دومین کنفرانس بین‌المللی ترکیبیات، رمزنگاری و محاسبات
Homepage: http://i4c.iust.ac.ir

نهان نگاری تصاویر رنگی دیجیتال با روش ماتریس بالا مثلثی هسنبرگ

۱-عطیه رحیمی زاده ۲-محمد بشارتلو ۳- محمد گرجی مهلبانی

گروه مهندسی کامپیوتر، موسسه آموزش عالی علوم و فناوری آریان، امیرکلا بابل

Atiye.rahimizade@gmail.com

چکیده

به منظور مقابله با استفاده غیر مجاز از رسانه‌های دیجیتال روش‌های متعددی پیشنهاد شده است و نهان‌نگاری یکی از راه حل‌های جدید و قابل اتکا برای مقابله با این معضل است. در واقع پنهان نگاری (نهان نگاری) فرآیندی است که در طی آن یک داده را در داده‌ای دیگر مثل فایل‌های عکس یا متن مخفی می‌کنند [۱]. تفاوت اصلی رمزنگاری و پنهان نگاری آن است که در رمز نگاری هدف اختفاء محتویات پیام است و نه بطور کلی وجود پیام، اما در پنهان نگاری هدف مخفی کردن هر گونه نشانه‌ای از وجود پیام است[۲].

هدف نهان نگاری دیجیتال به منظور حفظ مالکیت اثر، پنهان سازی علامت یا اطلاعاتی که منجر به شناسایی مالک حقیقی اثر می‌شود در محتوای دیجیتال است؛ این نهان نگاری باید به گونه‌ای باشد که تا حد ممکن هیچ نشانه‌ای از وجود پیام را آشکار نکند و در مقابل تغییراتی که عموما ناشی از انتقال، فشرده سازی و بریدن قسمتی از محتوای مورد حفاظت است نیز مقاوم باشد.

با توجه به محبوبیت فراگیر اینترنت و پیشرفت سریع فناوری چند رسانه‌ای، بستری برای انتقال سریع و آسان اطلاعات فراهم شده است و رفع معضل حفظ مالکیت اثر پر متقاضی تر از گذشته شده و اهمیت بیشتری پیدا کرده است [۳]. بنابراین پژوهش و ارتقاء کیفیت روش‌های نهان نگاری دیجیتال، بعنوان یک راه حل برای حفاظت بیشتر از محتوای دیجیتال و حفظ حق مالکیت آثار دیجیتال مسئله‌ای مهم و ضروری خواهد بود.

کلمات کلیدی: نهان نگاری- تبدیل هسنبرگ- دستکاری محتوا- استخراج تصویر- SVD- ماتریس بالا مثلثی

مقدمه

با محبوبیت فراگیر اینترنت و پیشرفت سریع فناوری چند رسانه ای، تکثیر غیرمجاز، دستکاری محتوای دیجیتال به منظور کارهای جاسوسی، به مساله ای بسیار بسیار پر اهمیت تبدیل شده است [۱-۳]. این پدیده، به افزایش تقاضا برای توسعه برخی از راه حل های استاندارد در جهت جلوگیری از این معضلات منجر شده است [۲۴-۳۱]. نهان نگاری دیجیتال، بعنوان یک راه حل برای حفاظت بیشتر از محتوای دیجیتال در نظر گرفته شده است. یکپارچگی نزدیک سینگال پنهان شده یا بعبارتی محتوای دیجیتال

نهان نگاری شده در رسانه میزبان (مانند ویدئو ، تصویر ، صوت و متن) میتواند برای تشخیص ویا تایید مالکیت محتوا، کنترل عملکرد نرم افزار و سخت افزار به منظور پیگیری و ردیابیِ جانی استفاده گردد[۱].

پیشینه پژوهش:

امروزه برخی از تحقیقات نهان نگاری کردن بر اساس استفاده از ماتریس تجزیه پی ریزی شده‌اند[٤-۱۲]. برای نمونه Lai [۴] یک نهان نگاری جدید برپایه سیستم بصری انسان (HVS) و تجزیه مقدار منفرد (SVD) طراحی کرد که در آن ، یک تصویر سیاه و سفیده به اندازه ۵۱۲*۵۱۲ با اصلاح ضرایب ماتریس واحد U نهان نگاریِ باینری و جایگذاری شده است. این روش در مقاومت در برابر افزودن نویز ، برداشتن و فیلتر کردن رسانه عملکرد بهتری دارد، اما در جنبه های مقاومت در برابر چرخش و تغییر مقیاس، بد است. و نیز مشکل تشخیص غلط– مثبت دارد. Golea و همکاران [۵] یک روش نهان نگاری کور برای تصویررنگی پیشنهاد داده اند که با استفاده از اصلاح مقادیر ویژه است، در این روش تصویر نهان نگاری شده ، به شدت تحت تاثیر قرار گرفته بود به این علت که یک یا چند مقدار ویژه به منظور جایگذاری باید اصلاح میشدند. بهاتناگار و همکاران [۶] یک تصویر سیاه و سفید، در اندازه ۲۵۶*۲۵۶ را در تصویر سیاه و سفید به اندازه ۵۱۲*۵۱۲ پنهان کرده‌اند. این روش به روش نهان نگاری غیر کور تعلق دارد، و مشکل تشخیص غلط-مثبت را دارد.

نادر احمدیان و همکارانش [۷] روشی را پیشنهاد کرده اند برای نهان نگاری کردن تصاویر خاکستری بر پایه تجزیه QR. قابل فهم است که این روش پیچیدگی محاسباتی کمتر و عملکرد نهان نگاری بهتری دارد، اما تصویر گنجانده شده در این نهان نگاری لوگو

دودویی با اندازه ۳۲*۳۲ است. در [۸] تصویر خاکستری با اندازه ۶۴*۶۴ در تصویر خاکستری با اندازه ۲۵۶*۲۵۶ جایگذاری شده، که بر پایه تبدیل هسنبرگ بوده و متعلق به روشهای نهان نگاری کور است. سدیک و همکاران [۹] یک روش نهان نگاری کور با استفاده از تبدیل هسنبرگ ، پیشنهاد داده اند، به طوری که تصویر میزبان تصویری خاکستری باشد؛ این روش بر پایه تجزیه QR است، بطوریکه یک بیت از اطلاعاتی که باید پنهان شود، در تمام عناصر سطر اول از ماتریس R در اندازه ۸*۸ نشانده می شود. در این روش تصویر نهان نگاری شده ۸۸*۸۸ دودویی بوده است. بعلاوه ، یک روش در [۱۱] پیشنهاد شده است، برای جایگذاری تصویر دودویی با اندازه ۳۲*۳۲ در تصویر میزبانی با اندازه ۵۱۲*۵۱۲، این روش با اصلاح عناصر ضرایب ماتریس Q در تجزیه QR عمل میکند.

در حال حاضر ، علامتهای تجاری یا نمادها از شرکتهای بسیاری رنگی شده اند و الگوبرداری محافظت شده با تصویررنگی بیشتر و بیشتر به یک معضل ضروری بدل شده است. اگرچه بسیاری از روشهای نهان نگاری برای تصاویررنگی، پیشنهاد شده اند[۱۲-۱۸]، همچنین هنگامی که تصویررنگی بعنوان تصویر میزبان انتخاب گردد، و نهان نگاری برای تصاویر خاکستری یا تصویر سیاه و سفید در این تصاویر رنگی باشد[۱۲-۱۶]. زمانیکه تصویررنگی بعنوان تصویری دودویی با همان اندازه در تصویرِ رنگیِ میزبان، جایگذاری گردد، حجم اطلاعات ناشی از نهان نگاری، تا ۲۴ بار بیشتر از نهان نگاری تصویر دودویی افزایش خواهد یافت، بطوریکه بر نامرئی ماندن و مقاوتِ نهان نگاری اثر مستقیم می گذارد. در کار قبلی ما[۱] و [۱۸]، دو طرح متفاوت نهان نگاری برپایه تجزیه QR پیشنهاد شده بود. اگرچه عملکرد روش دوم ما [۱۸] از روش قبلی [۱] بهتر است اما پیچیدگی محاسباتی این روش بالاتر از روش [۱] است. همانطور که مشخص است، پیچیدگی محاسباتی تجزیه SVD یا Schur بزرگتر از تجزیه QR است و نیز تبدیل هسنبرگ، یک گام میانی در تجزیه QR می باشد. بنابراین تبدیل هسنبرگ پیچیدگی محاسباتی کمتری از دیگر روشهای تجزیه داشته و برای تکنیک نهان نگاری استفاده خواهد شد.

با توجه به مباحث مطرح شده، بر آن شدیم که یک روش نهان نگاری کور بر مبنای استفاده از ماتریس بالا مثلثیِ هسنبرگ در تبدیل هسنبرگ ارائه دهیم که بتوان بر مشکلات بیان شده غلبه کرد. با تحلیل بیشتر بلوک تصویری تجزیه شده ۴*۴ توسط

تبدیل هسنبرگ، دریافت می گردد که بزرگترین عنصر انرژی ماتریس بالا هسنبرگ ، می تواند برای جایگذاری اطلاعات نهان نگاری در نظرگرفته شود. هنگامِ استخراجِ تصویر نهان نگاری شده ، تصویر میزبان اصلی و یا تصویر نهان نگاری شده،به هیچ عنوان موردِ نیاز نیستند. نتایج شبیه سازی شده نشان می دهد که روشهای پیشنهاد شده عملکرد بهتری از لحاظ نامرئی بودن، پایداری، ظرفیت و پیچیدگی محاسباتی نشان میدهد.

تبدیل تصویر رنگی که قرار است نهان شود، به اطلاعات دودویی :

در ابتدا، تصویر رنگی اصلی که باید نهان شود (W)، با اندازه p*q به سه لایه رنگی با مدل RGB تبدیل میشود. دوم اینکه ، به هریک از این لایه ها بوسیله تبدیل آرنولد با کلید خصوصی $KA_m(m = 1.2.3)$ به منظور بهبود امنیت نهان نگاری اعمال میشود [۲۰]. سوم ، هر پیکسل به صورت ۸ بیتی تبدیل میشود. در نهایت همه دنباله های دودویی لایه ها برای کسب لایه‌ی دودویی که باید نهان نگاری شود (w_j) ترکیب میشوند.(j=1,2,3)

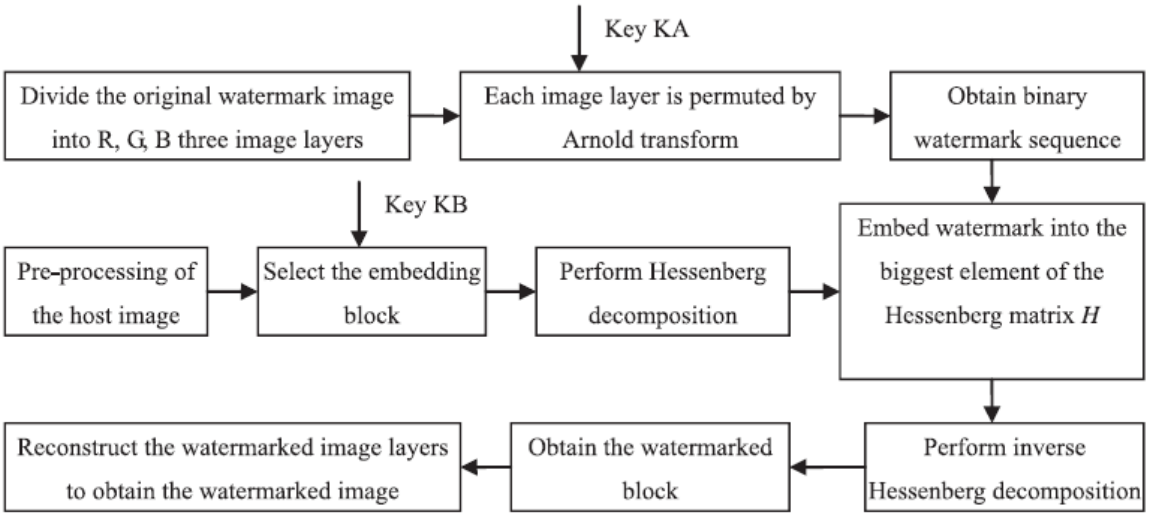

Fig. 1. Diagram of the watermark embedding process.

2. پردازش تصویر میزبان:

برای جایگذاری نهان نگاری ، تصویر میزبان I به سه لایه تصویری از R، G و Bجزبندی می شود .

$I_j(j = 1.2.3)$ و هر لایه تصویری I_j ، به بلوکهای تصویری غیرهمپوشانی با اندازه ۴*۴ تقسیم میشود.

3. برای نهان نگاری، بلوکها را بصورت تصادفی انتخاب می کنیم. انتخاب بلوکها بصورت پراکنده، بجای انتخاب بلوکها بصورت متمرکز و مرتب، برای بهبود بخشیدن به قابلیت اطمینان، در مقابل حملاتی مانند برش خوردن تصویر(crop) پیشنهاد شده است. الگوریتم جایگزینی شبه تصادفی هش، که مبتنی بر MD5 با کلید خصوصی KBn (n = 1, 2, 3) می باشد، به منظور استخراج بلوکهای تصاویر به طور تصادفی از لایه تصاویر $I_j(j = 1.2.3)$ در این روش استفاده میشود[۲۱] و تنها نیمی از بلوکها انتخاب میشوند.

نتایج تجربی و بررسی:

در این مقاله، کارایی روش پیشنهاد شده، توسط معیارهای نامرئی بودن، پایداری، ظرفیت و پیچیدگی محاسباتی تعیین شده است. برای ارزیابی عملکرد روش نهان نگاریِ پیشنهاد شده، همه تصاویر رنگی ۵۱۲*۵۱۲ و ۲۴ بیتی، موجود در پایگاه داده CVG-UGR بعنوان تصویر میزبان استفاده شده است [۲۲] و دو تصویررنگی ۲۴ بیتی ، ۳۲*۳۲ که در شکل ۳ نشان داده شده ، بعنوان تصاویری که باید نهان شوند مورد استفاده قرار می‌گیرد. برای مقایسه منصفانه با [۵و۱۸]، تصاویر نشان داده شده در شکل ۴ که به عنوان تصویر میزبان در [۵و۱۸] استفاده شده را نیز به عنوان تصویر میزبان استفاده کرده ایم.

روند استخراج نهان نگاری:

می توان دید که تصویر میزبان اصلی و تصویر اصلی نهان نگاری شده، در این فاز به هیچ عنوان لازم نیست. بنابراین روش پیشنهادی، به عنوان روشی از نهان نگاری کور خواهد بود. روند استخراج نهان نگاری در ادامه بیان میشود:

1. پیش پردازش تصویر نهان نگاری شده :

در ابتدا تصویر نهان نگاری شده I^* به سه لایه تصویر R,G,B جز به جز می شود. سپس هر لایه تصویر به بلوک های تصویری غیرهمپوشان ۴*۴ تقسیم می شوند.

2. بلوک تصویری نهان نگاری شده را انتخاب کنید.

الگوریتم جایگزینی شبه تصادفی هش بر پایه MD5 با کلید خصوصی $KB_n(n = 1.2.3)$ برای انتخاب بلوکهای تصویری نهان نگاری شده استفاده می گردد.

3. انجام تبدیل هسنبرگ

هر بلوک تصویری انتخاب شده با تبدیل هسنبرگ تجزیه شده ، و ماتریس بالا مثلثی هسنبرگِ آن (H^*) استخراج میشود.

تحلیل نامرئی بودنِ نهان نگاری

در روش پیشنهاد شده ، دو تصویر رنگی ۲۴ بیتی، در تصاویر رنگی میزبان ۲۴ بیتیِ تهیه شده از پایگاه داده تصویر CVG-UGR ، جایگذاری شده است. جدول ۱ میانگین مقادیر PSNR و SSIM از تصاویر نهان نگاری شده را لیست کرده است. داده های تجربی نشان می دهند که روش نهان نگاری پیشنهاد شده، قابلیت نامرئی بودن بهتری دارد. همچنین میانگین مقادیر NC مربوط به تصاویر نهان شده، بهبودِ پروسه استخراج را نیز اثبات می کند.

تحلیل ظرفیت:

در این مقاله ، روش پیشنهادی قابلیت این را دارد که نهان نگاری با طول $(4 * 4)/3 * 512 * 512$ برابر با 49152 بیت ، را در تصویر میزبان رنگی ۲۴ بیتی با سایز ۵۱۲*۵۱۲ (با توجه به محدودیتهای نظری) جایگذاری کند. اما کیفیت تصویر نهان نگاری شده زمانی که به محدودیت نظری مسئله نهان نگاری، می رسد به طور جدی تضعیف می شود. بنابربراین ، در این مقاله از تصویر رنگی ۲۴ بیتی با اندازه ۳۲*۳۲ برای نهان شدن استفاده گردیده، بطوریکه طول آن ۲۴۵۷۶ بیت (۳۲*۳۲*۲۴) است. جدول ۳ نتایج مقایسه ای ظرفیت نهان نگاری را نشان می دهد.

تحلیل مقایسه ای زمان اجرا :

زمان اجرا در الگوریتم پیشنهادی ، کمتر از بقیه است. از لحاظ نظری، پیچیدگی محاسباتی SDV یا تجزیه Schur، بیشتر از تجزیه QR می باشد و تبدیل هسنبرگ نیز یک گام میانی از تجزیه QR می باشد. بنابراین زمان جایگذاری و استخراج در روش پیشنهادی، از روش ارائه شده در [۵] که براساس SVD میباشد و روش ارائه شده در [۱۸] که بر اساس تجزیه QR است، کمتر است. این هزینه‌ی کمِ زمانیِ روش پیشنهادی نسبت به روش ارائه شده در [۱۰] بدین خاطر است که در روش پیشنهادی فقط از تبدیل هسنبرگ استفاده میشود، در حالیکه در [۱۰] از تبدیل موجک و تجزیه QR استفاده می‌شود.

در روش پیشنهادی مرحله کوانتیزه کردن نقش مهمی را ایفا می کند. برای تصمیم گیری گام کوانتیزاسیون (T)، تصاویرِ استاندارد که از پایگاه داده CVG-UGR انتخاب شده اند، به صورت مکرر مورد شبیه سازی قرار گرفته است. همانطور که در شکل ۵ قابل مشاهده است ، با افزایش گام کوانتیزاسیون، میانگینِ معیارِ SSIM در حال کاهش، اما میانگینِ معیارِ NC در حال افزایش است. این بدان معناست که نامرئی بودن نهان نگاری ضعیف و ضغیفتر می شود اما مقاومت نهان نگاری قدرتمندتر می شود. با در نظر گرفتن مصالِحه بین نامرئی بودن و مقاومتِ نهان نگاری، محدوده گام کوانتیزه (T) بین ۶۳ و ۶۸ است. در این مقاله ،به منظور سنجش عملکرد روش پیشنهادی، گام کوتنتیزاسون برابر با عدد ۶۵ در نظر گرفته شده است.

نتایج :

یک الگوریتم نوآورانه نهان نگاری کور برای تصاویر رنگی ، با استفاده از ماتریس بالا مثلثی هسنبرگ در این مقاله پیشنهاد شده است. براساس تبدیل هسنبرگ، اطلاعات نهان نگاریِ تصویرِ رنگی در عنصری از ماتریس بالا مثلثی هسنبرگ گنجانده میشود که بیشترین انرژی را داشته باشد. علاوه بر این اطلاعات نهان نگاری جایگذاری شده، می تواند از تصاویر مورد حمله قرار گرفته شده مورد استخراج قرار گیرد بطوریکه نیاز به وجود تصاویر اصلی نباشد. نتایج شبیه سازی نشان می دهند که طرح پیشنهادی نسبت به طرح های مرتبط دیگر در جنبه های مختلفی از جمله نامرئی بودن، پایداری ، ظرفیت و پیچیدگی محاسباتی بهتر عمل میکند. با این حال کارایی مقاومت در برابر حمله‌ی چرخشِ تصویر میتواند در کارهای آینده بیشتر مورد توجه قرار گیرد.

مراجع

[1] Su Q, Niu Y, Wang G, Jia S, Yue J. Color image blind watermarking scheme based on QR decomposition. Signal Process 2014;94(1):219–35.

[2] Li J, Li X, Yang B, Sun X. Segmentation-based image copy-move forgery detection scheme. IEEE Trans Inf Forensics Secur 2015;10(3):507–18.

[3] Zheng Y, Jeon B, Xu D, Wu QMJ, Zhang H. Image segmentation by generalized hierarchical fuzzy C-means algorithm. J Intell Fuzzy Syst 2015;28(2):961–73.

[4] Lai CC. An improved SVD-based watermarking scheme using human visual characteristics. Opt Commun 2011;284(4):938–44.

[5] Golea NEH, Seghir R, Benzid R. A bind RGB color image watermarking based on singular value decomposition. In: 2010 IEEE/ACS international conference on computer systems and applications (AICCSA). p. 1–5.

[6] Bhatnagar G, Raman B. A new robust reference logo watermarking scheme. Multimedia Tools App 2011;52(2–3):621–40.

[7] Naderahmadian Y, Hosseini-Khayat S. Fast and robust watermarking in still images based on QR decomposition. Multimedia Tools App 2013;72 (3):2597–618.

[8] Bhatnagar G, Wu QMJ. Biometircs inspired watermarking based on a fractional dual tree complex wavelet transform. Future Gener Comput Syst 2013;29 (1):182–95.

[9] Seddik H, Sayadi M, Fnaiech F, Cheriet M. Image watermarking based on the Hessenberg transform. Int J Image Graphics 2009;9(03):411–33.

[10] Yashar N, Saied HK. Fast watermarking based on QR decomposition in Wavelet domain. In: 2010 Sixth international conference on intelligent information hiding and multimedia signal processing. p. 127–30.

[11] Song W, Hou J, Li Z, Huang L. Chaotic system and QR factorization based robust

digital image watermarking algorithm. J Cent South Univ Technol 2011;18 (1):116–24.

[12] FindIk O, Babaoglu I, Ülker E. A color image watermarking scheme based on artificial immune recognition system. Expert Syst Appl 2011;38(3):1942–6.

[13] Niu PP, Wang XY, Yang YP, Lu MY. A novel color image watermarking scheme in nonsampled contourlet-domain. Expert Syst Appl 2011;38(3):2081–98.

[14] Vahedi E, Zoroofi RA, Shiva M. Toward a new wavelet-based watermarking approach for color images using bio-inspired optimization principles. Digital Signal Process 2012;22(1):153–62.

[15] Wang X, Wang C, Yang H, Niu P. A robust blind color image watermarking in quaternion Fourier transform domain. J Syst Softw 2013;86(2):255–77.

[16] Shao Z, Duan Y, Coatrieux G, Wu J, Meng J, Shu H. Combining double random phase encoding for color image watermarking in quaternion gyrator domain. Opt Commun 2015;343:56–65.

[17] Chen B, Coatrieux G, Chen G, Sun X, Coatrieux JL, Shu H. Full 4-D quaternion discrete Fourier transform based watermarking for color images. Digital Signal Process 2014;28(5):106–19.

[18] Su Q, Niu Y, Zou H, Zhao Y, Yao T. A blind double color image watermarking algorithm based on QR decomposition. Multimedia Tools App 2014;72

[19] Golub GH, Loan CFV. Matrix computations. Baltimore: Johns Hopkins University Press; 1996.

[20] Chen W, Quan C, Tay CJ. Optical color image encryption based on Arnold transform and interference method. Opt Commun 2009;282(18):3680–5.

[21] Rivest RL. The MD5 message digest algorithm, Internet RFC 1321; April 1992.

[22] University of Granada, Computer Vision Group. CVG-UGR Image Database. [2012-10-22]. http://decsai.ugr.es/cvg/dbimagenes/c512.php. 20.

[23] Wang Z, Bovik AC, Sheikh HR, Simoncelli EP. Image quality assessment: from

error visibility to structural similarity. IEEE Trans Image Process 2004;13 (4):600–12.

[24] Ma T, Zhou J, Tang M, Tian Y, Abdullah AD, Mznah AR, Sungyoung L. Social network and tag sources based augmenting collaborative recommender system. IEICE Trans Inf Syst 2015;98(4):902–10.

[25] Xia Z, Wang X, Sun X, Wang B. Steganalysis of least significant bit matching using multi-order differences. Secur Commun Netw 2014;7(8):1283–91.

[26] Zhou Z, Wang Y, Wu QMJ, Yang C, Sun X. Effective and efficient global context verification for image copy detection. IEEE Trans Inf Forensics Secur 2017;12 (1):48–63.

[27] Xia Z, Wang X, Zhang L, Qin Z, Sun X, Ren K. A privacy-preserving and copydeterrence content-based image retrieval scheme in cloud computing. IEEE Trans Inf Forensics Secur 2016;11(11):2594–608.

[28] Fu Z, Wu X, Guan C, Sun X, Ren K. Toward efficient multi-keyword fuzzy search over encrypted outsourced data with accuracy improvement. IEEE Trans Inf Forensics Secur 2016;11(12):2706–16.

[29] Fu Z, Ren K, Shu J, Sun X, Huang F. Enabling personalized search over encrypted outsourced data with efficiency improvement. IEEE Trans Parallel Distrib Syst 2016;27(9):2546–59.

[30] Zhou Z, Yang C, Chen B, Sun X, Liu Q, Wu QMJ. Effective and efficient image copy detection with resistance to arbitrary rotation. IEICE Trans Inf Syst 2016; E99-D(6):1531–40.

[31] Liu Q, Cai W, Shen J, Fu Z, Liu X, Linge N. A speculative approach to spatialtemporal efficiency with multi-objective optimization in a heterogeneous cloud environment. Secur Commun Netw 2016;9(17):4002–12.