# ارائه روشی جدید برای افزایش امنیت انتقال اطلاعات با ترکیب پنهان‌نگاری و رمزنگاری بصری در سطوح تصاویر خاکستری

سعید طلعتی[۱]، پوریا اعتضادی‌فر[۲]، محمدرضا حسنی آهنگر[۳]

۱- دانشجوی دکتری مهندسی برق، جنگ الکترونیک، دانشگاه جامع امام حسین(علیه‌السلام)، P9513621342@ihu.ac.ir

۲- استادیار، دانشگاه جامع امام حسین(علیه‌السلام)، petezadifar@ihu.ac.ir

۳- استاد، دانشگاه جامع امام حسین(علیه‌السلام)، mrhassani@ihu.ac.ir

**چکیده**

امنیت انتقال اطلاعات مخفی‌شده، می‌تواند توسط دو روش رمزنگاری و پنهان‌نگاری تأمین شده و ترکیب این دو روش می‌تواند جهت بالا بردن امنیت اطلاعات به‌کار برده شود. مزیت رمزنگاری این است که پیام رمز شده، اگر در بین راه توسط یک مهاجم دریافت شود؛ فاش نمی‌گردد؛ درحالی‌که در پنهان‌نگاری اطلاعات، پیام پنهان‌شده در یک رسانه پوشش جاسازی شده و سپس برای گیرنده ارسال می‌شود. در روش پیشنهادی از پنهان‌نگاری به روش افزودن ضرایب تبدیل ویولت استفاده شده که مشکل زیگزاگ شدن هیستوگرام اطلاعات با بیت‌های کم‌ارزش تصویر میزبان را حل نموده و مقاومت را نسبت به سایر روش‌ها بالا می‌برد؛ لذا در این روش همبستگی بین پیکسل‌های هم‌جوار تصویر به حداقل رسیده که باعث شده هیستوگرام تصویر با وجود پنهان نمودن حتی چهار پیام در دل رسانه پوشش، زیگزاگ نشود. برای بالاتر بردن امنیت از روش رمزنگاری بصری با چهار اشتراک استفاده می‌شود که حتی در صورت تشخیص پنهان‌نگاری محتوای رسانه پوشش نامفهوم بوده و اطلاعات اصلی به دست گیرنده غیرمجاز نخواهد رسید. نتایج نشانگر آن است که ترکیب این دو روش دارای امنیت بسیار بالایی بوده، پیچیدگی محاسباتی این روش بسیار پایین است؛ دارای پیاده‌سازی الگوریتم ساده‌ای است؛ زمان بسیار کمی برای اجرای الگوریتم پیاده‌سازی‌شده لازم است و بازیابی تصویر رمزشده، بسیار ساده است.

**واژه‌های کلیدی**

رمزنگاری بصری، پنهان‌نگاری، امنیت، اطلاعات

# Introducing a New Approach to Increase the Security of Information Transmission by Combining Steganography and Visual Cryptography in the Levels of Gray Images

**Saeed Talati[1], Pouriya Etezadifar[2,*], Mohammadreza Hasani Ahangar3**

1- Doctoral student of electrical engineering, electronic warfare, Imam Hossein University

2- Assistant Professor, Imam Hossein University

3- Professor, Imam Hossein University

**Abstract**

The security of concealed information transfer can be ensured by both Steganography and Cryptography. The combination of these two methods can be used to enhance information security. In Cryptography because the message is encrypted, if the message is received by an attacker in the middle of the message, the original message is not disclosed. While Steganography the message information, the hidden message is embedded in an image called the cover image and then sent to the recipient. The proposed method uses Steganography to add Wavelet conversion coefficients that solves the problem of zigzagging the information histogram with LSB of the host image to increase resistance to other methods. Therefore, in this method the correlation between adjacent pixels of the image is minimized, which makes the image histogram not hide in the zigzag cover media despite the four messages being undercover. And to increase the security of undercover file encrypted by visual Cryptography with four subscriptions that even if the hidden media content is encrypted, the key information is not unauthorized. The combination of these two methods is highly secure and the results show that the computational complexity of this method is very low, it has simple algorithm implementation, very short time to run the implemented algorithm, and the recovery of the encrypted image is very easy.

**Keywords**

Steganography, Visual Cryptography, Information, Security.

## ۱- مقدمه

روش‌های پنهان‌نگاری برای پنهان کردن یک پیام به‌طور نامحسوس در داخل علائم دیگر به کار می‌روند[۱]. با این روش‌ها اطلاعات از گیرندگان غیرمجاز دور نگه‌داشته می‌شود[۲]. اطلاعات پنهان‌شده بدون اینکه ضرری به علائم وارد کنند درون آن پنهان می‌شوند[۳]. حامل پیام می‌تواند تصویر، فیلم، صوت، متن و غیره باشد. نکته جالب اینکه می‌توان در پنهان‌سازی اطلاعات از عملیات رمزنگاری نیز به‌طور همزمان برای برقراری امنیت بیشتر استفاده کرد[۴]. اصل و اساس پنهان‌سازی، استفاده از فضاهایی از حامل اطلاعات هست که به هویت حامل لطمه وارد نکند[۵]. باکمی دقت می‌توان دید که پنهان‌سازی در تصویر دارای بیشترین امکان برای پنهان‌سازی است زیرا پهنای باند زیادی برای انتقال تصویر وجود دارد[۶]. بنابراین فضاهای بیشتری را برای پنهان‌سازی در اختیار ما می‌گذارد. پنهان‌سازی اطلاعات به دو روش کلی روش‌های حوزه زمان و تبدیل قابل پیاده‌سازی است[۷].

در سال ۲۰۱۱ خلیل چلیتا و همکارش دو روش متفاوت را پیشنهاد دادند که برای رسیدن به یک سطح بالاتر از پنهان‌نگاری و امنیت همراه با محدودیت‌شان کمک می‌کند. روش اول در مورد ترکیب پنهان‌نگاری و رمزنگاری است. در چنین روشی اگر رمزگشایی اعمال نشده باشد برای یک پنهان‌کاو بازیابی متن اصلی از روی تصویر محرمانه بسیار سخت هست. روش دوم از هیچ ابزار رمزنگاری استفاده نمی‌کند و صرفاً متکی بر پنهان‌نگاری است. از دو روش در نهان‌نگاری جهت پنهان‌کردن پیام محرمانه در درون رسانه نهانی استفاده‌شده است که یکی روش بیت‌های کم‌ارزش و دیگری روش‌های شناخته‌شده دیگری است که یک نهان کاو آن‌ها را برمی‌شمرد. در روش اول، رسانه پوشش تغییر نخواهد کرد و شامل ارسال یک بردار (احتمالاً رمزنگاری‌شده) که دربرگیرنده موقعیت‌های مختلف از رسانه پوششی است که به ما اجازه بازسازی پیام‌های مخفی از آن را می‌دهد. در این نمونه هر دو ارسال‌کننده و دریافت‌کننده باید یک الگوریتم مخفی (یا یک کلید) در مورد چگونگی بازیابی پیام‌های مخفی با توجه به رسانه پوشش و بردار (ارسال مخفیانه) به اشتراک بگذارند [۸].

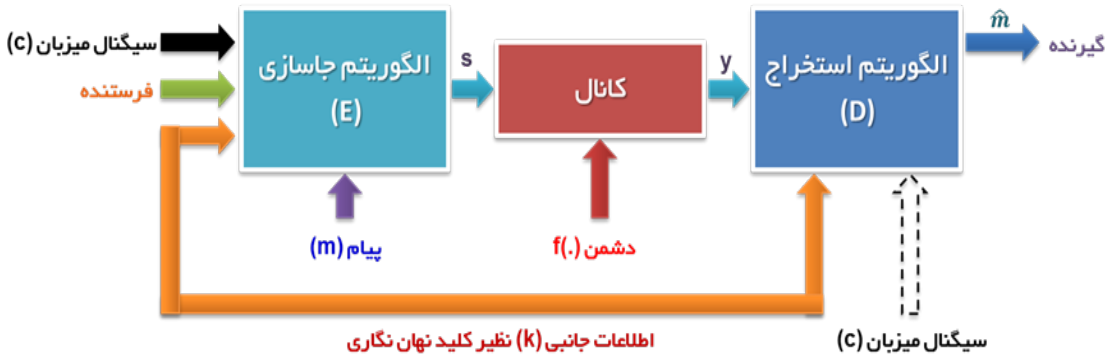
در سال ۲۰۱۲ راویندرا گوپتا و همکارانش روشی پیشنهاد دادند که پیام اصلی را در بیت‌های کم‌ارزش از تصویر اصلی کدگذاری می‌کرد. سیستم پیشنهادی داده‌ها را در یک تصویر واقعی پنهان می‌کند و دستیابی به آن‌ها از طریق آشکارسازی پس از اعمال رمزنگاری بصری بر روی داده‌ها می‌باشد. در عمل هدف اصلی از مدل پیشنهادی، طراحی یک الگوریتم امن مقاوم است که عملکرد آن با استفاده از ترکیب پنهان‌نگاری و رمزنگاری بصری جهت بهبود امنیت، قابلیت اطمینان و کارایی برای پیام‌های مخفی است[۹].

در سال ۲۰۱۰ ریتا رانا و همکارش ترکیب دولایه از امنیت یعنی رمزنگاری و پنهان‌نگاری را پیشنهاد دادند که آشکارسازی پیام مخفی‌شده را دشوار می‌ساخت؛ به‌طوری‌که اگر استراق‌سمع‌کننده، حامل پیام را موردحمله قرار دهد، قادر نخواهد بود پیام اصلی را دریافت کند، بدین علت که تمام داده‌های اصلی در اینجا به‌صورت رمز شده می‌باشند[۱۰].

در سال ۲۰۱۴ راحانت بیگام و همکارش یک روش برای پنهان‌نگاری بر پایه بیت کم‌ارزش ارائه کردند. سیستم پیشنهادی روشی برای مخفی کردن داده‌های امن و انتقال در شبکه‌ها با استفاده از پنهان‌نگاری بر پایه بیت کم‌ارزش همراه با الگوریتم ژنتیک و رمزنگاری بصری را فراهم می‌کند. در این روش پیام‌های مخفی در حداقل بیت قابل‌توجهی از تصویر پوشش کدگذاری می‌شود که در طول این روند تصویر به‌عنوان تصویر مخفی با استفاده از کلید مخفی نامیده می‌شود. در این مقاله از الگوریتم ژنتیک و رمزنگاری بصری برای افزایش امنیت استفاده‌شده است. از الگوریتم ژنتیک برای تغییر موقعیت پیکسل از تصویر مخفی استفاده شده است که یکی دیگر از قفل‌های حفاظتی برای پیام‌های مخفی و تصویر هست و دیگر اینکه تشخیص و آشکارسازی آن پیچیده می‌گردد. اساس رمزنگاری بصری بر شکستن این تصاویر به دو سهم بر اساس یک آستانه خاص است، بعدازآن سهام رمزگذاری شده و کلیدهای مخفی به‌طور جداگانه به دیگران بر روی شبکه ارسال می‌شود. کاربری که سهام مخفی دریافت کرده است باید روند معکوس یعنی بازیابی تصویر و پیام‌های مخفی را با استفاده از کلیدهای مخفی انجام دهد[۱۱].

## ۲- پنهان‌نگاری

در شکل ۱ مدل عمومی یک سیستم پنهان‌نگاری آورده شده است. در این شکل f تابعی است که دشمن بر s (سیگنال گنجانه) اعمال می‌کند تا در صورت وجود پیام، گیرنده نتواند آن را استخراج کند. (همچنین می‌تواند شامل اثر ناخواسته کانال بر s باشد) [۱۲].




شکل ۱ - مدل عمومی یک سیستم نهان‌نگاری [۱۲]

### ۲-۱ معیارهای متداول ارزیابی روش‌های پنهان‌نگاری

به‌منظور ارزیابی منطقی عملکرد انواع روش‌های پنهان‌نگاری، سه نیازمندی متداول امنیت، ظرفیت و نامحسوس بودن که معیارهایی برای میزان عملکرد روش‌های پنهان‌نگاری است بررسی می شوند با توجه به اینکه این سه معیار کیفی هستند نیاز است تا با استفاده از معیارها MSE و PPSNR به ارزیابی عملکرد روش پیشنهادی و مقایسه با سایر روش‌ها بپردازیم که در ادامه این دو معیار تشریح می‌شوند.

- **معیار MSE**

MSE معیاری برای محاسبه میانگین مربعات خطاست. این خطا به‌وسیله تفریقِ مقدارِ پیکسل از تصویر اصلی با تصویرِ پس از پنهان‌نگاری است که به‌صورت زیر محاسبه می شود. رابطه زیر برای محاسبه میانگینِ مربعات خطا در تصاویر است.

$$MSE = \frac{\sum_k \sum_{i=1}^{M} \sum_{j=1}^{N} (I[i,j]_k - I'[i,j]_k)^2}{3MN} \quad (۱)$$

M و N مشخص‌کننده‌ی ارتفاع و عرضِ تصویر و I تصویر اصلی و 'I تصویرِ پس از پنهان‌نگاری است [۶].

- **معیار PSNR**

منظور از غیرقابل مشاهده بودن توسط انسان این است که یک فرد عادی با نگاه کردن به تصویر اولیه و تصویر حاوی پیام نتواند بین دو تصویر تفاوتی قائل شود. ازآنجاکه این معیار دقیق نیست باید معیاری تعریف شود تا توسط آن بتوان کارایی الگوریتم‌ها را در زمینه حفظ امنیت سنجید؛ این معیار PSNR می‌باشد که این مقایسه نشان‌دهنده میزان نویز اضافه شده به تصویر در اثر تعبیه اطلاعات در تصویر می‌باشد.

هرچه مقدار PSNR بیشتر باشد تصویر حاوی پیام پنهان از کیفیت ظاهری بهتری برخوردار است. غالباً مقدار PSNR بیش از ۳۵ دسی‌بل ازنظر درک نشدن تغییرات توسط انسان قابل‌قبول است. PSNR به‌صورت ذیل محاسبه می‌شود.

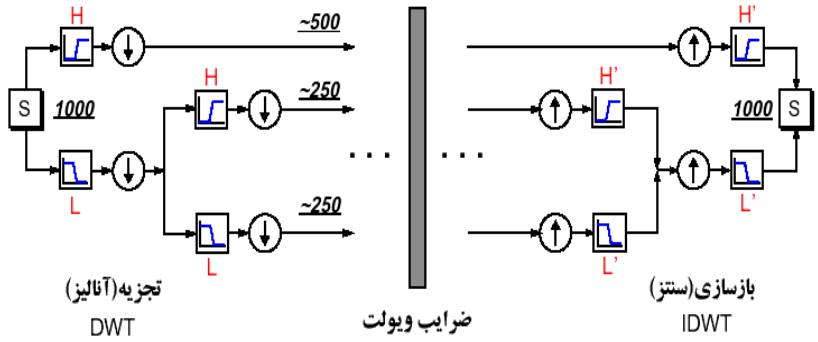
$$SNR = 10\, log \frac{(2^n - 1)^2}{MSE} \quad (۲)$$

## ۳- تبدیل ویولت

تبدیل ویولت در ابتدای دهه ۱۹۸۰ توسط مورلت و بقیه معرفی گردید که برای ارزیابی داده‌های زلزله بکار رفت[۱۵]. از آن زمان تاکنون انواع متفاوتی از تبدیلات ویولت توسعه‌یافته‌اند.

یکی از علل استفاده از تبدیل ویولت این است که تحقیقات جدید در مورد بینایی چشم انسان نشان داده است که شبکیه چشم انسان تصاویر را به چندین کانال فرکانسی تقسیم می‌کند و سیگنال‌های هر یک از این کانال‌ها در مغز به‌طور جداگانه پردازش می‌شوند.

تبدیل ویولت با ایجاد طول‌های متغیر در آنالیز، دقت‌های فرکانسی متغیری را ایجاد می‌نماید؛ بدین ترتیب که هرگاه اطلاعات دقیق در فرکانس‌های کم مطلوب باشد از فواصل زمانی طولانی استفاده می‌کند و بالعکس از فواصل کوتاه به هنگام آنالیز دقیق فرکانس در فرکانس‌های بالا استفاده می‌کند. محاسبه ضرایب ویولت در هر انتقال و مقیاس بسیار مشکل است. یک روش سریع برای به دست آوردن ضرایب ویولت، استفاده از بانک‌های فیلتر است (شکل ۲). در آن صورت آنالیز ویولت شامل فیلترکردن و کاهش نرخ نمونه‌برداری و بازسازی سیگنال اولیه، شامل افزایش نرخ نمونه‌برداری و فیلتر کردن است.




شکل ۲ - سیستم آنالیز و سنتز مبتنی بر ویولت [۴]

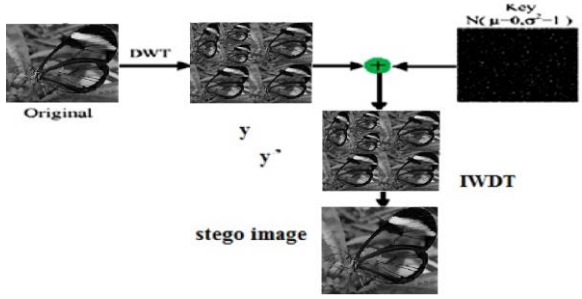
در تبدیل ویولت فیلترهای پایین‌گذر و بالاگذر آنالیز (L و H) به همراه فیلترهای بازسازی مکمل آن‌ها (L' و H') سامانه‌ای را تحت عنوان فیلترهای آینه‌ای مربعی (QMF) تشکیل می‌دهند. فیلترهای QMF متناظر درخت تبدیل، وابسته به تابع ویولت مادر می‌باشند.

### ۳-۱- الگوریتم روش تبدیل ویولت

الگوریتم پنهان‌سازی داده در تصویر با استفاده از تبدیل ویولت به‌صورت زیر است:

- از تصویر حامل تبدیل ویولت گرفته می‌شود.
- پیام سری به کد اسکی[۱] و یک‌رشته از بیت‌های صفر و یک تبدیل می‌گردد.
- رشته بیتی در لابه‌لای ردیف‌های یکی از چهار جزء تبدیل ویولت پنهان می‌گردد.

مراحل این روش در شکل زیر آورده شده است (شکل ۳).




شکل ۳ - مخفی کردن اطلاعات در تصویر به روش تبدیل ویولت

### ۳-۲- مزایای روش تبدیل ویولت

- عدم نیاز به تقسیم داده ورودی به بلوک‌های دوبعدی بدون همپوشانی
- استفاده از ساختار سلسله‌مراتبی و چند دقته
- قرار گرفتن اطلاعات در تمامی باندها و تمامی مکان‌ها

### ۳-۳- روش استفاده از بیت‌های کم‌ارزش ضرایب تبدیل ویولت

این روش پراستفاده‌ترین روش در پنهان‌سازی اطلاعات در حوزه تبدیل ویولت است و اکثر الگوریتم‌ها برای پنهان‌سازی اطلاعات از این روش سود می‌برند، لذا یک الگوریتم اولیه بر پایه این روش پیاده‌سازی شده است. مراحل پنهان نمودن اطلاعات در تصویر به‌صورت زیر است:

- از تصویر میزبان تبدیل ویولت گرفته می‌شود.
- ضرایب تبدیل ویولت تصویر میزبان به باینری تبدیل می‌گردند.
- مقادیر پیام در بیت‌های کم‌ارزش ضرایب تبدیل ویولت تصویر میزبان پنهان می‌گردند.
- از ضرایب حاصل تبدیل ویولت معکوس گرفته می‌شود و تصویر حامل پیام به دست می‌آید.

مراحل آشکارسازی پیام نیز به‌صورت زیر است:

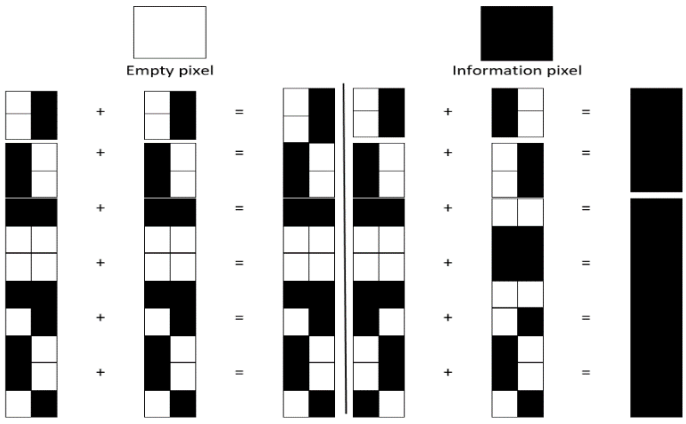
- از تصویر حامل تبدیل ویولت گرفته می‌شود.
- مقادیر پیام از بیت‌های کم‌ارزش ضرایب تبدیل ویولت تصویر حامل جدا می‌گردند.
- پیام به دست می‌آید.

## ۴- رمزنگاری بصری

رمزنگاری بصری روشی برای رمزنگاری اطلاعات دیداری (عکس، متن، صوت و ...) است. در این روش اطلاعات به‌گونه‌ای در تصاویر پنهان می‌گردد که رمزگشایی با کمک بینایی انسان و بدون نیاز به محاسبات کامپیوتری صورت گیرد. این روش، اولین بار توسط نائور و شامیر در سال ۱۹۹۴ میلادی معرفی شد[۱۳]. در این طرح تصویر به n

[۱] کد استاندارد آمریکایی (ASCII) برای تبادل اطلاعات، یک استاندارد رمزگذاری شخصیت برای ارتباطات الکترونیکی است.

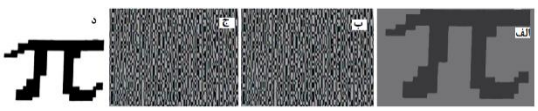
سهم تجزیه می‌گردد به‌طوری‌که تنها کسی که تمام n سهم را در اختیار دارد می‌تواند تصویر را بازیابی کند و هیچ دسته n-1 تایی از سهم‌ها اطلاعاتی درمکرد تصویر نمی‌دهد. برای رمزگشایی کافی است هر سهم بر روی سطح شفافی چاپ شود و با روی هم قراردادن همه صفحات شفاف تصویر اصلی به‌راحتی قابل‌مشاهده خواهد بود. اگر تصویر به دو سهم تجزیه شود، آنگاه هر یک از دو سهم که توزیعی تصادفی از نقطه‌های سفیدوسیاه هستند را می‌توان به‌عنوان کلید و سهم دیگر را به‌عنوان متن رمز شده در نظر گرفت که رمزگشایی با داشتن هر دو سهم امکان‌پذیر است و کلید نیز تصادفی و یک‌بارمصرف است. متن ساده نیز، از XOR دو سهم به دست می‌آید. هر پیکسل تصویر به بلوک‌هایی نگاشت می‌شود، به‌گونه‌ای که در هر بلوک، تعداد برابری از پیکسل‌های سفید و سیاه وجود داشته باشد (شکل ۴).




شکل ۴ - تقسیم پیکسل به زیر پیکسل‌ها در رمزنگاری بصری

### ۴-۱- رمزنگاری بصری تصاویر سیاه و سفید

ویژگی اولیه‌ی رمزنگاری بصری این است که از روش برهم‌نهی سهم‌ها به‌منظور بازیابی پیام محرمانه استفاده می‌کند. مالک رمز دو یا چند سهم را برای پیام محرمانه ایجاد می‌کند که هر یک به‌تنهایی برای آشکارسازی تصویر بکار نمی‌رود. دریافت همه‌ی سهم‌ها و چاپ هر سهم بر روی یک شفافیت، برهم‌نهی شفافیت‌ها و استفاده از سیستم بینایی انسان، باعث می‌شوند که بدون نیاز به هیچ‌گونه محاسبات پیچیده‌ای، پیام محرمانه آشکار شود. طرح تقسیم راز بصری آستانه (k,n) که ($k \leq n$)، به‌منظور اجرای تقسیم راز بکار برده می‌شود مالک رمز می‌تواند بر اساس یک گروه از n شرکت‌کننده، n سهام برای پیام محرمانه تولید کند. هر شرکت‌کننده در گروه می‌تواند سهم خودش را داشته باشد؛ هنگام بازیابی تصویر محرمانه تنها قرارگیری k یا تعداد بیشتری شفافیت موردنیاز است. اگر تعداد شفافیت‌ها کمتر از k باشد پیام محرمانه نمی‌تواند بازیابی شود.[۱۴].یک نمونه برای نمایش طرح تقسیم راز بصری را نشان داده شده است (شکل ۵).



شکل ۵ – الف: تصویر اصلی ب: سهم اول ج: سهم دوم د: نتیجه حاصل از برهم‌نهی

### ۵- ارائه روش پیشنهادی

به‌منظور پیاده‌سازی پنهان‌نگاری و رمزنگاری بصری و ترکیب آن‌ها نیاز به معرفی چند تصویر است (شکل ۶).


شکل ۶ – الف: پروانه ب: مرد عکاس پ: پیام ت:پیام ج: پیام چ: پیام

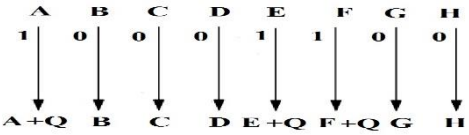
تصاویر الف و ب دارای ابعاد ۲۵۶×۲۵۶ با هشت سطح خاکستری به‌عنوان تصویر اصلی (حامل پیام) هستند و سایر تصاویر دوسطحی هستند که از آنها به‌عنوان پیام برای پنهان‌سازی و رمزنگاری بصری استفاده می‌شود.

**۵-۱- روش پیشنهادی افزودن ضرایب در تبدیل ویولت**

برای حل مشکل زیگزاگ شدن هیستوگرام در روش‌های بیت کم‌ارزش و تبدیل ویولت سعی بر این است روشی ارائه گردد که اطلاعات با بیت‌های کم‌ارزش تصویر میزبان جایگزین نگردد؛ زیرا جایگزین شدن داده با بیت‌های کم‌ارزش حامل، علی‌الخصوص اگر این امر در مورد بیت‌های باارزش بالاتر صورت گردد همبستگی بین پیکسل‌های هم‌جوار تصویر را از بین می‌برد و این امر سبب زیگزاگ شدن هیستوگرام تصویر می‌گردد؛ بنابراین باید سعی شود روشی ارائه گردد که آسیبی به این همبستگی وارد نسازد و یا آن را به حداقل برساند. لذا الگوریتم زیر پیشنهاد و پیاده‌سازی می‌گردد. مراحل پنهان نمودن اطلاعات در تصویر در الگوریتم پیشنهادی به‌صورت زیر است:

- از تصویر اصلی تبدیل ویولت گرفته می‌شود.
- عدد Q به‌عنوان گام کوانتیزاسیون در نظر گرفته می‌شود.
- اگر بیت پیام یک باشد مقدار Q به ضریب تبدیل ویولت تصویر میزبان اضافه می‌گردد و اگر بیت پیام صفر باشد تغییری داده نمی‌شود.
- از ضرایب حاصل تبدیل ویولت معکوس گرفته می‌شود و تصویر حامل پیام به دست می‌آید.

در شکل ۷ طریقه پنهان نمودن پیام '10001100' داخل تعدادی از ضرایب، نشان داده‌شده است.




شکل ۷ - طریقه پنهان‌سازی پیام '10001100' داخل تعدادی از ضرایب

مراحل آشکارسازی پیام نیز به‌صورت زیر است:

- از تصویر حامل تبدیل ویولت گرفته می‌شود.
- از تصویر اصلی نیز تبدیل ویولت گرفته می‌شود.
- ضرایب تبدیل ویولت دو تصویر باهم مقایسه می‌گردند؛ اگر بجای هر ضریب تبدیل ویولت تصویر حامل که از ضریب تبدیل ویولت تصویر اصلی بزرگ‌تر است '۱' و در غیر این صورت صفر قرار دهیم پیام بازیابی می‌گردد.

**۵-۲- مزایای مدل پنهان‌نگاری پیشنهادی**

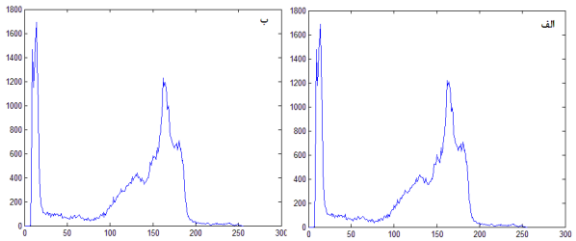
- عدم نیاز به تقسیم داده ورودی به بلوک‌های دوبعدی بدون همپوشانی
- استفاده از ساختار سلسله‌مراتبی و چند دقته
- قرار گرفتن اطلاعات در تمامی باندها و تمامی مکان‌ها.

**۵-۳- پنهان کردن یک پیام در روش پیشنهادی**

مطابق شکل ۸ با استفاده از روش پنهان‌نگاری تبدیل ویولت با استفاده از افزودن ضرایب یک پیام را در یک بیت کم‌ارزش روش پیشنهادی پنهان می‌کنیم.


شکل ۸ - الف: تصویر اصلی ب: تصویر حامل پیام پ: تصویر پیام ت: تصویر پیام بازیابی شده درروش افزودن ضرایب

با تحلیل هیستوگرام (شکل ۹) می‌توان دریافت که تغییرات محسوسی دیده نمی‌شود که مقاومت بالای روش را نشان می‌دهد.




شکل ۹ - هیستوگرام تصویر اصلی و تصویر حامل پیام

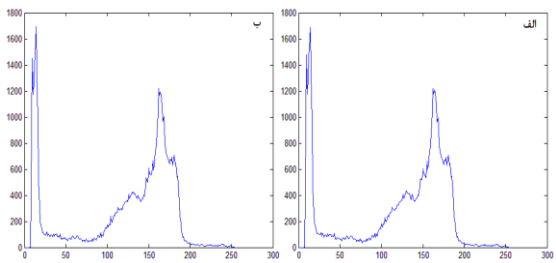
نرخ داده در این روش کمتر از روش بیت‌های کم‌ارزش و بیت‌های کم‌ارزش تبدیل ویولت است و مقاومت با کمی توجه می‌توان دریافت که هیستوگرام تصویر تغییر محسوسی نکرده است. این اتفاق در مقایسه با روش‌های بیت‌های کم‌ارزش و بیت‌های کم‌ارزش تبدیل ویولت است که هیستوگرام‌ها دستخوش تغییرات قرار می‌گرفتند بسیار حائز اهمیت است و با توجه به این موضوع می‌توان نتیجه گرفت که این روش در مقابل تحلیل هیستوگرام مقاوم است.

**۵-۴- پنهان کردن دو تا چهار پیام در روش پیشنهادی**

در این قسمت با استفاده از روش پنهان‌نگاری تبدیل ویولت با استفاده از افزودن ضرایب دو الی چهار پیام را به ترتیب در دو الی چهار بیت کم‌ارزش این مدل پنهان می‌کنیم. حال باید از نظر شفافیت، ظرفیت و مقاومت روش را مورد ارزیابی قرار دهیم. نتایج پیاده‌سازی این روش ادامه آورده شده است.


شکل ۱۰ - الف: تصویر اصلی ب: پیام۱ پ: پیام۲ ت:تصویر بازیابی شده ث: پیام بازیابی شده ۱ ج: پیام بازیابی شده۲

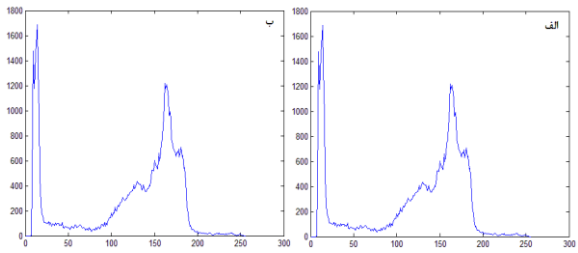
همان‌طور که در شکل ۱۰ مشاهده می‌شود با وجود استفاده از دو تصویر برای پنهان‌سازی، تصویر حامل پیام از شفافیت بسیار بالایی برخوردار است و با تحلیل هیستوگرام (شکل ۱۱) هم می‌توان دریافت که تغییرات محسوسی دیده نمی‌شود که این اتفاق باعث بالا رفتن مقاومت می‌شود.




شکل ۱۱ - الف: هیستوگرام تصویر اصلی ب: هیستوگرام تصویر حامل پیام مربوط به دو تصویر پیام


شکل ۱۲- الف: تصویر اصلی ب: پیام۱ پ: پیام۲ ت: پیام۳ ث: تصویر بازیابی شده ج: پیام بازیابی شده۱ چ: پیام بازیابی شده۲ ح: پیام بازیابی شده۳

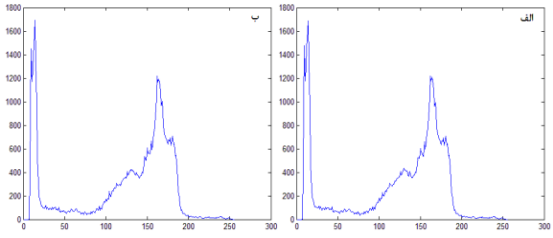
با تحلیل هیستوگرام (شکل ۱۳) می‌توان دریافت که تغییرات محسوسی دیده نمی‌شود که مقاومت بالای روش را نشان می‌دهد.




شکل ۱۳- الف: هیستوگرام تصویر اصلی ب: هیستوگرام تصویر حامل پیام مربوط به سه تصویر پیام


شکل ۱۴ - الف: تصویر اصلی ب: پیام۱ پ: پیام۲ ت:پیام۳ ث: پیام۴ ج: تصویر بازیابی شده چ: پیام بازیابی شده۱ ح: پیام بازیابی شده۲ خ: پیام بازیابی شده۳ د: پیام بازیابی شده۴

با تحلیل هیستوگرام (شکل۱۵) می‌توان دریافت که تغییرات محسوسی دیده نمی‌شود که مقاومت بالای روش را نشان می‌دهد.




شکل ۱۵ الف: هیستوگرام تصویر اصلی ب: هیستوگرام تصویر حامل پیام مربوط به چهار تصویر پیام

### ۵-۵- ارزیابی

نتایج و مزایای به‌دست‌آمده از ارزیابی این روش بر اساس مشخصه‌های سه‌گانه سیستم به شرح زیر است:

- همان‌طور که از هیستوگرام تصاویر و هیستوگرام ضرایب تبدیل ویولت مشخص است در این روش حتی با اضافه شدن تعداد تصاویر پیام زیگزاگ شدن هیستوگرام وجود ندارد و هیستوگرام تصویر حامل و هیستوگرام ضرایب تبدیل ویولت به مقدار بسیار زیادی شبیه تصویر اصلی است.
- با توجه به مقادیر MSE و PSNR ارزیابی‌شده در جدول‌های ۱ و ۲ می‌توان نتیجه گرفت با افزایش نرخ داده شفافیت تصویر به میزان بسیار کمی کاهش پیدا می‌کند که این‌یک برتری نسبت به دو روش قبل است.
- مقاومت این روش نسبت به روش‌های استفاده از بیت‌های کم‌ارزش و همچنین بیت‌های کم‌ارزش تبدیل ویولت.

### ۵-۶- مقایسه مقادیر MSE و PSNR

برای رسیدن به یک نتیجه مطلوب مقادیر MSE و PSNR مربوط به سه روش پنهان‌نگاری به روش بیت‌های کم‌ارزش، بیت‌های کم‌ارزش تبدیل ویولت و افزودن ضرایب تبدیل ویولت در جدول‌های ۱ و ۲ مورد ارزیابی قرار می‌گیرد.

جدول ۱: مقادیر PSNR در سه روش بیت‌های کم‌ارزش، بیت‌های کم‌ارزش تبدیل ویولت و افزودن ضرایب تبدیل ویولت

| PSNR / نام تصویر | مرد عکاس | پروانه |
|---|---|---|
| PSNR-LSB-1 bit | ۴۵/۶ | ۴۶/۵ |
| PSNR-LSB-2 bit | ۳۷/۱ | ۳۸/۱ |
| PSNR-LSB-3 bit | ۳۰/۲ | ۳۱/۱ |
| PSNR Wavelet-LSB-1 bit | ۵۲/۵ | ۵۳/۴ |
| PSNR Wavelet-LSB-2 bit | ۴۳/۸ | ۴۴/۸ |
| PSNR Wavelet-LSB-3 bit | ۳۶/۵ | ۳۷/۵ |
| PSNR Wavelet quantization-1 bit | ۵۴/۵ | ۵۵/۵ |
| PSNR Wavelet quantization-2 bit | ۵۱/۵ | ۵۲/۵ |
| PSNR Wavelet quantization-3 bit | ۴۹/۷ | ۵۰/۷ |
| PSNR Wavelet quantization-4 bit | ۴۸/۵ | ۴۹/۵ |

جدول ۲: مقادیر MSE در سه روش بیت‌های کم‌ارزش، بیت‌های کم‌ارزش تبدیل ویولت و افزودن ضرایب تبدیل ویولت

| MSE / نام تصویر | مرد عکاس | پروانه |
|---|---|---|
| MSE-LSB-1 bit | ۰/۴۹ | ۰/۵ |
| MSE -LSB-2 bit | ۳/۴۶ | ۳/۵۱ |
| MSE -LSB-3 bit | ۱۷/۱ | ۱۷/۶ |
| MSE Wavelet-LSB-1 bit | ۰/۱ | ۰/۱ |
| MSE Wavelet-LSB-2 bit | ۰/۷۴ | ۰/۷۵ |
| MSE Wavelet-LSB-3 bit | ۴ | ۴/۰۲ |
| MSE Wavelet quantization-1 bit | ۰/۰۶ | ۰/۰۶۳ |
| MSE Wavelet quantization-2 bit | ۰/۱۲ | ۰/۱۲ |
| MSE Wavelet quantization-3 bit | /۱۹ | /۱۹ |
| MSE Wavelet quantization-4 bit | /۲۵ | /۲۵ |

با توجه به مقادیر جدول‌های ۱ و ۲ و همچنین نتایج حاصل از ارزیابی‌های انجام‌شده بر روی سه روش مطرح‌شده می‌توان دریافت که برای رسیدن به یک نتیجه مطلوب در پنهان‌سازی پیام، روش افزودن ضرایب تبدیل ویولت از کارایی بهتری برخوردار است.

### ۵-۷- پیاده‌سازی رمزنگاری بصری بر روی تصویر

به‌منظور رمزنگاری بصری نیاز به معرفی دو تصویر است (شکل ۱۶).


شکل ۱۶- الف: پروانه ب: پیام۱

در ابتدا تصاویر توسط نرم‌افزار متلب با استفاده از یک تصویر باینری الگوریتم مربوط به رمزنگاری بصری را پیاده‌سازی کرده و سپس این روش را مورد ارزیابی قرار می‌دهیم. سپس با ترکیب رمزنگاری بصری و پنهان‌نگاری با استفاده از افزودن ضرایب تبدیل ویولت به یک روش

بهینه می‌رسیم. نتایج حاصل از پیاده‌سازی این الگوریتم توسط نرم‌افزار متلب در شکل ۱۷ قابل‌مشاهده است.

شکل ۱۷ الف: اشتراک ناشی از پیکسل‌های سیاه تصویر پیام ب: اشتراک ناشی از پیکسل‌های سفید تصویر پیام پ: تصویر پیام ت: تصویر بازیابی شده

نتایج به‌دست‌آمده از پیاده‌سازی این روش به شرح زیر است:

- پیاده‌سازی الگوریتم رمز بصری مطرح‌شده ساده است.
- زمان بسیار کمی برای اجرای الگوریتم پیاده‌سازی شده لازم است.
- بازیابی تصویر رمز شده بسیار ساده است.
- ولی تصویر بازیابی شده ازلحاظ اندازه گسترده شده است.
- تصویر بازیابی شده از کیفیت پایینی برخوردار است.

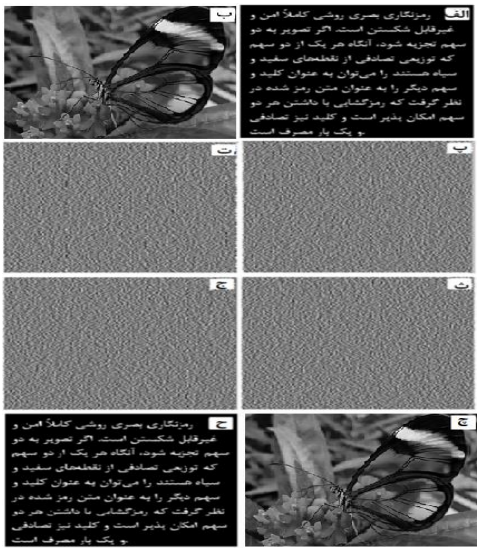
**۵-۸- مراحل پیاده‌سازی ترکیب رمزنگاری و پنهان‌نگاری:**

۱. یک تصویر خاکستری به‌عنوان تصویر میزبان انتخاب می‌شود.
۲. یک تصویر باینری به‌عنوان تصویر پیام انتخاب می‌شود.
۳. تصاویر پیام را انتخاب می‌کنیم و بر روی آن الگوریتم رمزنگاری بصری پیاده‌سازی می‌شود. (با اعمال این الگوریتم تصویر پیام به ۴ اشتراک تبدیل می‌شود.)
۴. مؤلفه‌ی تصویر انتخاب می‌شود و از آن تبدیل ویولت گرفته می‌شود.
۵. با استفاده از روش افزودن ضرایب اشتراک‌های مربوط به تصویر پیام را در درون ضرایب تبدیل ویولت پنهان می‌شود.
۶. از ضرایب حاصل تبدیل ویولت معکوس گرفته می‌شود و تصویر حامل پیام مربوطه به دست می‌آید.
۷. تصویر حامل به‌دست‌آمده از مؤلفه باهم ترکیب‌شده و تصویر حامل اصلی به دست می‌آید.

**۵-۹- مراحل آشکارسازی تصویر به شرح زیر است:**

۱. مؤلفه‌ی تصویر حامل خاکستری انتخاب می‌شود و از آن تبدیل ویولت گرفته می‌شود.
۲. مراحل آشکارسازی پیام به روش افزودن ضرایب تبدیل ویولت انجام و اشتراک‌ها تولید می‌شود.
۳. اشتراک‌های حاصل از مرحله ۲ ترکیب می‌شوند و تصویر پیام بازسازی می‌گردد.

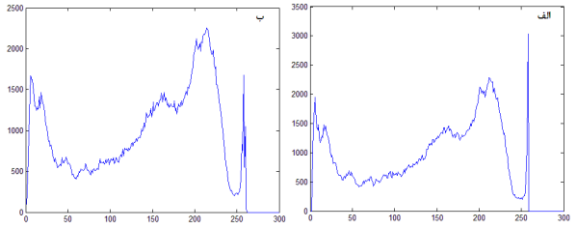
نتایج حاصل از پیاده‌سازی این الگوریتم توسط نرم‌افزار متلب در شکل‌های ۱۸ و ۱۹ قابل‌مشاهده است.



شکل ۱۸ الف: تصویر پیام۲ ب: تصویر پروانه پ، ت، ث و ج: اشتراک‌های پیام در خروجی الگوریتم رمز بصری چ: تصویر حامل پیام رمزنگاری‌شده ح: تصویر بازیابی شده۲

**۵-۱۰- ارزیابی**

همان‌طور که در شکل ۱۸ قابل‌مشاهده است شفافیت در این الگوریتم بالاست. نرخ داده در این روش هر تصویر باینری که به‌عنوان پیام در نظر گرفته می‌شود به ۴ اشتراک تبدیل می‌گردد. در یک تصویر خاکستری ۸ بیتی که به‌عنوان تصویر اصلی برای حمل پیام استفاده کنیم قادر به انتقال یک پیام هستیم. مقاومت هیستوگرام‌های مربوط به مؤلفه‌های تصویر اصلی و تصویر حامل در شکل ۱۹ آمده است.



شکل ۱۹ الف: هیستوگرام مؤلفه R تصویر اصلی ب: هیستوگرام مؤلفه R تصویر حامل

نتایج به‌دست‌آمده از پیاده‌سازی این روش به شرح زیر است:

- با توجه به تحلیل هیستوگرام‌های فوق که نشان می‌دهد هیستوگرام تصویر اصلی و هیستوگرام تصویر حامل پیام تفاوتی با یکدیگر ندارند

می‌توان نتیجه گرفت که این روش در مقابل این نوع تحلیل مقاوم است.

- پیاده‌سازی این الگوریتم ساده است.
- زمان بسیار کمی برای اجرای الگوریتم پیاده‌سازی شده لازم است.
- بازیابی تصویر رمز شده بسیار ساده است.
- پهن‌شدگی تصویر بازیابی شده که درروش رمزنگاری بصری وجود داشت برطرف شده است.
- تصویر بازیابی شده از کیفیت خوبی برخوردار است.

مقایسه PSNR روش پیشنهادی با سایر روش‌ها در جدول ۳ آورده شده است.

جدول ۳ - مقایسه روش پیشنهادی با سایر روش‌ها

| عنوان مقاله | سال انتشار | روش پیشنهادی | مقدارPSNR |
|---|---|---|---|
| Improved wavelet-based image watermarking through SPIHT.[16] | 2020 | LWT[۲] ANN[۳] | ۴۳,۸ dB |
| Guided Dynamic Particle Swarm Optimization for Optimizing Digital Image Watermarking in Industry Applications.[17] | 2018 | IWT[٤] | ۵۰dB |
| Neural network based robust image watermarking technique in LWT domain.[18] | 2018 | LSB[٥] GA[٦] | ۵۳,۱۱ dB |
| An adaptive hybrid fuzzy-wavelet approach for image steganography using bit reduction and pixel adjustment.[19] | 2018 | DCT[۷] | ۳۶,۲ dB |
| A Secure Spatial Domain Image Steganography u sing Genetic Algorithm and Linear Congruential Generator.[20] | 2018 | DWT[۸] ANN | ۳۶,۲۶ dB |
| A secure image steganography algorithm based on least significant bit and integer wavelet transform", .[21] | 2018 | FDM[۹] EAG | ۴۹,۰۱ dB |
| روش پیشنهادی این مقاله | | LSB VC[۱۰] | ۵۴,۵ dB |

[2] lifting wavelet transform

[3] Edge Adaptive Grid

[4] Integer wavelet transform

[5] Least Significant Bit

[6] Genetic Algorithm

[7] Discrete cosine transform

[8] Artificial Neural Network

[9] Flipping Distortion measurement

[1] Visual Cryptography

## ۶- نتیجه‌گیری

با پیاده‌سازی و بررسی روش‌های بالا نتایج زیر حاصل گردید:

- برای حل مشکل زیگزاگ شدن هیستوگرام تصویر، روش افزودن ضرایب پیشنهاد کردیم که با پیاده‌سازی این روش و مقایسه آن با روش بیت‌های کم‌ارزش تبدیل ویولت نتایج مطلوبی حاصل گردید که هم باعث تغییر بسیار کم شفافیت تصویر با افزایش نرخ داده ورودی شد و هم مشکل زیگزاگ هیستوگرام تصویر در روش بیت‌های کم‌ارزش تبدیل ویولت برطرف شد.
- درروش پیشنهادی، برخلاف سایر روش‌ها، رمزنگاری بصری به‌طور مستقیم بر روی تصاویر پیام انجام می‌شود و سپس با استفاده از پنهان‌نگاری تبدیل ویولت این تصاویر صورت می‌گیرد؛ اما در روش‌های ارائه‌شده ابتدا درروی پیام الگوریتم پنهان‌نگاری پیاده‌سازی می‌شد و سپس تصویر خروجی توسط الگوریتم رمز بصری به چند اشتراک نامفهوم تبدیل می‌شد.
- پیچیدگی محاسباتی این روش بسیار پایین است.
- چون الگوریتم رمز بصری بر روی تصاویر پیام پیاده‌سازی می‌شود و سپس پنهان‌نگاری بر روی اشتراک‌های نامفهوم تولیدشده توسط این الگوریتم انجام می‌شود. تصویر خروجی یک تصویر شفاف و با مفهوم است؛ این باعث می‌شود تا مهاجم در نگاه اول متوجه رمز شدن تصویر پیام نشود.
- پیاده‌سازی این الگوریتم ساده است.
- زمان بسیار کمی برای اجرای الگوریتم پیاده‌سازی شده لازم است.
- بازیابی تصویر رمز شده بسیار ساده است.
- پهن‌شدگی تصویر بازیابی شده که درروش رمزنگاری بصری وجود داشت برطرف شده است.
- تصویر بازیابی شده از کیفیت خوبی برخوردار است.

## مراجع


[1] Poonam Bidgar, Neha Shahare “Key based Visual Cryptography Scheme using Novel Secret Sharing Technique with Steganography” IOSR Journal of Electronics and Communication Engineering, Volume 8, Issue 2, Dec. 2013.

[2] Dr M. Umamaheswari, Prof. S. Sivasubramanian, S. Pandiarajan “Analysis of Different Steganographic Algorithms for Secured DataHiding”, IJCSNS International Journal of Computer Science andNetwork Security, VOL.10 No.8, Aug 2010.

[3] Siddaram Shetty, Minu P. Abraham “A Proposal to Secure Visual Cryptographic Shares of Secret Image using RSA” International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 12, Dec 2014.

[4] Biswapati lana, Partha Chowdhuri, Madhumita Mallick, Shyamal Kumar Mondal “Cheating Prevention in Visual Cryptography using Steganographic Scheme” IEEE Conference 2014.

[5] Mehdi Hussain and Mureed Hussain” A Survey of Image Steganography Techniques” International Journal of Advanced Science and Technology Vol. 54, May 2013.

[6] Mr. Deepak S. Bhiogade, Prof. Shaikh Phiroj Chhaware” Steganography and Visual Cryptography for Secured Data Hiding” International Conference on Industrial Automation and Computing (ICIAC),13th Apr 2014.

[7] Shaveta Mahajan, Arpinder Singh” A Review of Methods and Approach for Secure Stegnography” International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE),Volume 2, Issue 10, Oct 2012.

[8] Khalil Challita and Hikmat Farhat “Combining Steganography and Cryptography: New Directions” International Journal on New Computer Architectures and Their Applications (IJNCAA), 2011

[9] Ravindra Gupta, Akanksha Jain, Gajendra Singh ” Combine use of Steganography and Visual Cryptography for Secured Data hiding in Computer Forensics” (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (3) , 2012.

[10] Rita Rana, Dheerendra Singh, Steganography-Concealing Messages in Images Using LSB Replacement Technique with Pre-Determined Random Pixel and Segmentation of Image, International Journal ofComputer Science & CommunicationVol. 1, No. 2, pp. 113-116, JuL-Dec 2010.

[11] Rehana Begum R.D and Sharayu Pradeep “Best Approach for LSB Based Steganography

Using Genetic Algorithm and Visual Cryptography for Secured Data Hiding and Transmission over Networks" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 6, Jun 2014.

[12] Der-Chyuan Lou, Hong-Hao Chen, Hsien-Chu Wu, and Chwei-Shyong Tsai. A novel authenticable color visual secret sharing scheme using non-expanded meaningful shares. Displays, 32:118{134, Feb 2011.

[13] Moni Naor, Adi Shamir. Visual cryptography II: Improving the contrast via the cover base Security Protocols Security Protocols pp 197-202, 1996.

[14] Moni Naor, Adi Shamir. Visual cryptography, Security Protocols: Advances in Cryptology, EUROCRYPT'94, pp 1-12, 1994.

[15] Mitsuru Nakai,A Measure on the Harmonic Boundary of a Riemann Surface. Nagoya Mathematical Journal, Volume 17, pp. 181-218, August 1960.

[16] Kumar C, Singh AK, Kumar Pu"Improved wavelet-based image watermarking through SPIHT", Multimedia Tools and Applications, vol. 79, no.15, pp.11069-11082.

[17] Zheng Z, Saxena N, Mishra KK, Sangaiah AK, ," Guided Dynamic Particle Swarm Optimization for Optimizing Digital Image Watermarking in Industry Applications", vol.88, pp.92–106, 2018.

[18] M. Islam, A. Roy, R.H. Laskar, "Neural network based robust image watermarking technique in LWT domain", Journal of Intelligent & Fuzzy Systems, vol.u34, pp.u1691– 1700, 2018.

[20] I. Shafi, M. Noman, M. Gohar, A. Ahmad, M. Khan, S. Din, S.H. Ahmad, J. Ahmad, "An adaptive hybrid fuzzy-wavelet approach for image steganography using bit reduction and pixel adjustment", Soft Computing, vol.u22, no.5, pp.1555–1567, 2018.

[21] P.D. Shah, R.S. Bichkar, A Sec re Spatial Domain Image Steganography u using Genetic Algorithm and Linear Congr ential Generator, In International conference on intelligent computing and applications, pp.119-129, 2018.

[22] Emad, E., Safey, A., Refaat, A., Osama, Z., Sayed, E., & Mohamed, E. "A usec ureu image steganography algorithm based on least significant bit and integer wavelet transform", Journal of Systems Engineering and Electronics, vol.29, no.3,uupp.639– 649, 2018.