوشانه در هر دو حالت پاک و آلوده (حاوی پیام) وجود داشته باشد، امنیت این سامانه در سطح بالاتری قرار دارد. با موضوع "دستاورد مهاجم در تمایز"[15] می‌توان تمایزناپذیری[16] قبل و بعد از درج پیام در پوشانه را مورد بررسی قرار داد [۴].

$$\mathrm{Adv}_{C,S}(W) =: \Pr[W^C = 1] - \Pr[W^S = 1] \qquad (۲)$$

$\mathrm{Adv}_{C,S}(W)$ دستاورد مهاجم در تمایز سیگنال قبل از درج پیام و سیگنال بعد از درج پیام است.

در یک گزارش [۵]، تمایزناپذیری هم‌ارز با امنیت در نظر گرفته شده است. امنیت نشان دهنده میزان محسوس بودن آماری اثر اعوجاج ناشی از درج پیام است. در بسیاری از پژوهش‌ها، یک سامانه نهان‌نگاری را ε-امن[17] می‌نامند اگر آنتروپی آنتروپی نسبی میان توزیع پوشانه و سیگنال نهان نگاشته (سیگنالی حاوی اطلاعات نهان شده در آن) حداکثر برابر ε باشد. هر گاه سیگنال C را قبل از درج پیام و سیگنال S را بعد از درج پیام در نظر گرفت، حال اگر مهاجم W بتواند فعالیتی بر روی C انجام دهد که احتمال آن $\Pr[W^C = 1]$ باشد و همچنین اگر مهاجم W بتواند فعالیتی بر روی S انجام دهد که احتمال آن $\Pr[W^S = 1]$ باشد و اگر رابطه (۳) برقرار باشد که ε مقدار

[1] Fuzzy Rules
[2] Union
[3] Conjunction
[4] Intersection
[5] Disjunction
[6] Complement
[7] Fuzzy Control
[8] Stability
[9] Performance
[10] Fuzzification
[11] Defuzzification
[12] Fuzzy Inference System (FIS)
[13] Mamdani
[14] Sugeno

[15] Advantage of a Warden Performing Distinguishable
[16] Indistinguishability
[17] Secure-ε

بسیار کوچکی است، آنگاه سیگنال C از سیگنال S غیر قابل تمایز است. هر گاه $\varepsilon \to 0$ باشد تا جایی که $\varepsilon \cong 0$ شود آنگاه تمایزناپذیری کامل و در نتیجه امنیت کامل را خواهید داشت:

$$|\Pr[W^C=1]-\Pr[W^S=1]|<\varepsilon \underset{\varepsilon\cong 0}{\Longrightarrow} \Pr[W^C=1]=\Pr[W^S=1] \quad (۳)$$

همان‌طور که بیان شد یک روش نهان‌نگاری را کاملاً امن نامیده می‌شود اگر ε=0 باشد. چنین تعریفی مشکلات زیادی را دربر دارد. چنین تعریفی از امنیت برای دنباله بیت‌های تصادفی مناسب است. ولی برای پوشانه‌هایی مانند تصاویر طبیعی این تعریف کارآمد نیست. زیرا در چنین سیگنال‌هایی وابستگی بالایی میان نمونه‌های سیگنال وجود دارد و از همین وابستگی‌ها حتی در حالت حفظ توزیع می‌توان برای طراحی نهان‌کاو مناسب جهت ارزیابی نهان‌نگاری استفاده کرد. دو معیار *SSIM* و *PSNR* سنجه‌های مناسبی برای شفافیت نهان‌نگاری هستند که درنهایت می‌توان جهت ارزیابی روش پیشنهادی از آن‌ها بهره جست. این دو معیار شفافیت را بر اساس تمایزناپذیری مورد ارزیابی قرار می‌دهند.

- *معیار SSIM :* معیارهایی جهت در نظر گرفتن مشابهت‌های ساختاری ارائه شده‌اند که شناخته شده‌ترین آن‌ها SSIM[1] نام دارد که در واقع یکی از معیارهای شفافیت به شمار می‌رود [۶] و در این مقاله برای ارزیابی و مقایسه نهایی از آن استفاده شده است. به طور خلاصه در این معیار، رابطه (۴) برای تشخیص میزان تشابه دو تصویر x و y استفاده شده است.

$$SSIM=\left(\frac{\sigma_{xy}}{\sigma_x\sigma_y}\right)^{\alpha}.\left(\frac{2\bar{x}\bar{y}}{(\bar{x})^2+(\bar{y})^2}\right)^{\beta}.\left(\frac{2\sigma_x\sigma_y}{\sigma_x^{\,2}+\sigma_y^{\,2}}\right)^{\gamma} \quad (۴)$$

که در آن:

$$\bar{x}=\frac{1}{N}\sum_{i=1}^{N}x_i \qquad \bar{y}=\frac{1}{N}\sum_{i=1}^{N}y_i$$
$$\sigma_x^{\,2}=\frac{1}{N-1}\sum_{i=1}^{N}(x_i-\bar{x})^2 \qquad \sigma_y^{\,2}=\frac{1}{N-1}\sum_{i=1}^{N}(y_i-\bar{y})^2 \quad (۵)$$
$$\sigma_{xy}=\frac{1}{N-1}\sum_{i=1}^{N}(x_i-\bar{x})(y_i-\bar{y})$$

مقدار SSIM که در رابطه (۴) با SoI_{stg} نشان داده شده است، در بازه $[-۱,۱]$ محدود است که مقدار ۱ نشانگر بیشینه شباهت بین دو تصویر است.

$$SSIM = SoI_{stg}(C_{n\times m}, M_k) \quad (۶)$$
$$\rightarrow \quad -1 \le SoI_{stg}(C_{n\times m}, M_k) \le 1$$
$$\text{اگر } Pr[W^C=1]=Pr[W^S=1] \Longrightarrow SoI_{Stg}(C_{n\times m}, M_k) \xrightarrow{Distinguishable} Perfect\ Secure$$

[1] Structural Similarity Measure

SSIM یا $SoI_{stg}(C_{n\times m}, M_k)$ [2] به معنی مقدار شفافیت تصویر حاوی اطلاعات نهان‌نگاری شده است که با توجه به تفسیر شفافیت به تمایزناپذیری، به سطح امنیت خواهید رسید. $C_{n\times m}$ تصویر پوشانه به ابعاد $n\times m$ و M_k به معنی پیام محرمانه به طول k است. همچنین با توجه به رابطه (۳) می‌توان *"امن کامل"* را در اینجا به شکل فوق مشاهده کرد.

همان‌گونه که در رابطه (۴) مشخص است این مدل هر گونه تغییر در تصویر را ناشی از سه پارامتر مختلف می‌داند: کاهش همبستگی بین دو تصویر، تغییرات روشنایی تصویر و تغییرات در اختلاف رنگ سطوح[3] با یکدیگر. مقادیر α, β, γ همگی بزرگ‌تر از صفر و نمایان‌گر نقش هر پارامتر در معیار پیشنهادی است و معمولاً هر سه برابر یک فرض می‌شوند.

جزء اول در رابطه (۴) بیانگر ضریب همبستگی بین دو تصویر x و y بوده و میزان وابستگی خطی بین دو تصویر را نمایش می‌دهد. این جزء همواره مقداری در بازه $[-۱,۱]$ دارد. جزء دوم در رابطه (۴) با مقداری در بازه $[۰,۱]$ نشان می‌دهد چه میزان متوسط روشنایی دو تصویر به هم نزدیک است و زمانی ۱ می‌شود که $x = y$ جزء سوم در بازه $[۰,۱]$ تغییر کرده و تخمینی برای تمایز رنگ‌ها در x و y است و حداکثر مقدار آن زمانی پیش می‌آید که $\sigma_x = \sigma_y$.

- معیار PSNR[4]: این معیار، «نسبت بیشینه سیگنال به نویز» است. این مقیاس نشان دهنده میزان نویز اضافه شده به سیگنال در اثر درج داده نهان به آن است. اگر چه این پارامتر دقیقاً مطابق با خاصیت نامریی بودن بصری داده نهان درج شده در تصویر نیست، اما رابطه جبری مناسبی برای بهینگی پنهان شدن اطلاعات در پوشانه ارائه می‌دهد. این معیار به صورت رابطه (۷) تعریف می‌شود:

$$PSNR(f,w)=10\log_{10}\left[\frac{\max_{\forall(m,n)} f^2(m,n)}{\frac{1}{N_f}\sum_{\forall(m,n)}(f_w(m,n)-f(m,n))^2}\right] \quad (۷)$$

رابطه (۷) میزان «نسبت بیشینه سیگنال به نویز» را در واحد دسی‌بل[5] ارائه می‌نماید. در این رابطه، f سیگنال تصویر اولیه، w داده نهان درج شده، f_w سیگنال تصویر درج شده، (m , n) اندیس پیکسل‌های تصاویر و N_f تعداد پیکسل‌های موجود در تصاویر f و f_w را نشان می‌دهند. هر چه مقدار این پارامتر بیشتر باشد، توانایی

[2] SoI_{stg} (Security of Image – Steg.)
[3] Contrast
[4] Peak Signal To Noise Ratio
[5] dB

روش در پنهان نمودن داده نهان در تصویر بیشتر است. غالباً مقادیر بالای ۳۵ دسی‌بل از نظر درک نشدن تغییرات توسط انسان، مقادیر قابل قبولی برای این پارامتر محسوب می‌شوند. مقدار رابطه $\max_{\forall(m,n)} f^2(m,n)$ را می‌توان ۲۵۵ در نظر گرفت [۷].

۱-۳. آشکارساز هریس

مرزهای اشیاء معمولاً باعث ایجاد تغییرات در شدت پیکسل‌ها می‌گردند. اصولاً از آشکارسازی لبه جهت شناسایی این تغییرات استفاده می‌شود. یکی از خواص لبه‌ها حساسیت کمتر آن‌ها به تغییرات روشنایی در مقایسه با ویژگی‌های رنگ است و به همین خاطر درج اطلاعات نهان‌نگاری در لبه‌های تصویر مناسب‌تر به نظر می‌رسد [۸]. الگوریتم‌هایی که به ردیابی مرزهای اشیاء می‌پردازند، لبه‌ها را به عنوان یک ویژگی و نماینده شیء در نظر می‌گیرند. در نزدیک بعضی از گوشه‌ها و لبه‌های تصویر، نقاط برجسته‌ای قرار دارند که به نقاط خاص معروف هستند. آشکارسازهای نقاط خاص، نقاط برجسته را در تصویر پیدا می‌کنند. معمولاً این نقاط، نزدیک گوشه‌ها و لبه‌های تصویر قرار دارند. آشکارساز گوشه هریس، یکی از آشکارسازهای نقاط خاص است که برای بازسازی سه بعدی مورد استفاده قرار می‌گیرد [۹]. آشکارساز گوشه هریس ابتدا گرادیان عمودی و افقی تصویر را محاسبه می‌کند (G_x, G_y) و سپس دو گرادیان تصویر توسط یک فیلتر پایین گذر، فیلتر می‌شوند (G'_x, G'_y). بنابراین ماتریس M برای هر پیکسل شکل می‌گیرد [۱۰].

$$M(i,j)=\begin{bmatrix}\sum_{m,n}(G'_x(m.n))^2 & \sum_{m,n}G'_x(m.n)G'_y(m.n)\\ \sum_{m,n}G'_x(m.n)G'_y(m.n) & \sum_{m,n}(G'_y(m.n))^2\end{bmatrix} \quad (۸)$$

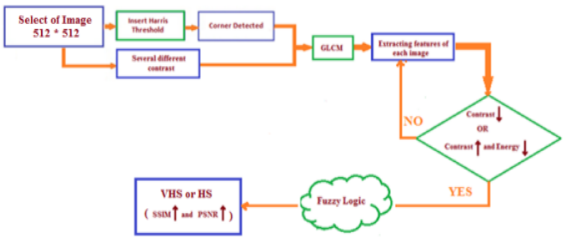
که در آن، (m,n) تمام پیکسل‌های یک پنجره به مرکزیت پیکسل (i,j) را نمایش می‌دهد. با استفاده از $M(i,j)$ خروجی آشکارساز گوشه هریس برای هر پیکسل بر مبنای ردیابی[1] و دترمینان M است [۱۱].

$$H(i,j)=\det(M(i,j))-k.trace(M(i,j))^2 \quad (۹)$$

که در آن، k یک ثابت دلخواه است. استخراج نقاط خاص با استفاده از جستجوی $H(i,j)$ بزرگ‌تر از یک سطح آستانه به‌دست می‌آید.

۲. روش پیشنهادی

با توجه به رشد و کارآمد شدن نهان‌کاوها، انتخاب یک رسانه پوششی مناسب با یک روند علمی می‌تواند در جهت ارتقاء روش‌های نهان‌نگاری و به طور مشابه مقاوم شدن طرح در مقابل نهان‌کاوهای متفاوت، مفید باشد. در ادامه با استفاده از کنتراست، انرژی، منطق فازی، تصویر پوشانه با امنیت مطلوب جهت جاگذری اطلاعات حاصل می‌شود. چگونگی روش پیشنهادی در شکل (۲) نمایش داده شده است. چنانچه مقادیر مربوط به رنگ‌های به‌کار رفته در یک تصویر را به کمک دستور imhist در متلب مشاهده کنید، ممکن است که بخشی از رنگ‌ها، به مقدار زیاد، در تصویر به‌کار رفته و بخشی دیگر، کمتر در تصویر باشند. افزایش کنتراست، باعث می‌شود که میزان به‌کار رفتن رنگ‌های مختلف، به هم نزدیک‌تر شوند و دیگر تفاوت زیادی که ذکر شد، وجود نداشته باشد. یکی از کارهای مهمی که در پردازش تصویر انجام می‌شود، بالا بردن دقت عکس به منظور دید و بررسی چشمی دقیق‌تر است. روش‌های بسیاری برای رسیدن به این هدف وجود دارند ولی مهم‌ترین آن‌ها، کنتراست تصویر و عملیات فیلتر کردن است. در ابتدا تصاویر مختلفی از یک تصویر با کنتراست‌های مختلف توسط دستورات histeq، imadjust، adapthisteq در نرم‌افزار متلب تولید شده و یک حالت هم original در نظر گرفته می‌شود و از بین آن‌ها تصویری مناسب استخراج می‌شود.



شکل ۲. چگونگی روش پیشنهادی: انتخاب تصویر پوشانه دارای شفافیت مناسب به کمک معیارهای کنتراست و انرژی

در ابتدا یک تصویر پوشانه انتخاب کرده و سپس از آن تصویر، تصاویری با یک سطح آستانه هریس ثابت و کنتراست‌های متفاوت ساخته شده و ویژگی‌های تصاویر به کمک ماتریس‌های هم‌رخدادی، استخراج می‌شود. سپس چند تصویر بر اساس ویژگی کنتراست و انرژی به کمک منطق فازی به صورتی مرتب می‌گردد که بالاترین $SSIM$ و $PSNR$ را در هنگام نهان‌نگاری در نقاط برجسته نزدیک بعضی از گوشه‌ها و لبه‌های تصویر (نقاط خاص حاصل از آشکارساز هریس) دارا است و می‌توان با یک سطح آستانه‌ای از کنتراست و انرژی، تصاویر مورد نظر را انتخاب کرد. طبق جدول (۱- الف) بازه کنتراست بین ۰ تا ۴۹ است. با توجه به وظیفه اصلی کنتراست که وضوح تصویر و ایجاد شفافیت است، بررسی کنتراست در نهان‌نگاری از اهمیت زیادی برخوردار است زیرا کنتراست بالا به تنهایی، به معنی وضوح بالای تصویر است که حفظ شفافیت و تمایزناپذیری در آن سخت است و با کوچک‌ترین تغییر (درج)، به شکل بصری و یا آماری رؤیت می‌شود. پس کنتراست پایین برای یک تصویر پوشانه جهت نهان‌نگاری مناسب است. البته در صورتی که کنتراست بالا ولی انرژی پایین (طبق جدول (۱- ب) بازه انرژی بین ۰ تا ۱ است) باشد نیز تغییرات (درج) را نشان نمی‌دهد. کنتراست توسط رابطه (۱۰) تعریف می‌شود که به کمک

[1] Trace

ماتریس‌های هم‌رخدادی سطوح خاکستری (GLCM)[1] حاصل شده است. i و j سطوح روشنایی دو پیکسل مجاور و $p(i,j)$ هیستوگرام دو بعدی در GLCM است. در واقع $\sum_i \sum_j p(i,j)$ درصد زوج پیکسل‌هایی است که سطح روشنایی آن‌ها به اندازه $(i\text{-}j)$ با یکدیگر اختلاف دارند. هر چه $|i\text{-}j|$ کوچک‌تر باشد، کنتراست نیز کوچک‌تر است ($c \downarrow$) :

$$C = \sum_i \sum_j p(i,j)(i-j)^2 \ , 0 < p(i,j) \leq 1 \underset{|i-j|<0}{\Longrightarrow} c \downarrow \quad (۱۰)$$

حال اگر در بعضی از پیکسل‌های مجاور با سطح روشنایی نزدیک به هم، درج اطلاعات به شکل LSB صورت گیرد به خاطر اختلاف کم سطح روشنایی پیکسل‌های مجاور، قابل تمایز نیست و در مجموع اگر c_C کنتراست تصویر پوشانه C (قبل از درج پیام) و c_S کنتراست تصویر گنجانه S (بعد از درج پیام) باشد آنگاه با توجه به رابطه (۳) دارید:

$$Adv_{C,S}(W^C) =: \Pr[W^{C_C} = 1] - \Pr[W^{C_S} = 1] = \varepsilon_1 \cong 0 \Longrightarrow SoI_{clr} \uparrow \quad (۱۱)$$

رابطه (۱۱) نشان می‌دهد در حالتی که تصویر پاک (قبل از درج پیام) دارای کنتراست پایین باشد، "دستاورد مهاجم در تمایز" به سمت تمایزناپذیری منتج شده است. عبارت SoI_{clr}[2] به معنی سطح امنیت تصویر پاک (قبل از درج پیام) است و علامت ↑ نشان دهنده امنیت بالا است. ولی مقدار p(i,j) نیز به لحاظ بزرگ و کوچک بودن، تأثیرگذار است. سطوح امنیت با توجه به کمینه مقدار ۳۵ دسی‌بل برای PSNR و بیشینه مقدار ۱ برای SSIM تعیین شده است. برای مشاهده مقدار $p(i,j)$ بهتر است معیار انرژی (E) را مورد بررسی قرار داد که توسط ماتریس‌های هم‌رخدادی سطوح خاکستری حاصل می‌شود (رابطه (۱۲)). انرژی، نَرمی تصویر را مشخص می‌کند که اگر تمام پیکسل‌ها دارای سطح روشنایی یکسان k باشند، با توجه به $p(k,k)=1$ آنگاه $E=1$ می‌شود. هر چه ناحیه نرم‌تر باشد توزیع یکنواخت‌تر و مقدار E کمتر می‌شود و کوچک بودن E هم یعنی $p(i,j)$ کوچک است.

$$E = \sum_i \sum_j (p(i,j))^2 \underset{p(i,j)\downarrow}{\Longrightarrow} E \downarrow \quad (۱۲)$$

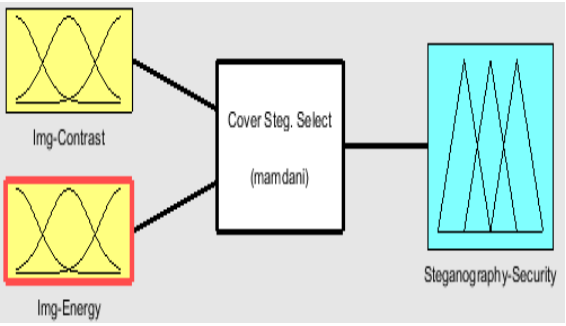
حال هر چه $|i\text{-}j|$ بزرگ‌تر باشد، کنتراست نیز بزرگ‌تر می‌شود ($c \uparrow$):

$$C = \sum_i \sum_j p(i,j)(i-j)^2 \underset{|i-j|\gg 0}{\Longrightarrow} c \uparrow \quad (۱۳)$$

اما اگر در حالت $c \uparrow$ مقدار $p(i,j)$ کوچک باشد که این مقدار را با مشاهده و رصد E می‌توان به‌دست آورد ($E \downarrow$)، آنگاه می‌توان گفت که تصویر پوشانه تصویری نرم و دارای توزیع یکنواخت و دارای اختلاف سطح روشنایی پیکسل‌های مجاور زیاد است. حال اگر در چنین تصویر درج صورت گیرد نیز غیر قابل تمایز است:

$$\text{اگر } c_C \uparrow \text{ و } E_C \downarrow \therefore \Pr[W^{(C_C,\ E_C)} = 1] \cong \Pr[W^{(C_S,\ E_S)} = 1] \Longrightarrow Adv_{C,S}(W^{(C,E)}) =: \Pr[W^{(C_C,\ E_C)} = 1] - \Pr[W^{(C_S,\ E_S)} = 1] = \varepsilon_2 \cong 0 \Longrightarrow SoI_{clr} \uparrow \quad (۱۴)$$

که در آن، E_C انرژی تصویر پوشانه C (قبل از درج پیام) و E_S انرژی تصویر پوشانه S (بعد از درج پیام) است. با توجه به اینکه در حالت حدی ε_1 در رابطه (۱۱) و ε_2 در رابطه (۱۴) هر دو به سمت صفر میل می‌کنند و $\varepsilon_1 < \varepsilon_2$ برقرار است، توسط منطق فازی وزن‌های متفاوتی به آن‌ها نسبت داده شده است که با توجه به امنیت مورد انتظار می‌توان از رابطه (۱۱) یا رابطه (۱۴) استفاده کرد. رابطه (۱۱) پوشانه‌ای با امنیت Very High Security و نتیجه رابطه (۱۴) پوشانه‌ای با امنیت High Security است. در روش‌های مرسوم ارزیابی امنیتی مانند *SSIM*، بر روی پوشانه ابتدا نهان‌نگاری انجام شده سپس ارزیابی صورت می‌گیرد. به علاوه در این روش، فقط یک مقدار عددی استخراج می‌شود که باید آن مقدار را با مقایسه‌هایی که صورت می‌گیرد تفسیر کرد، در حالی که در روش پیشنهادی امکان تخمین سطح امنیت قبل از نهان‌نگاری امکان پذیر است. اگر یک تصویر پوشانه با کنتراست پایین و یا کنتراست بالا و انرژی پایین تنظیم شود، شفافیت آن حفظ می‌شود و احتمال وجود پیام محرمانه در نهان‌کاوی[3] (موفقیت تلاش مهاجم در شنود) بسیار پایین است. پس دو پارامتر کنتراست و انرژی تصویر پوشانه به عنوان دو آرگومان ورودی جهت تعیین سطح امنیت در نظر گرفته می‌شوند. مطابق شکل (۳) در روش پیشنهادی، برای سامانه استنتاج فازی دو نوع ورودی در نظر گرفته شده است:



شکل ۳. سامانه استنتاج فازی با دو ورودی کنتراست و انرژی

اولین ورودی سامانه استنتاج فازی، کنتراست در بازه $0 \leq Cnt \leq (S-1)^2$ که S اندازه ماتریس‌های هم‌رخدادی سطوح خاکستری با مقدار $S=8$ است و ورودی دوم سامانه استنتاج فازی در این روش پیشنهادی، انرژی در بازه $0 \leq E \leq 1$ است. خروجی سامانه استنتاج فازی هم سطح امنیت تصویر پوشانه (تصویر پاک) است و پنج سطح در بازه $0 \leq Sec \leq 1$

[1] Gray Level Co-occurrence Matrix

[2] SoI_{clr} (Security of Image - Clear)

[3] Steganalysis

برای آن در نظر گرفته شده است که البته می‌توان تعداد خروجی را بیشتر یا کمتر در نظر گرفت.

همان‌طور که در ستون آخر جدول (۱- ج) مشاهده می‌شود احتمال هر یک از خروجی‌ها با توجه به قوانین استنتاج حاصل از نخبگی که شامل ۲۰ قانون بوده، حاصل شده است (شکل (۴)). به عنوان مثال با توجه به جدول (۱- ج) احتمال سطح VHS[1] در این روش، با توجه به تعداد VHSهای احصاء شده از ۲۰ قانون استنتاج به شکل رابطه (۱۵) محاسبه شده است:

$$\Pr[SoI_{clr}(C_{n\times m}, M_k)] = \Pr[VHS] = \frac{4}{20} \qquad (۱۵)$$

که در آن، احتمال رویداد سطح امنیت تصویر پاک با وزن VHS، با قوانین استنتاج شکل (۴) برابر با $\frac{4}{20}$ است.

در شکل (۵)، گراف تخمین امنیت نهان‌نگاری بر اساس ورودی‌های کنتراست و انرژی نمایش داده شده است. با توجه به جدول (۱- ج) تصاویر با کنتراست و انرژی مناسب که دارای امنیت بالا (VHS و HS[2]) هستند برای بانک تصاویر پوشانه انتخاب می‌شوند.

جدول ۱. ورودی‌ها و خروجی سامانه استنتاج فازی؛ الف) ورودی اول: سطوح کنتراست تصویر پوشانه؛ ب) ورودی دوم: سطوح انرژی تصویر پوشانه؛ ج) خروجی: سطوح کنتراست تصویر پوشانه

No	Contrast Weight	Contrast Range	Summary
1	Very High Contrast	$22.7 < Cnt \leq 49$	VHC
2	High Contrast	$9.5 < Cnt \leq 22.7$	HC
3	Middle High Contrast	$4.7 < Cnt \leq 9.5$	MHC
4	Middle Low Contrast	$2.8 < Cnt \leq 4.7$	MLC
5	Low Contrast	$1.2 < Cnt \leq 2.8$	LC
6	Poor Contrast	$0 < Cnt \leq 1.2$	PC

(الف)

No	Energy Weight	Energy Range	Summary
1	Very High Energy	$0.15 < E \leq 1$	VHE
2	High Energy	$0.06 < E \leq 0.15$	HE
3	Middle High Energy	$0.04 < E \leq 0.06$	MHE
4	Middle Low Energy	$0.01 < E \leq 0.04$	MLE
5	Low Energy	$0.005 < E \leq 0.01$	LE
6	Very Low Energy	$0 < E \leq 0.005$	VLE

(ب)

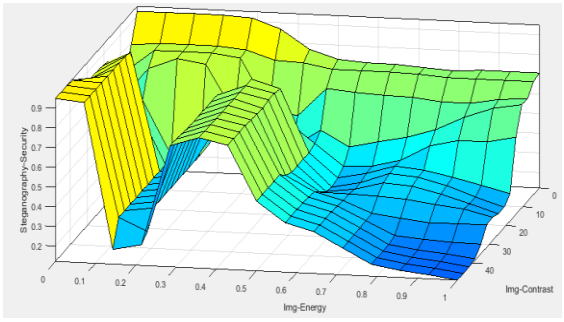
No	Security Weight	Security Range	Summary	Pr.
1	Very High Security	$0.8 < Sec \leq 1$	VHS	4/20
2	High Security	$0.5 < Sec \leq 0.8$	HS	6/20
3	Middle Security	$0.1 < Sec \leq 0.5$	MS	3/20
4	Low Security	$0.07 < Sec \leq 0.1$	LS	3/20
5	Poor Security	$0 < Sec \leq 0.07$	PS	4/20

(ج)

[1] Very High Security
[2] High Security

1. If (Img-Contrast is PC) then (Steganography-Security is VHS) (1)
2. If (Img-Contrast is LC) then (Steganography-Security is HS) (1)
3. If (Img-Contrast is MLC) then (Steganography-Security is HS) (1)
4. If (Img-Contrast is VHC) and (Img-Energy is LE) then (Steganography-Security is VHS) (1)
5. If (Img-Contrast is VHC) and (Img-Energy is VLE) then (Steganography-Security is VHS) (1)
6. If (Img-Contrast is VHC) and (Img-Energy is MLE) then (Steganography-Security is HS) (1)
7. If (Img-Contrast is VHC) and (Img-Energy is MHE) then (Steganography-Security is MS) (1)
8. If (Img-Contrast is VHC) and (Img-Energy is HE) then (Steganography-Security is LS) (1)
9. If (Img-Contrast is VHC) and (Img-Energy is VHE) then (Steganography-Security is PS) (1)
10. If (Img-Contrast is HC) and (Img-Energy is VLE) then (Steganography-Security is VHS) (1)
11. If (Img-Contrast is HC) and (Img-Energy is MLE) then (Steganography-Security is HS) (1)
12. If (Img-Contrast is HC) and (Img-Energy is LE) then (Steganography-Security is HS) (1)
13. If (Img-Contrast is HC) and (Img-Energy is HE) then (Steganography-Security is MS) (1)
14. If (Img-Contrast is HC) and (Img-Energy is MHE) then (Steganography-Security is LS) (1)
15. If (Img-Contrast is HC) and (Img-Energy is VHE) then (Steganography-Security is PS) (1)
16. If (Img-Contrast is MHC) and (Img-Energy is VHE) then (Steganography-Security is HS) (1)
17. If (Img-Contrast is MHC) and (Img-Energy is HE) then (Steganography-Security is MS) (1)
18. If (Img-Contrast is MHC) and (Img-Energy is MLE) then (Steganography-Security is LS) (1)
19. If (Img-Contrast is MHC) and (Img-Energy is LE) then (Steganography-Security is PS) (1)
20. If (Img-Contrast is MHC) and (Img-Energy is VLE) then (Steganography-Security is PS) (1)

شکل ۴. ۲۰ قانون مربوط به خروجی سامانه استنتاج



شکل ۵. گراف تخمین امنیت نهان‌نگاری بر اساس ورودی‌های کنتراست و انرژی

۳. نتایج و بحث

در یک تجربه عملی سه تصویر انتخاب شده و با چهار نوع کنتراست متفاوت تصاویر مناسب انتخاب می‌شوند. سطح آستانه هریس، ۱۰۰۰ در نظر گرفته شده است. در هر کنتراست، تعداد نقاط برجسته لبه‌ها یا همان نقاط خاص متفاوت هستند. با تغییر سطح آستانه هریس، تعداد نقاط خاص و مابقی پارامترها تغییر می‌کنند و با افزایش تعداد نقاط خاص، نرخ درج (ظرفیت) هم افزایش می‌یابد و در هر سطح آستانه هریس، ظرفیت و در نتیجه سطح امنیت تغییر می‌کنند.

همان‌طور که در جدول‌های شکل (۶) مشاهده می‌شود، با توجه به تغییر نوع کنتراست تصویر، آنتروپی و نقاط خاص (نقاط برجسته نزدیک لبه‌ها) و همچنین پارامترهای دیگر تغییر کرده‌اند. رفتار هر معیار در انواع کنتراست هر تصویر تقریباً مشابه هم هستند. جهت مقایسه روش، توسط یک الگوریتم نهان‌نگاری *DCT*، در تصاویر پوشانه با ۲۵٪ ظرفیت اطلاعات درج شده است و دو ستون آخر هر جدول مربوط به دو پارامتر *PSNR* و *SSIM* است. هر چند با کاهش کنتراست، مقادیر دو پارامتر *PSNR* و *SSIM* افزایش می‌یابند ولی در صورت افزایش ناگهانی کنتراست باید به مقدار انرژی توجه داشت که اگر انرژی کاهش یافته باشد، همچنان دو پارامتر *PSNR* و *SSIM* افزایش می‌یابند. درنهایت،

تصاویر بر اساس کنتراست پایین و یا کنتراست بالا و انرژی پایین‌تر در هر تصویر مرتب می‌شوند.

Image1 : Harris Threshold = 1000				Steg. Embedded = %25 of Capacity			
Corner Detected	Entropy	Contrast	Correlation	Energy	Homogeneity	SSIM	PSNR
920	7.6097 9	5.2513	0.224	0.0401	0.5348	0.999	52.0504
2796	7.7317 5	5.1297	0.1461	0.0307	0.5054	0.9992	52.8117
3110	7.6431 6	4.5754	0.1078	0.0343	0.5004	0.9994	54.5222
500	7.3652 4	3.2588	0.2908	0.0461	0.5882	0.9998	63.8214

Image2 : Harris Threshold = 1000				Steg. Embedded = %25 of Capacity			
Corner Detected	Corner Detected	Corner Detected	Corner Detected	Corner Detected	Corner Detected	Corner Detected	Corner Detected
1369	1369	1369	1369	1369	1369	1369	1369
1173	1173	1173	1173	1173	1173	1173	1173
5994	5994	5994	5994	5994	5994	5994	5994
1135	1135	1135	1135	1135	1135	1135	1135

Image3 : Harris Threshold = 1000				Steg. Embedded = %25 of Capacity			
Corner Detected	Corner Detected	Corner Detected	Corner Detected	Corner Detected	Corner Detected	Corner Detected	Corner Detected
1807	1807	1807	1807	1807	1807	1807	1807
1255	1255	1255	1255	1255	1255	1255	1255
2419	2419	2419	2419	2419	2419	2419	2419
1028	1028	1028	1028	1028	1028	1028	1028

شکل ۶. نتایج رفتار تقریباً مشابه ویژگی‌های تصاویر ۱، ۲ و ۳ با کنتراست‌های متفاوت و مرتب بر اساس ویژگی‌های کنتراست و انرژی هر تصویر

۴. نتیجه‌گیری

تاکنون کار نظری و تجربی مشابه این موضوع انجام نشده است. با شبیه‌سازی در محیط متلب و نتایج حاصل شاخص‌های ارزیابی در این مقاله، به نتایج قابل قبولی دست یافته‌ایم. انتخاب پوشانه مناسب برای نهان‌نگاری مسئله مهمی است که باید به آن توجه کرد. اهمیت این مقاله، موضوع سطح‌بندی امنیت پوشانه‌ها قبل از درج اطلاعات است که تاکنون هیچ مقاله‌ای به آن نپرداخته است. در اختیار قرار دادن پوشانه مناسب نهان‌نگاری که امنیت آن تخمین زده شده باعث اطمینان بیشتر و تسریع در کار می‌شود. انتخاب هر تصویر پوشانه بر اساس ویژگی‌های کنتراست و انرژی تصویر و سپس قرار دادن آن پوشانه در یک بانک بر مبنای امنیت سطح‌بندی شده توسط منطق فازی، باعث می‌شود تا پوشانه‌های مناسب نهان‌نگاری از قبل آماده و در اختیار کاربران قرار گیرد. لازم به ذکر است که در این مقاله سطح آستانه هریس و تعداد نقاط خاص ثابت (نزدیک بعضی از گوشه‌ها و لبه‌های تصویر) در نظر گرفته شده است، که می‌توان سطح آستانه هریس متغیر را در تحقیق آینده بررسی کرد. همچنین انتخاب پوشانه بر اساس ویژگی‌های دیگر نیز از موضوعات قابل تحقیق و پژوهش است.

۵. مراجع

[1] Nazari, S.; Moin, M. S. “Cover Selection Steganography via Run Length Matrix and Human Visual System”; J. Inform. Sys. Telecom. 2013, 1, 131-138.

[2] Kuo, W.; Chen, Y.; Chuang, C. “High-Capacity Steganographic Method Based on Division Arithmetic and Generalized Exploiting Modification Direction”; J. Inf. Hiding and Multimedia Signal Processing 2014, 5, 213-222.

[3] Sajasi, S.; Eftekhari Moghadam, A. M. “A High Quality Image Steganography Scheme Based on Fuzzy Inference System”; 13th Iranian Conf. on Fuzzy Systems (IFSC) 2013.

[4] Li, M.; Reischuk, R.; Wolfel, U. “Security Levels in Steganography Insecurity does not Imply Detectability”; Electronic Colloquium on Computational Complexity, 2015, Report No. 10.

[5] Goldreich, O.; Goldwasser, S.; Nussboim, A. “On the Implementation of Huge Random Objects”; 44th Symp. Foundations of Computer Science, IEEE Computer Society, 2003, 68-79.

[6] Wang, W.; Farid, H. “Exposing Digital Forgeries in Video by Detecting Double Quantization”; Princeton the College of New Jersey, United States of America, Association for Computing Machinery, 2009.

[7] Sahraee-Ardakan, M.; Joneidi, M. “Joint Dictionary Learning for Example-Based Image Super-Resolution”; arXiv: 1701.03420v1 [cs.CV] 12 Jan 2017.

[8] Kaur, A.; Kaur, S. “Image Steganography Based on Hybrid Edge Detection and 2k Correction Method”; Int. J. Eng. Innov. Tech. 2012, 1, 167-170.

[9] Harris, C.; Stephens, M. "A Combined Corner and Edge Detector"; Proc. of the IFII Alvey Vision Conf. 1988, 189-192.

[10] Simitopoulos, D.; Koutsonanos, D. E.; Strintzis, M. G. "Image Watermarking Resistant to Geometric Attacks using Generalized Radon Transformations"; Proc. of DSP 2002, 1, 85-88.

[11] Amandeep, A.; Parveen, S. "Designing and Performance Evaluation of an Advanced Method for Corner Detection using Harris Technique"; Int. J. Comput. Appl. 2016, 139, 6-11.