پنهان نگاری معکوس پذیر در تصاویر رمز شده با استفاده از پیش بینی کننده صفحه شطرنج

عمار محمدی[۱]، دانشجوی دکتری، منصور نخکش[۲]، دانشیار

۱- دانشکده مهندسی برق و کامپیوتر - دانشگاه یزد - یزد - ایران - mohammadi_a@stu.yazd.ac.ir
۲- دانشکده مهندسی برق و کامپیوتر - دانشگاه یزد - یزد - ایران - nakhkash@yazd.ac.ir

چکیده: این مقاله روشی جدیدی در پنهان نگاری معکوس پذیر در تصویر رمز شده معرفی می کند. در روش پیشنهادی بعد از رمز نگاری تصویر توسط صاحب تصویر، پنهان کننده پیام بدون اینکه هیچ اطلاعاتی از محتوای تصویر اصلی داشته باشد اقدام به ایجاد فضا به منظور پنهان نگاری داده می کند. این امر با بهره گیری از MSB[۱] پیکسل های تصویر رمز شده محقق می شود. این MSB ها تجمیع می شوند و بیت های داده در آنها تعبیه می گردد. این تجمیع قدرت بیشتری به منظور بازیابی بدون اتلاف تصویر اصلی در گیرنده ایجاد می کند. بنابراین با بهره گیری از این تجمیع و همچنین یک پیش بینی کننده مناسب نظیر پیش بینی کننده صفحه شطرنج می توان در گیرنده تصویر اصلی را بدون اتلاف بازیابی کرد. همچنین در طرح پیشنهادی استخراج داده تحت هر شرایطی بدون خطا انجام می شود. الگوریتم پیشنهادی بازیابی بدون اتلاف تصویر اصلی را حتی بدون داشتن کلید پنهان کننده داده محقق می سازد. نتایج آزمایش تایید می کند که الگوریتم پیشنهادی روش های مطرح در این زمینه را بهبود داده است.

واژه‌های کلیدی: بیت با بیشترین ارزش، پنهان نگاری معکوس پذیر، پیش بینی کننده صفحه شطرنج، تجمیع، تصویر رمز شده.

Reversible Data Hiding in Encrypted Images using Chessboard Predictor

Ammar Mohammadi [1], Ph.D Candidate, Mansor Nakhkash [2], Associate Professor

1- Faculty of Electrical and Computer Engineering, Yazd University, Yazd, Iran, Email: mohammadi_a@stu.yazd.ac.ir
2- Faculty of Electrical and Computer Engineering, Yazd University, Yazd, Iran, Email: nakhkash@yazd.ac.ir

Abstract: This paper presents a novel method in reversible data hiding in encrypted image. In the proposed method, after image encryption by image owner, data hider vacates room to embed data without having any knowledge of original content. It realizes employing most significant bit (MSB) of pixels in the encrypted image. These MSBs are integrated and data bits are embedded in the integrated ones. The integration provides more strength for lossless reconstruction of the original image at the recipient. Therefore, employing the integration and a proper predictor such as chessboard predictor, original image can be losslessly reconstructed at the recipient. Also, in the proposed scheme, error-free extraction of data is done under any circumstances. Proposed algorithm realizes lossless reconstruction of the original image even without having data hider key. Experimental results confirm that the proposed algorithm outperforms state of the art ones.

Keywords: MSB, reversible data hiding, chessboard predictor, integration, encrypted image.

نام نویسنده مسئول:
نشانی نویسنده مسئول: ایران - تبریز - بلوار ۲۹ بهمن - دانشگاه تبریز - دانشکده مهندسی برق و کامپیوتر

۱- مقدمه

در سال های اخیر به علت گسترش محاسبات ابری[۲] و فضای ذخیره ابری[۳] محققین بسیاری علاقمند به گسترش روش های پنهان نگاری معکوس پذیر در تصویر رمز شده شده اند [۱]. به طور کلی در هر روش رمز نگاری معکوس پذیر در تصویر رمز شده سه بخش عمل کننده داریم که عبارتند از : صاحب تصویر[۴]، پنهان کننده داده[۵] و گیرنده[۶]. صاحب تصویر کسی است که تصویر را قبل از ارسال برای سرپرست شبکه جهت حفظ حریم شخصی خود رمز می کند. پنهان کننده داده که می تواند سرپرست شبکه نیز باشد داده های مورد نیاز خود را در تصویر رمز شده تعبیه می کند. این داده ها می توانند مشخصات صاحب تصویر، داده های مربوط به مبدا و یا مقصد تصویر و غیره باشند. چالش هایی که در روش های پنهان نگاری معکوس پذیر در تصویر رمز شده مطرح می باشد افزایش ظرفیت تعبیه داده، امکان استخراج بدون خطای داده و بازیابی بدون اتلاف تصویر در گیرنده هستند.

روش های مطرح در پنهان نگاری معکوس پذیر در تصویر رمز شده به سه دسته اصلی تقسیم می شوند. که عبارتند از: الگوریتم هایی مبتنی بر ایجاد فضا قبل از رمز نگاری (**افقر**) [۲-۱۰]، ایجاد فضا توسط رمز نگاری (**افتر**) [۱۱-۱۷] و ایجاد فضا بعد از رمز نگاری (**افبر**) [۱۸-۲۳].

در **افقر** پیش از رمز نگاری پیش پردازشی به منظور ایجاد فضای خالی محقق می شود.

بیشتر روش ها در **افتر** بر مبنای استفاده از بایت های رمز یکسان به منظور رمز کردن چند پیکسل مجاور در تصویر شکل گرفته اند. در این روش ها همبستگی پیکسل ها مجاور در فرایند رمز نگاری حفظ می شود. اگرچه به واسطه حفظ این همبستگی پنهان کننده می تواند داده را در تصویر رمز شده پنهان کند وجود این همبستگی می تواند به معنای نشت اطلاعات تصویر اصلی نیز باشد.

روش های مطرح در **افقر** و **افتر** روش های جدایی پذیر هستند به این معنا که استخراج داده در گیرنده به داشتن تصویر رمز گشایی شده گره نخورده است. به بیان دیگر در روش های جدایی ناپذیر استخراج پیام تنها با داشتن تصویر رمز گشایی شده در گیرنده امکان پذیر است.

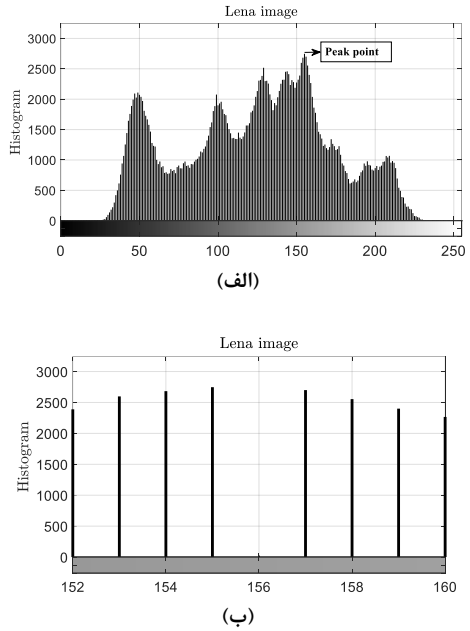
در طرح های **افبر** پنهان کننده هیچ اطلاعاتی از تصویر اصلی ندارد. تصویر اصلی رمز می شود و پنهان کننده ای که کاملا ناآگاه به اطلاعات تصویر اصلی است در تصویر رمز شده فضایی به منظور پنهان نگاری داده فراهم می کند. بعضی از روش های **افبر** مطرح شده جدایی پذیر [۱۸، ۲۰] و برخی دیگر جدایی ناپذیر [۱۹، ۲۱، ۲۲] هستند. در طرح [۲۳] دو روش مجزا یکی جدایی پذیر و دیگری جدایی ناپذیر مطرح شده است.

در نگاه کلی مشابه با طرح های پنهان نگاری معکوس پذیر بیشتر طرح ها در پنهان نگاری معکوس پذیر در تصویر رمز شده از همبستگی پیکسل های مجاور بهره می برند. علاوه بر این، آنها ایده های مطرح در پنهان نگاری معکوس پذیر نظیر تغییر هیستوگرام تصویر [۲۴]، گسترش تفاوت [۲۵] و محاسبه خطای پیش بینی [۲۶، ۲۷] را نیز به کار گرفته اند. به عنوان مثال طرح های [۵، ۸] گسترش خطا و طرح [۲] تغییر هیستوگرام خطای پیش بینی را به منظور ایجاد فضا قبل از رمز نگاری به کار گرفته اند. Huang و همکاران طرح جدیدی را در پنهان نگاری معکوس پذیر در تصویر رمز شده معرفی کردند که استفاده از بیشتر ایده های مطرح در پنهان نگاری معکوس پذیر را ممکن ساخته است [۱۵].

طرح های [۱۰، ۱۱] ایده پیش بینی کننده تفاوت محلی را به منظور تعبیه داده در تصویر رمز شده به کار گرفته اند. آنها بازیابی بدون اتلاف را برای تصویر اصلی و استخراج بدون خطای بیت های داده را محقق کردند. همچنین طرح [۲۰] همبستگی محلی پیکسل های همسایه را به منظور بازیابی تصویر اصلی در گیرنده به کار گرفته است. با بهره گیری از پیش بینی کننده MED[۷] ([۲۸])، Yin و همکاران برچسب هایی را برای هر پیکسل قبل از رمز نگاری در نظر گرفته اند [۴]. این برچسب ها سپس با بهره گیری از کدبندی هافمن فشرده و به همراه بیت های داده در تصویر رمز شده تعبیه می شوند. آنها طرح های [۱۰، ۱۱] را با کمک کدبندی منبع بهبود دادند.

فلاح پور و صداقی [۲۹] روشی را در پنهان نگاری معکوس پذیر مطرح می کنند که روش [۲۴] را در بلوک های غیر هم پوشان به منظور تعبیه داده با استفاده از تغییر هیستوگرام پیکسل ها در یک بلوک به کار می گیرد. در رویکردی مشابه Ge و همکاران [۱۶] روشی را در پنهان نگاری معکوس پذیر در تصویر رمز شده معرفی کردند که روش تغییر هیستوگرام تصویر ([۲۴]) را در بلوک های غیر هم پوشان از تصویر رمز شده به منظور ایجاد فضا برای تعبیه داده به کار بستند.

همان طور که بیان کردیم روش های زیادی در پنهان نگاری معکوس پذیر در تصویر رمز شده هستند که از ایده های مطرح در پنهان نگاری معکوس پذیر به منظور تعبیه داده در تصویر رمز شده بهره برده اند. در این مقاله روش جدیدی در پنهان نگاری معکوس پذیر در تصویر رمز شده به کار گرفته می شود که از ایده اولیه تغییر هیستوگرام تصویر برای ایجاد فضا بعد از رمز نگاری استفاده می کند. بیت های داده صرفاً در MSB های پیکسل های هدف تعبیه می شوند که این MSB ها در ادامه تجمیع می شوند و پنهان نگاری بر اساس تغییر هیستوگرام آنها محقق می شود. پیکسل های هدف پیکس هایی هستند که بیت های داده بر روی آنها تعبیه می شود. به عنوان ایده دیگر که در پنهان نگاری معکوس به کار گرفته شده ما از پیش بینی کننده صفحه شطرنج به منظور بازیابی بدون اتلاف تصویر اصلی در گیرنده بهره می بریم. در این مقاله از دو کلید مستقل رمز،



(الف)

(ب)

شکل ۱: (الف) هیستوگرام تصویر Lena. **(ب) ایجاد فضا به منظور تعبیه بیت های داده.**

K_e و K_d به ترتیب به منظور رمز کردن تصویر اصلی و بیت های داده استفاده می کنیم.

در طرح پیشنهادی نه تنها بیت های داده بدون خطا بازیابی می شوند بلکه فرایند استخراج این بیت ها جدا پذیر از بازیابی تصویر اصلی انجام می گردند. طرح پیشنهادی می تواند به عنوان یک روش کاربردی مطرح شود که الگوریتم های مطرح در پنهان نگاری معکوس پذیر در تصویر رمز شده را بهبود می دهد.

۲- کارهای مرتبط

روش پیشنهادی در این مقاله از ایده تغییر هیستوگرام تصویر بهره می گیرد. در روش ما پیش بینی کننده صفحه شطرنج به منظور بازیابی تصویر اصلی در گیرنده به وسیله تحلیل خطای پیش بینی به کار گرفته می شود. در این بخش به بررسی آنها با بیان جزئیات بیشتر می پردازیم.

۲-۱- تغییر هیستوگرام تصویر

همان طور که مطرح شده Ni و همکاران [۲۴] طرحی را در RDH با استفاده از تغییر هیستوگرام تصویر اصلی مطرح کردند. بدین منظور آنها بیت های داده را در نقطه بیشینه هیستوگرام که پیکسلی است با بیشترین تکرار در کل تصویر تعبیه می کنند. در این رویکرد آنها فضایی را به منظور پنهان نگاری داده به وسیله تغییر هیستوگرام تصویر فراهم می کنند به طوری که بازیابی تصویر اصلی به شکل معکوس پذیر امکان پذیر باشد. به عنوان مثال نقطه بیشینه در هیستوگرام Lena (شکل ۱- الف) عدد ۱۵۵ می باشد. به منظور ایجاد فضا تمام پیکسل های بیشتر از ۱۵۵ با عدد یک جمع می شوند (شکل ۱- ب). در روش پیشنهادی، ایده ایجاد فضا با تغییر هیستوگرام تصویر به کار گرفته می شود.

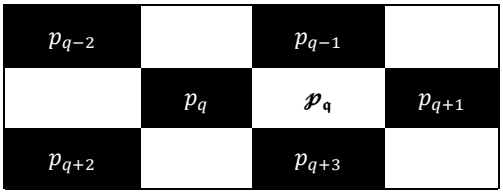
۲-۲- پیش بینی کننده صفحه شطرنج

پیش بینی کننده صفحه شطرنج که یک پیش بینی کننده غیر علی است می تواند پیش بینی بهتری از پیش بینی کننده های علی نظیر MED ([۲۸]) و GAP^A ([۳۰]) فراهم کند. در پیش بینی کننده صفحه شطرنج (شکل ۲) یک پیکسل سفید می تواند توسط همسایه های سیاهش پیش بینی شود. برای مثال پیش بینی یک پیکسل سفید ($\mathcal{P}_q$) با به کار گیری همسایه های سیاهش با استفاده از رابطه (۱) امکان پذیر می شود.

$$\tilde{\mathcal{P}}_q = \lfloor \frac{P_{q-1}+P_q+P_{q+1}+P_{q+3}}{4} \rceil \qquad (۱)$$

در جایی که $\lfloor . \rceil$ مقدار بدست آمده را به نزدیک ترین عدد حسابی گرد می کند. با استفاده از $\tilde{\mathcal{P}}_q$ و $\mathcal{P}_q$ خطای پیش بینی e_q به وسیله رابطه (۲) محاسبه می شود.

$$e_q = \mathcal{P}_q - \tilde{\mathcal{P}}_q \qquad (۲)$$



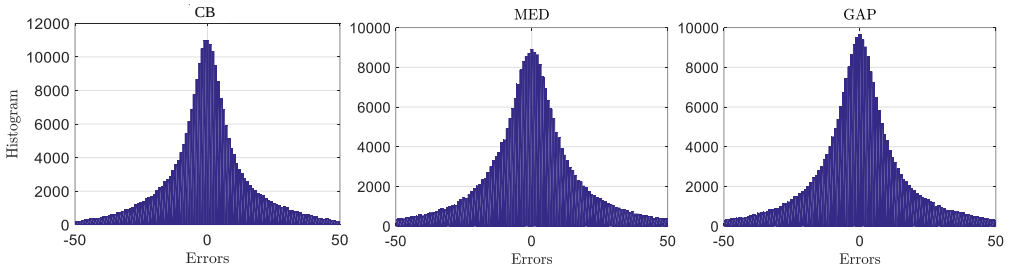
شکل ۲: بخشی از تصویر که پیکسل های آن به بخش های سیاه و سفید تقسیم شده اند.

۲-۳- آنالیز خطای پیش بینی

بر طبق رابطه (۲)، با داشتن خطای پیش بینی و مقدار پیش بینی شده از مقدار اصلی یک پیکسل، آن پیکسل قابل پیش بینی است. اگر چه در [۱۰] ما ثابت کردیم حتی با داشتن حدود خطا می توان چند بیت با ارزش بیشتر از پیکسل اصلی را نیز بازیابی کرد. برای توضیح بیشتر خطای پیش بینی ($\mathbb{e}$) که طبق رابطه (۳) از تفاوت پیکسل اصلی ($\mathfrak{p}$) و مقدار پیش بینی شده آن ($\mathbb{p}$) حاصل می شود را در نظر می گیریم.

$$\mathfrak{p} - \mathbb{p} = \mathbb{e} \qquad (۳)$$

در [۱۰] ما ثابت کردیم که حداقل یک بیت ظرفیت در MSB پیکسل "$\mathfrak{p}$" زمانی که رابطه (۴) برقرار باشد فراهم می شود.



شکل ۳: هیستوگرام خطای پیش بینی برای تصویر Baboon **که به وسیله پیش بینی کننده های صفحه شطرنج** (CB)، MED **و** GAP **ایجاد شده اند.**

$$|e| < 64 \qquad (۴)$$

به منظور بررسی بیشتر نمایش بیتی یک پیکسل را به صورت $p = p_7p_6p_5p_4p_3p_2p_1p_0$ که شامل ۸ بیت از LSB یعنی p_0 تا MSB یعنی p_7 است در نظر می گیریم. در صورت برقرار بودن رابطه (۴)، p_7 می تواند با یک بیت داده جایگزین شود به طوری که بتوان آن را در گیرنده بازیابی کرد.

با بهره گیری از پیش بینی کننده بهتر که باعث تحقق خطای پیش بینی کوچکتر می شود پیکسل های بیشتری وجود خواهند داشت که خطای پیش بینی آنها در رابطه (۴) صدق کند. بنابراین MSB های بیشتری می تواند به منظور تعبیه بیت های داده به کار گرفته شود.

هیستوگرام خطای پیش بینی که به وسیله پیش بینی کننده های MED ، GAP و صفحه شطرنج (CB[۹]) برای تصویر Baboon فراهم شده در شکل ۳ تشرح گریده است. پیش بینی کننده صفحه شطرنج بر روی تمام پیکسل ها اعمال شده اند. همان طور که نشان داده شده است پیش بینی کننده صفحه شطرنج هیستوگرام تیزتری از خطای پیش بینی نسبت به پیش بینی کننده های دیگر ایجاد می کند. به علاوه خطای پیش بینی با استفاده از پیش بینی کننده GAP هیستوگرام تیزتری نسبت به پیش بینی کننده MED دارد.

در این بین مسئله حائز اهمیت یافتن تعداد خطاهای پیش بینی است که اندازه آنها بیشتر از ۶۴ است. آنها نمی توانند حتی برای تعبیه یک بیت داده به کار گرفته شوند به این علت که در رابطه (۴) صدق نمی کنند. اگر "l" تعداد خطاهای پیش بینی با شند که رابطه (۴) را تایید نکنند و "L" تعداد کل خطای پیش بینی در کل تصویر باشد می توان $f_{predictor}$ را طبق رابطه (۵) تعریف کرد که نشان دهنده احتمال عدم بازیابی یک MSB تغییر یافته باشد که به طور تصادفی انتخاب شده است.

$$f_{predictor} = l/L \qquad (۵)$$

بر این اساس برای پیش بینی کننده های مختلف و برای تصویر Baboon داریم $f_{CB} = 0.0017$، $f_{GAP} = 0.014$ و $f_{MED} = 0.016$. اگرچه f_{CB} به طور قابل ملاحظه ای از بقیه کمتر است هنوز احتمال ایجاد خطا در بازیابی MSB در استفاده از پیش بینی کننده صفحه شطرنج نیز وجود دارد. در این مقاله به عنوان یک راه حل به منظور کاهش ریسک خطای بازیابی ما از روش تجمیع MSB های پیک سل های هدف بهره می گیریم. بنابراین MSB ها در دسته های $\mathcal{N}$ تایی تجمیع شده و مقدار تجمیع شده به منظور تعبیه بیت داده به کار گرفته می شود.

همیشه می توان مقداری برای $\mathcal{N}$ انتخاب کرد که بتواند بازیابی بدون اتلاف را تضمین کند. مقدار محاسبه شده برای $f_{pre.}$ نه تنها به نوع پیش بینی کننده بلکه به نوع تصویر انتخاب شده وابسته است. هر چقدر تصویر آنتروپی کمتری را ایجاد کند احتمال خطا در بازیابی بدون اتلاف تصویر کاهش می یابد. به بیان دیگر به طور کلی تصاویر نرم تر $f_{pre.}$ کمتر دارند. برای مثل برخلاف Baboon، برای Lena و F16، $f_{CB} = 0$ است. بر این اساس در روش پیشنهادی بهترین پیش بینی کننده یعنی پیش بینی کننده صفحه شطرنج به کار گرفته می شود.

۳- روش پیشنهادی

در این بخش جزئیات روش پیشنهادی مطرح می گردد که شامل رمز نگاری تصویر، درهم سازی ساده، نادرهم سازی ساده، تعبیه و استخراج بیت های داده، بازیابی تصویر اصلی و نمای کلی طرح پیشنهادی است.

۳-۱- رمز نگاری تصویر

رمز نگاری تصویر اصلی با استفاده از کلید K_e و توسط صاحب تصویر محقق می شود. به منظور رمز نگاری نه تنها امکان استفاده از هر روش رمز نگاری ممکن است بلکه امکان بهره گیری از هر الگوریتم رمز نگاری استاندارد فراهم شده است. تنها محدودیت این است که مکان پیکسل های تصویر در حین رمز نگاری تغییر نکنند. اگر این تغییر اتفاق بیافتد پنهان کننده پیام می باید اطلاعات مکان های تغییر کرده را داشته باشد تا پنهان نگاری به درستی محقق شود. بنابراین از نظر امنیت، صاحب تصویر می تواند هر الگوریتم رمز دلخواه را انتخاب کند.

الگوریتم ۱: تبدیل هر m_j کوچکتر از $2^{\mathcal{N}-1}$ به مقدار بزرگتر s_j.

```
for j = 0 to J do
s_j = m_j
  if (m_j < 2^(N-1)) then
      s_j = 2^N − 1 − m_j
  end if
end for
```

الگوریتم ۲: تعبیه بیت های داده.

```
for j = 0 to J do
c_j = s_j
  if (d̂_j == 1) then
    c_j = |2^N − 1 − s_j|
  end if
end for
```

الگوریتم ۳: استخراج بیت های داده.

```
for j = 0 to J do
  if (c_j < 2^(N-1)) then
     d̂_j = 1
  else if (2^(N-1) ≤ c_j < 2^N)
     d̂_j = 0
  end if
end for
```

الگوریتم ۴: بازیابی پیکسل های اصلی.

```
for j = 0 to J do
    q = N × (j + 1) − 1
  if (E''_j ≤ E'_j) then
     [p_(q−N+1), ..., p_q] = [p''_(q−N+1), ..., p''_q]
  else
     [p_(q−N+1), ..., p_q] = [p'_(q−N+1), ..., p'_q]
  end if
end for
```

الگوریتم ۵: ریسک بازیابی بدون اتلاف.

```
  if (R_j < 16 × N) then
      High risk
  else if (R_j < 32 × N) then
      Median risk
  else if (R_j < 64 × N) then
      Low risk
  else
      Very low risk
  end if
```

اگر تصویر اصلی را با O نمایش دهیم $\hat{O}$ نمایشی از تصویر رمز شده است. بر این اساس پیکسل هایی که $\hat{O}$ را شکل می دهند را به دو گروه پیکسل های هدف رمز شده سفید $\{\hat{p}_0, \hat{p}_1, \dots, \hat{p}_q, \dots, \hat{p}_Q\}$ و پیکسل های رمز شده سیاه $\{\hat{p}_0, \hat{p}_1, \dots, \hat{p}_q, \dots, \hat{p}_Q\}$ تقسیم می کنیم. پیکسل های رمز شده سیاه در حین فرایند پنهان نگاری داده بدون تغییر باقی می مانند و به منظور بازیابی پیکسل های هدف سفید در گیرنده به کار گرفته می شوند.

۳-۲- درهم سازی و نادرهم سازی ساده

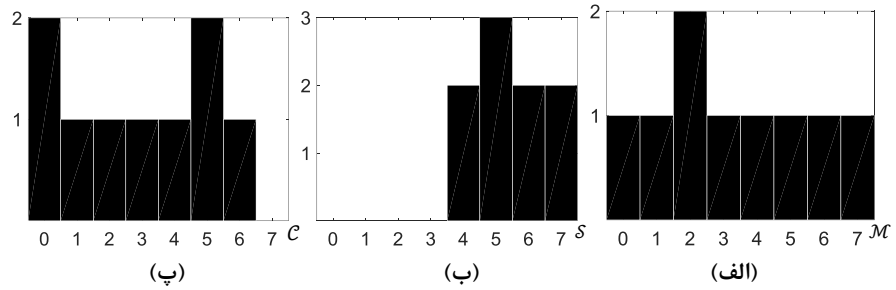
فرض می کنیم مجموعه $\mathcal{X} = \{x_0, x_1, \dots, x_q, \dots, x_Q\}$ موجود است. می خواهیم این مجموعه را به شیوه ای ساده درهم سازی کنیم. بدین منظور در ابتدا $\mathcal{X}$ را به $\mathcal{N}$ زیر مجموعه کوچکتر تقسیم می کنیم به طوری که هر کدام شامل $\frac{Q+1}{\mathcal{N}}$ عضو هستند، $\mathcal{N} \in \mathbb{N}$. با قرار دادن اعضای متناظر از هر مجموعه در کنار یکدیگر مجموعه در هم سازی شده $\mathcal{Y} = \{y_0, y_1, \dots, y_i, \dots, y_Q\}$ بدست می آید. تعداد اعضا در $\mathcal{X}$ به گونه ای انتخاب می شود که بر $\mathcal{N}$ بخش پذیر باشد. برای مثال با در نظر گرفتن $\mathcal{X} = \{x_0, x_1, x_2, x_3, x_4, x_5\}$ و $\mathcal{N} = 3$، با تقسیم $\mathcal{X}$ به سه زیر مجموعه کوچکتر داریم $\mathcal{X}_1 = \{x_0, x_1\}$, $\mathcal{X}_2 = \{x_2, x_3\}$ و $\mathcal{X}_3 = \{x_4, x_5\}$. مکان های جدید، $\mathcal{Y} = \{x_0, x_2, x_4, x_1, x_3, x_5\}$، با قرار دادن اعضای هر زیر مجموعه در کنار هم بدست می آید.

با در نظر گرفتن درهم سازی ساده که تبدیل $\mathcal{X}$ به $\mathcal{Y}$ است در شیوه معکوس مجموعه $\mathcal{Y}$ به $\frac{Q+1}{\mathcal{N}}$ زیر مجموعه کوچک تر شامل $\mathcal{N}$ عضو تقسیم می شود. اعضای مطابق با هر زیر مجموعه در کنار هم قرار می گیرند و $\mathcal{X}$ به شکل معکوس پذیر بازیابی می شود. به عنوان مثال با توجه به $\mathcal{Y} = \{x_0, x_2, x_4, x_1, x_3, x_5\}$ و $\mathcal{N} = 3$، $\mathcal{Y}$ به دو زیر مجموعه $\mathcal{Y}_1 = \{x_0, x_2, x_4\}$ و $\mathcal{Y}_2 = \{x_1, x_3, x_5\}$ تقسیم می شود. با کنار هم قرار دادن اعضای این دو زیر مجموعه $\mathcal{X} = \{x_0, x_1, x_2, x_3, x_4, x_5\}$ که نتیجه یک نادرهم سازی ساده است بازیابی می گردد.

۳-۳- پنهان نگاری بیت های داده با تجمیع و تجزیه MSB ها

بیت های داده در MSB های تجمیع شده از پیکسل های رمز شده تعبیه می شوند. با به کارگیری تجمیع چندین MSB به جای استفاده از فقط یک MSB، قدرت بیشتری به منظور بازیابی تصویر اصلی فراهم می شود. این تجمیع با اختصاص یک سطح باینری جدید برای $\mathcal{N}$ مقدار از MSB ها محقق می شود به طوری که مقدار بدست آمده از تجمیع کمتر از $2^{\mathcal{N}}$ می باشد. با تغییر هیستوگرام مقادیر حاصل از تجمیع، فضایی به منظور پنهان نگاری داده فراهم می شود.

$\hat{p}_q = \hat{p}_{(q,7)} \dots \hat{p}_{(q,3)} \dots \hat{p}_{(q,0)}$ را به عنوان نمایش بیتی از پیکسل رمز $\hat{p}_q$ از مقدار LSB، $\hat{p}_{(q,0)}$، تا MSB $\hat{p}_{(q,7)}$ در نظر می گیریم. همان طور که تشریح شد زمانی که رابطه (۴) برای p_q برقرار باشد، $\hat{p}_{(q,7)}$ می تواند با یک بیت داده جایگزین شود به طوری که به



شکل ۴: هیستوگرام یک مثال از مجموعه های $\mathcal{C}$، $\mathcal{S}$ و $\mathcal{M}$

طور کامل قابل بازیابی باشد. با داشتن $(\mathcal{Q}+1)$-MSBs از پیک سل های هدف، $\hat{\mathcal{P}}_7=\{\hat{\boldsymbol{p}}_{(0,7)},\hat{\boldsymbol{p}}_{(1,7)},\dots,\hat{\boldsymbol{p}}_{(\mathrm{q},7)},\dots,\hat{\boldsymbol{p}}_{(\mathcal{Q},7)}\}$، فرایند تجمیع به وسیله رابطه (۶) محقق می شود.

$$m_j=\sum_{k=0}^{\mathcal{N}-1}2^k\times\left(\hat{\boldsymbol{p}}_{(\mathrm{q}-k),7}\right),\ \mathrm{q}=\mathcal{N}\times(j+1)-1,\ j=0,1,\dots,\mathcal{J} \quad (۶)$$

بنابراین $\mathcal{M}=\{m_0,m_1,\dots,m_j,\dots,m_{\mathcal{J}}\}$، $0\le m_j<2^{\mathcal{N}}$، $\mathcal{J}=\frac{\mathcal{Q}-\mathcal{N}+1}{\mathcal{N}}$، نمایشی از MSB ها تجمیع شده است.

با توجه به طبیعت تصویر رمز شده، هیستوگرام $\mathcal{M}$ توزیع یکنواخت دارد. به منظور پنهان نگاری بیت های داده در $\mathcal{M}$، نیاز داریم فضایی را به وسیله تغییر هیستوگرام $\mathcal{M}$ فراهم کنیم. این مهم با تبدیل هر m_j کوچکتر از $2^{\mathcal{N}-1}$ به مقداری بزرگتر و یا برابر با $2^{\mathcal{N}-1}$ محقق می شود. بنابراین با انجام این تبدیل به وسیله الگوریتم ۱، $\mathcal{S}=\{s_0,s_1,\dots,s_j,\dots,s_{\mathcal{J}}\}$، $2^{\mathcal{N}-1}\le s_j<2^{\mathcal{N}}$ بدست می آید. در این الگوریتم اگر $m_j<2^{\mathcal{N}-1}$ باشد، این مقدار تبدیل به s_j که بیشترین تغییر بیتی را نسبت به m_j دارد می شود. به بیان دیگر m_j با مکمل[10] خودش جایگزین می گردد.

با فراهم شدن فضا، $(\mathcal{J}+1)$ بیت از داده رمز شده، $\widehat{\mathcal{D}}=\{\hat{d}_0,\hat{d}_1,\dots,\hat{d}_j,\dots,\hat{d}_{\mathcal{J}}\}$، با بهره گیری از الگوریتم ۲ در $\mathcal{S}$ تعبیه می شوند. لازم به ذکر است این داده ها قبل از تعبیه با استفاده از کلید K_d رمز شده اند. در این الگوریتم به منظور تعبیه یک بیت داده رمز شده با مقدار یک در s_j، این مقدار با مکمل یک خود جایگزین و به منظور تعبیه بیت صفر این مقدار بدون تغییر باقی می ماند.

با یک مثال روند پنهان نگاری داده را تشریح می کنیم. در این مثال $\mathcal{N}=3$ و مقادیر تجمیع شده ناشی از ۲۷ مقدار MSB به صورت $\mathcal{M}=\{3,0,4,7,2,2,6,1,5\}$ نمایش داده می شود. با به کارگیری الگوریتم ۱، فضایی به منظور پنهان نگاری داده فراهم می شود یعنی داریم $\mathcal{S}=\{4,7,4,7,5,5,6,6,5\}$. به بیان دیگر با استفاده از تغییر هیستوگرام $\mathcal{M}$ به معنی تغییر مقادیر بین ۰ و ۳ به مقادیر بزرگتر فضای خالی به منظور تعبیه $\widehat{\mathcal{D}}=\{1,1,0,1,0,0,1,0,1\}$ فراهم می شود. سرانجام با بهره گیری از الگوریتم ۲ مجموعه حامل $\mathcal{C}=\{3,0,4,0,5,5,1,6,2\}$ بدست می آید. هیستوگرام $\mathcal{M}$، $\mathcal{S}$ و $\mathcal{C}$ در شکل ۴ به ترتیب الف، ب و پ نمایش داده شده اند.

به منظور ایجاد یک تصویر رمز شده حامل در ابتدا مجموعه $\mathcal{C}$ با استفاده از رابطه (۷) تجزیه می شود.

$$\left[\!\left[\hat{\boldsymbol{p}}_{((\mathcal{N}\times j+k-1),7)}\right]\!\right]=mod\left(\left\lfloor\frac{c_j}{2^{\mathcal{N}-k}}\right\rfloor,2\right),\ 0\le j\le\mathcal{J},\ 0<k\le\mathcal{N} \quad (۷)$$

در نتیجه MSB های رمز شده حامل $[\![\hat{\mathcal{P}}_7]\!]=\{[\![\hat{\boldsymbol{p}}_{(0,7)}]\!],[\![\hat{\boldsymbol{p}}_{(1,7)}]\!],\dots,[\![\hat{\boldsymbol{p}}_{(\mathrm{q},7)}]\!],\dots,[\![\hat{\boldsymbol{p}}_{(\mathcal{Q},7)}]\!]\}$ فراهم می گردد. یک پیکسل حامل، $[\![\hat{\boldsymbol{p}}_{\mathrm{q}}]\!]$، $\mathrm{q}=0,1,\dots,\mathcal{Q}$. با جایگزینی $[\![\hat{\boldsymbol{p}}_{\mathrm{q},7}]\!]$ در MSB پیکسل $\hat{\boldsymbol{p}}_{\mathrm{q}}$ ایجاد و در نتیجه پیکسل های هدف سفید رمزشده حامل، $[\![\hat{\mathcal{P}}]\!]=\{[\![\hat{\boldsymbol{p}}_0]\!],[\![\hat{\boldsymbol{p}}_1]\!],\dots,[\![\hat{\boldsymbol{p}}_{\mathrm{q}}]\!],\dots,[\![\hat{\boldsymbol{p}}_{\mathcal{Q}}]\!]\}$، تشکیل می شوند.

۳-۴- استخراج بیت های داده

استخراج بیت های داده صرفا با داشتن کلید پنهان کننده داده، K_d، امکان پذیر است. در ابتدا، MSB های پیکسل های هدف سفید رمز شده حامل که با $[\![\hat{\mathcal{P}}_7]\!]$ نمایش داده می شوند انتخاب و به منظور بازیابی $\mathcal{C}$، تجمیع می شوند. این تجمیع توسط رابطه (۶) انجام می شود در جایی که $(\hat{\boldsymbol{p}}_{(\mathrm{q}-k),7})$ و $\boldsymbol{m}_j$ به ترتیب با $[\![\hat{\boldsymbol{p}}_{(\mathrm{q}-k),7}]\!]$ و $\boldsymbol{c_j}$، $\boldsymbol{j}=\boldsymbol{0,1},\dots,\boldsymbol{\mathcal{J}}$ جایگزین می گردد. در این مقاله پیکسل ها و مجموعه های بازیابی شده به صورت پررنگ[11] نمایش داده می شوند.

با داشتن $\boldsymbol{\mathcal{C}}=\{\boldsymbol{c_0},\boldsymbol{c_1},\dots,\boldsymbol{c_j},\dots,\boldsymbol{c_{\mathcal{J}}}\}$، استخراج داده با به کارگیری الگوریتم ۳ انجام می شود. در الگوریتم ۳، $\boldsymbol{j}$ امین بیت از داده رمز شده $\widehat{\boldsymbol{d_j}}$، با استفاده از $\boldsymbol{c_j}$ استخراج و داده های رمز شده با استفاده از K_d رمزگشایی شده و کل داده بازیابی می شود.

۳-۵- بازیابی تصویر اصلی

بازیابی تصویر اصلی با رمزگشایی تصویر رمزشده حامل با استفاده از K_e آغاز می شود. فرض کنیم $\mathcal{P}'=\{\boldsymbol{p}'_0,\boldsymbol{p}'_1,\dots,\boldsymbol{p}'_{\mathrm{q}},\dots,\boldsymbol{p}'_{\mathcal{Q}}\}$ پیکسل های هدف سفید رمز گشایی شده هستند. هدف بازیابی MSB های آنها است که با $\mathcal{P}'_7=\{\boldsymbol{p}'_{0,7},\boldsymbol{p}'_{1,7},\dots,\boldsymbol{p}'_{\mathrm{q},7},\dots,\boldsymbol{p}'_{\mathcal{Q},7}\}$ نمایش داده می شوند. بقیه بیت های پیکسل های رمزگشایی شده برابر با بیت های پیکسل های اصلی است.

فرایند بازیابی با محاسبه مکمل اول $\mathcal{P}'_7$ که با $\mathcal{P}''_7=\{\boldsymbol{p}''_{0,7},\boldsymbol{p}''_{1,7},\dots,\boldsymbol{p}''_{\mathrm{q},7},\dots,\boldsymbol{p}''_{\mathcal{Q},7}\}$ نمایش داده می شود ادامه می یابد.

با جایگزینی $\mathcal{P}_7'$ و $\mathcal{P}_7''$ در MSB پیکسل های هدف سفید رمزگشایی شده دو دسته پیکسل نامزد داریم که عبارتند از $\mathcal{P}' = \{\mathcal{p}_0', \mathcal{p}_1', \dots, \mathcal{p}_q', \dots, \mathcal{p}_Q'\}$ و $\mathcal{P}'' = \{\mathcal{p}_0'', \mathcal{p}_1'', \dots, \mathcal{p}_q'', \dots, \mathcal{p}_Q''\}$. با تجمیع $\mathcal{N}$- خطای پیش بینی برای هر دو نامزد، تابع هزینه ای به منظور انتخاب یک دسته $\mathcal{N}$ – پیکسلی از میان این دو نامزد به عنوان دسته بازیابی شده پیکسل های اصلی در نظر گرفته می شود. در ادامه این شیوه با جزییات بیشتر تشریح می گردد.

با رمزگشایی، پیکسل های سیاه به صورت کامل بازیابی می شوند زیرا آنها در فرایند تعبیه داده دست نخورده باقی مانده بودند. آنها به منظور پیش بینی پیکسل های متعلق به دو نامزد با استفاده از رابطه (۱) استفاده می شوند به طوری که در این رابطه $\mathcal{p}_q$ با $\mathcal{p}_q'$ و یا $\mathcal{p}_q''$، $0 \le q \le Q$، جایگزین می شود. بنابراین با داشتن مقادیر پیش بینی شده از دو نامزد متفاوت، خطای پیش بینی آنها $\mathcal{P}_e' = \{e_0', e_1', \dots, e_q', \dots, e_Q'\}$ و $\mathcal{P}_e'' = \{e_0'', e_1'', \dots, e_q'', \dots, e_Q''\}$ با استفاده از رابطه (۲) محاسبه می شود. در ادامه تجمیع $\mathcal{N}$ مقدار از خطا با استفاده از رابطه (۸) به عنوان مثال برای $\mathcal{P}_e'$ انجام می شود.

$$\mathcal{E}_j' = \sum_{k=0}^{\mathcal{N}-1} \left| e'_{(q-k)} \right|, q = \mathcal{N} \times (j+1) - 1 \qquad (۸)$$

به طور مشابه، $\mathcal{E}_j''$ با استفاده از رابطه (۸) برای $\mathcal{P}_e''$، در جایی که $e'_{(q-k)}$ با $e''_{(q-k)}$ جایگزین می شود بدست می آید. در نهایت $\mathcal{N}$ – پیکسل اصلی که می تواند متعلق به $\mathcal{P}'$ و یا $\mathcal{P}''$ باشد با مقایسه $\mathcal{E}_j'$ و $\mathcal{E}_j''$ و با به کارگیری الگوریتم ۴ بازیابی می شود. بر این اساس برای هر j، اگر $\mathcal{E}_j' \le \mathcal{E}_j''$، $\mathcal{N}$ – پیکسل های بازیابی شده متعلق به $\mathcal{P}''$ و به صورت برعکس آنها به $\mathcal{P}'$ تعلق دارد. در نهایت پیکسل های بازیابی شده با $\boldsymbol{\mathcal{P}} = \{\mathcal{p}_0, \mathcal{p}_1, \dots, \mathcal{p}_q, \dots, \mathcal{p}_Q\}$ نمایش داده می شوند.

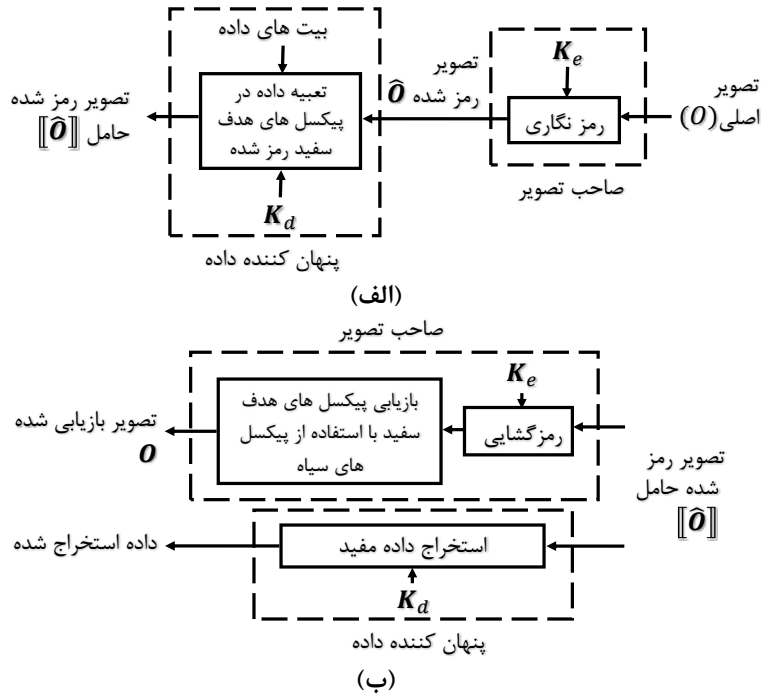
اگر $[\mathcal{p}_{q-\mathcal{N}+1}, \dots, \mathcal{p}_q] = [\mathcal{p}_{q-\mathcal{N}+1}, \dots, \mathcal{p}_q]$ به معنای بازیابی بدون اتلاف $\mathcal{N}$ – پیکسل از تصویر اصلی است. اگر $\mathcal{E}_j'$ و $\mathcal{E}_j''$ به هم نزدیک باشند ریسک بالایی در بازیابی بدون اتلاف پیکسل های اصلی وجود خواهد داشت. بنابراین ریسک بازیابی بدون اتلاف با محاسبه تفاوت بین $\mathcal{E}_j'$ و $\mathcal{E}_j''$ بررسی می شود.

$$\mathcal{R}_j = \left| \mathcal{E}_j' - \mathcal{E}_j'' \right| \qquad (۹)$$

هر چقدر $\mathcal{R}_j$ بزرگتر باشد ریسک کمتری برای بازیابی بدون اتلاف فراهم می شود و برعکس. به کارگیری $\mathcal{R}_j$ و $\mathcal{N}$ در الگوریتم ۵ می توان چهار نوع ریسک مختلف را تعریف کرد که عبارتند از ریسک بالا، ریسک متوسط، ریسک پایین و ریسک بسیار پایین. بنابراین برای هر دسته $\mathcal{N}$ – پیکسلی سنجشی از ریسک بازیابی داریم. هر چقدر $\mathcal{N}$ بزرگتر انتخاب شود ارزیابی دقیق تری از ریسک حاصل می شود.

۳-۶- نگاه کلی به طرح پیشنهادی

شکل ۵ - الف نمایی کلی از طرح پیشنهادی است. تعبیه داده بر روی پیکسل های هدف سفید رمز شده همان طور که در بخش ۳-۳ تشریح گردید انجام می شود. در این بین پیکسل های سیاه فقط رمز می شوند و داده بر روی آنها تعبیه نمی شود. آنها به منظور بازیابی



شکل ۵ : نمای کلی از طرح پیشنهادی. (الف) تعبیه بیت های داده و ایجاد تصویر رمز شده حامل. (ب) استخراج بیت های داده و بازیابی تصویر اصلی.

پیکسل های دیگر در گیرنده به کار گرفته می شوند. آنها ۵۰ در صد از تصویر را تشکیل می دهند.

اگر اندازه یک تصویر را $\mathbb{P} \times \mathbb{Q}$ در نظر بگیریم با توجه به مقدار انتخاب شده از $\mathcal{N}$ و به کار گیری تمام پیکسل های هدف سفید، کل ظرفیت تعبیه داده از رابطه زیر حاصل می شود.

$$\mathbb{P} \times \mathbb{Q} \times (\frac{1}{2\mathcal{N}}) \qquad (۱۰)$$

طبق این رابطه با انتخاب $\mathcal{N} = 1$ بیشترین ظرفیت تعبیه برابر است با $\frac{1}{2}(\mathbb{P} \times \mathbb{Q})$.

در شکل ۵ – ب استخراج بیت های داده و بازیابی تصویر اصلی تشریح گردیده است که می توانند به شیوه جدایی پذیر محقق شوند.

استخراج داده از پیکسل های هدف سفید رمز شده حامل همان طور که در زیر بخش ۳-۴ تشریح گردید محقق می شود.

بازیابی تصویر با رمزگشایی تصویر رمز شده حامل با استفاده از کلید K_e شروع می شود. بنابراین پیکسل های سیاه صرفا با رمز گشایی بازیابی می شوند. با داشتن پیکسل های سیاه، پیکسل های هدف سفید همان طور که در بخش ۳-۵ تشریح گردید بازیابی می گردند. ریسک بازیابی بدون اتلاف برای دسته های $\mathcal{N}$ پیکسلی در حین بازیابی می تواند محاسبه شود.

اگر MSB پیکسل های هدف را به صورت پشت سرهم به منظور تجمیع در نظر بگیریم MSB پیکسل های ناصافتر نیز می توانند در کنار هم قرار بگیرند. بنابراین با درهم سازی MSB ها می توانیم ریسک بازیابی بدون اتلاف را کاهش دهیم. به بیان دیگر درهم سازی از تجمیع و در کنار هم قرار گرفتن MSB هایی که متعلق به پیکسل های ناصاف هستند جلوگیری می کند. اگر چه درهم سازی می تواند به شکل تصادفی و با استفاده از کلید K_d انجام شود به منظور پیچیدگی کمتر در طرح پیشنهادی درهم سازی برای MSB های رمز شده، $\hat{\mathcal{P}}_7$، به شیوه ای ساده همان طور که در بخش ۳-۲ تشریح گردید انجام می شود. بنابراین به منظور افزایش کارایی در بازیابی بدون اتلاف مجموعه های درهم سازی شده تجمیع و داده بر روی آنها تعبیه و در نهایت نادرهم سازی می گردند تا پیکسل های رمز شده حامل متناظر را تشکیل دهند.

در گیرنده، MSB های پیکسل های هدف رمز شده به منظور استخراج داده به روش مشابه درهم سازی می شود. بر این اساس به منظور بازیابی تصویر اصلی خطاهای پیش بینی درهم سازی می شوند. بنابراین در الگوریتم ۴ می باید پیکسل های متناظر با خطاهای درهم سازی شده به منظور بازیابی مقادیر اصلی در نظر گرفته شود.

۴- نتایج آزمایش

کارایی الگوریتم پیشنهادی که یک الگوریتم **افبر** جدایی پذیر است با انجام چندین آزمایش در این بخش بررسی می شود. ۱۲ تصویر F16، Lena، Splash، House، Boat، Elaine، Lake، Peppers، Baboon، Stream، Aerial و APC از پایگاه داده USC-SIPI به عنوان تصاویر تست در نظر گرفته شده و چندین آزمایش به منظور تشریح کارایی الگوریتم پیشنهادی به خصوص از نظر افزایش ظرفیت تعبیه داده در نظر گرفته می شوند. همچنین ۱۰۰۰۰ تصویر از پایگاه داده BOWS2 به منظور اثبات این موضوع که بازیابی بدون اتلاف و استخراج بدون خطای داده در طرح پیشنهادی محقق شده است به کار گرفته می شوند. تمام تصاویر دارای اندازه 512×512 هستند. در این آزمایش دو سطر و یا ستون اول و یا آخر از تصویر در نظر گرفته نمی شوند. PSNR[۱۲] به عنوان معیاری به منظور تخمین کیفیت تصویر بازیابی شده در نظر گرفته شده و PSNR= ∞ به معنی بازیابی بدون اتلاف تصویر اصلی است.

انتخاب $\mathcal{N}$ می تواند مرتبط با آنتروپی یک تصویر باشد. هر چقدر آنتروپی یک تصویر بیشتر باشد مقادیر بیشتری برای $\mathcal{N}$ به منظور بازیابی بدون اتلاف در نظر گرفته می شود. با انتخاب مقادیر بیشتر برای $\mathcal{N}$ ظرفیت تعبیه کمتری فراهم می شود. بنابراین یک بده بستانی بین ظرفیت تعبیه و PSNR با توجه به انتخاب مقدار $\mathcal{N}$ وجود دارد. در جدول ۱، مقدار دقیقی از $\mathcal{N}$ به منظور بازیابی بدون اتلاف تصاویر تست در نظر گرفته شده است. با انتخاب $\mathcal{N} = 1$ برای تصاویر F16، Lena، Splash، House، Elaine و Peppers بیشترین مقدار ممکن برای تعبیه داده که مقدار ۱۳۰۰۵۰ بیت است فراهم می شود. در طرف دیگر در تصاویر Boat، Lake، Baboon، Stream، Aerial و APC میزان ظرفیت نصف این مقدار یعنی ۶۵۰۲۵ است. همچنین در این جدول ریسک بازیابی بدون اتلاف با محاسبه تعداد دسته های $\mathcal{N}$ – پیکسلی که ریسک بالا و یا میانی دارند ارزیابی می شود. اگرچه، تصاویر F16، Peppers و Baboon بدون اتلاف بازیابی شدند به ترتیب شامل 4، 8 و 5 دسته $\mathcal{N}$ – پیکسلی با ریسک بالا هستند.

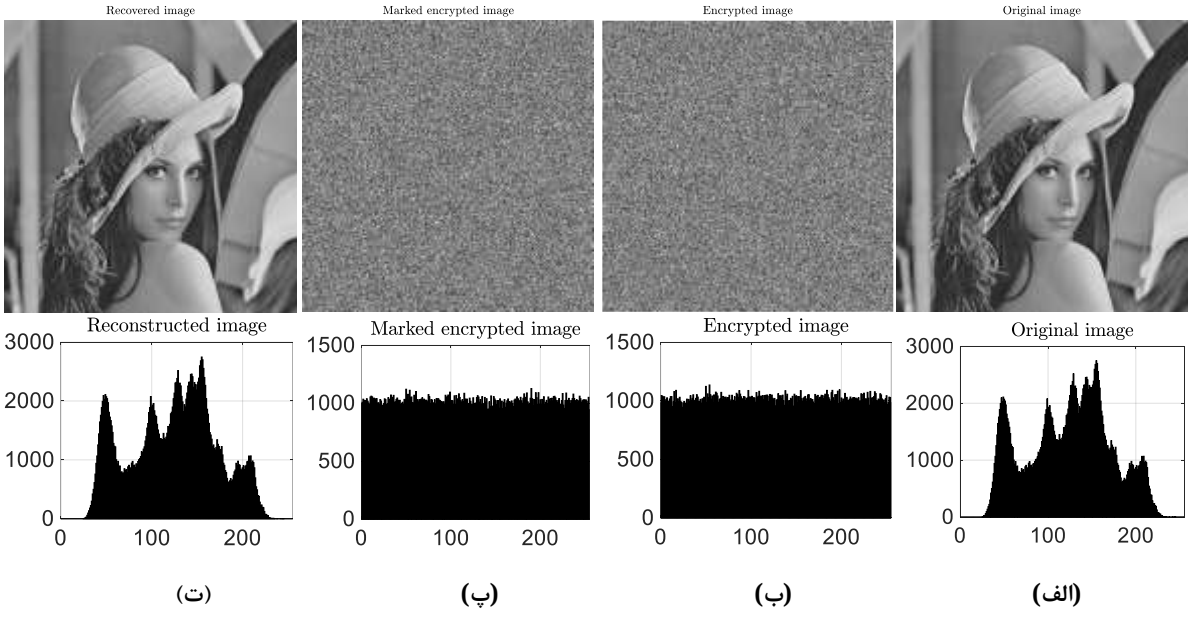
از طرف دیگر فرض می کنیم پنهان کننده پیام در طرح پیشنهادی به طور کامل نسبت به محتوای اصلی تصویر ناآگاه است و هیچ ویژگی و یا اطلاعاتی از آن ندارد بنابراین یافتن کمترین مقدار ممکن برای $\mathcal{N}$ به منظور بازیابی بدون اتلاف امکان پذیر نیست ولی می توان همیشه مقداری برای $\mathcal{N}$ یافت که برای مجموعه ای از تصاویر، بازیابی بدون اتلاف محقق شود. با آزمایش بر روی ۱۰۰۰۰ تصویر تست از پایگاه داده BOWS2 مشخص شد که با انتخاب $\mathcal{N} = 4$، بازیابی کامل برای تمام تصاویر تست محقق شده است.

جدول۱: تحلیل کارایی الگوریتم پیشنهادی با به کار گیری دوازده تصویر تست.

موارد		تصاویر											
		F16	Lena	Splash	House	Boat	Elaine	Lake	Peppers	Baboon	Stream	Aerial	APC
ظرفیت تعبیه (بیت)		۱۳۰۰۵۰	۱۳۰۰۵۰	۱۳۰۰۵۰	۱۳۰۰۵۰	۶۵۰۲۵	۱۳۰۰۵۰	۶۵۰۲۵	۱۳۰۰۵۰	۶۵۰۲۵	۶۵۰۲۵	۶۵۰۲۵	۶۵۰۲۵
$\mathcal{N}$		۱	۱	۱	۱	۲	۱	۲	۱	۲	۲	۲	۲
PSNR		∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
دسته های $\mathcal{N}$ پیکسلی	ریسک بالا	۴	۰	۰	۰	۰	۰	۰	۸	۵	۰	۰	۰
	ریسک متوسط	۱۳۶	۸۰	۴	۱۶۳	۴۴	۲۷	۲	۱۶۱	۱۰۵۲	۱۸۲	۱۳۰	۴

جدول۲: مقایسه بر اساس کارایی بین روش پیشنهادی و طرح های افبر تجزیه پذیر دیگر برای نه تصویر تست.

طرح ها	موارد	تصاویر								
		F16	Lena	Splash	House	Boat	Elaine	Lake	Peppers	Baboon
Zhang2012 [۱۸]	ظرفیت تعبیه (بیت)	۱۹۲۰	۱۹۲۰	۱۹۲۰	۱۹۲۰	۱۹۲۰	۱۹۲۰	۱۹۲۰	۱۹۲۰	۱۹۲۰
	LR	موفق	موفق	موفق	موفق	موفق	موفق	موفق	موفق	موفق
	LR فقط توسط K_e	ناموفق	ناموفق	ناموفق	ناموفق	ناموفق	ناموفق	ناموفق	ناموفق	ناموفق
Wu [۲۳]	ظرفیت تعبیه (بیت)	**۱۳۰۰۵۰**	**۱۳۰۰۵۰**	**۱۳۰۰۵۰**	**۱۳۰۰۵۰**	**۱۳۰۰۵۰**	**۱۳۰۰۵۰**	**۱۳۰۰۵۰**	**۱۳۰۰۵۰**	**۱۳۰۰۵۰**
	LR	**موفق**	**موفق**	**موفق**	**ناموفق**	**ناموفق**	**موفق**	**ناموفق**	**ناموفق**	**ناموفق**
	LR فقط توسط K_e	**موفق**	**موفق**	**موفق**	**ناموفق**	**ناموفق**	**موفق**	**ناموفق**	**ناموفق**	**ناموفق**
Qian [۲۰]	ظرفیت تعبیه (بیت)	۷۷۳۷۶	۷۷۳۷۶	۷۷۳۷۶	۷۷۳۷۶	۷۷۳۷۶	۷۷۳۷۶	۷۷۳۷۶	۷۷۳۷۶	۷۷۳۷۶
	LR	موفق	موفق	موفق	موفق	موفق	موفق	موفق	موفق	موفق
	LR فقط توسط K_e	ناموفق	ناموفق	ناموفق	ناموفق	ناموفق	ناموفق	ناموفق	ناموفق	ناموفق
طرح پیشنهادی	ظرفیت تعبیه (بیت)	**۶۵۰۲۵**	**۶۵۰۲۵**	**۶۵۰۲۵**	**۶۵۰۲۵**	**۶۵۰۲۵**	**۶۵۰۲۵**	**۶۵۰۲۵**	**۶۵۰۲۵**	**۶۵۰۲۵**
	LR	**موفق**	**موفق**	**موفق**	**موفق**	**موفق**	**موفق**	**موفق**	**موفق**	**موفق**
	LR فقط توسط K_e	**موفق**	**موفق**	**موفق**	**موفق**	**موفق**	**موفق**	**موفق**	**موفق**	**موفق**



شکل ۶: تشریح بصری از طرح پیشنهادی

۴-۱- تشریح بصری طرح پیشنهادی

شکل ۶ تشریح بصری از طرح پیشنهادی شامل تصویر اصلی، رمز شده، رمز شده حامل و بازیابی شده به همراه هیستوگرام هایشان است. الگوریتم رمز AES در حالت کانتر[۱۳] به عنوان یک روش دنباله رمز برای رمز کردن تصویر تست Lena به کار گرفته می شود. همان طور که در شکل ۶ – ب نمایش داده شده است بعد از رمز نگاری تصویر هیچ اطلاعاتی از تصویر اصلی باقی نمانده است. به عنوان یک دلیل می توان به هیستوگرام آن اشاره کرد که توزیع یکنواخت دارد. ما امنیت الگوریتم پیشنهادی را به دلیل داشتن دو ویژگی مهم

تضـــمین می کنیم که عبارتند از: ۱- هیچ ویژگی و یا اطلاعاتی از تصویر اصلی باقی نمانده که رمز نشده باشد. ۲- انتخاب الگوریتم رمز دلخواه اســت. ازآنجاکه پنهان کننده پیام در روش پیشـــنهادی هیچ آگاهی نسـبت به محتوای اصـلی ندارد این روش حریم خصـوصـی صاحب تصویر را کاملا حفظ می کند. علاوه بر این صاحب تصویر می تواند محتوای اصلی را با هر الگوریتم رمز دلخواهی رمز کند.

شکل ۶ – پ توصیفی از تصویر رمز شده حامل است. هیستوگرام همچنان توزیع یکنواخت خود را حفظ کرده است. تصویر اصلی همان طور که در شـکل ۶ – ت نمایش داده شـده اسـت به صـورت بدون اتلاف بازیابی شده است.

۴-۲- مقایسه با طرح های دیگر

روش های **افبر** تجزیه پذیر از بقیه روش های این حوزه کاربردی تر ه ستند. روش پی شنهادی تنها روش مطرح در این حوزه ا ست که بازیابی بدون اتلاف (LR[۱۴]) تصویر اصلی را صرفا با داشتن K_e ممکن ساخته است. در اینجا با چندین آزمایش این امر را ثابت می کنیم.

در جدول ۲، طرح پیشنهادی با طرح های **افبر** تجزیه پذیر دیگر مقایسه شده ا ست. طرح های [۱۸، ۲۰] برخی از بیت های پیکسل های رمز شده را به منظور تعبیه بیت های داده فشرده می کنند. در این بین آنها پارامترهایی را به کار می گیرند که می تواند بده بستانی را بین ظرفیت تعبیه و بازیابی بدون اتلاف فراهم کند. این کارکرد برای این طرح ها مشـابه با کارکرد $\mathcal{N}$ برای طرح پیشـنهادی اسـت. برای مقایسـه منصـفانه بین طرح پیشـنهادی و روش های [۱۸، ۲۰] این پارامترها به گونه ای انتخاب شـدند که بازیابی بدون اتلاف برای همه تصـاویر تسـت محقق شـود. در این روش پارامتر های $\{M = 4, S = 2, L = 271\}$، $\{q = 0.1\}$ و $\{\mathcal{N} = 2\}$ بـه ترتیـب برای طرح های [۱۸، ۲۰] و طرح پی شنهادی در نظر گرفته شده اند. با انتخاب مقادیر کوچکتر برای L، q و $\mathcal{N}$ به ترتیب برای طرح های [۱۸، ۲۰] و طرح پیشـــنهادی ظرفیت تعبیه داده و ریســک بازیابی بدون اتلاف تصـــویر تواماً افزایش می یابند. این امر احتمال خطای بیشتری در بازیابی بدون اتلاف ایجاد می کند.

در [۲۰] به منظور بازیابی بدون اتلاف در گیرنده اطلاعاتی مورد نیاز ا ست که تنها با دا شتن K_d قابل د سترس ا ست. بنابراین همان طور که در جدول ۲ تشـریح شـده اسـت بدون داشـتن K_d تنها یک نسخه باکیفیت از تصویر اصلی قابل بازیابی است در حالی که در طرح پی شنهادی بازیابی بدون اتلاف به طور کامل انجام می شود. هر چند که [۲۰] ظرفیت بی شتری را نسبت به طرح پی شنهادی ایجاد کرده است.

همان طور که در جدول ۲ توصیف شده است در مقایسه با [۱۸] ظرفیت تعبیه داده در طرح پی شنهادی افزایش یافته ا ست. م شابه با [۲۰] الگوریتم آنها نیز به داشـــتن K_d به منظور بازیابی بدون اتلاف تصویر اصلی وابسته است.

در [۲۳] با توجه به K_d، آنها چندین پیکسل هدف در تصویر رمز شـده را به منظور تعبیه داده انتخاب و یک پیش بینی کننده که می توان آن را تغییر یافته پیش بینی کننده صـفحه شـطرنج دانسـت به منظور بازیابی تصـویر اصـلی در گیرنده به کار می گیرند. روش آنها بازیابی بدون اتلاف را تضـمین نمی کند اگرچه این مهم در طرح آنها با کاهش تعداد پیکسـل های هدف انتخاب شـده در شـرایط خاص امکان پذیر اسـت. در این آزمایش بیشـترین مقدار از پیکسـل های هدف قابل انتخاب شدن در طرح [۲۳] را در نظر می گیریم. با توجه به موارد مطرح شده الگوریتم آنها نمی تواند ۵ تصویر تست از مجموع ۹ تصویر تست را بدون اتلاف بازیابی کند. همان طور که در جدول ۲ تشریح شده ا ست ما الگوریتم آنها را با طراحی شیوه ای که بازیابی بدون اتلاف را تضـمین می کند بهبود دادیم. این امر با به کار گیری تغییر هیستوگرام تصویر و تجمیع MSB ها محقق می شود. هر چند هزینه آن کاهش ظرفیت تعبیه داده اسـت. در تمام روش های مطرح و روش پیشنهادی استخراج بیت های داده بدون خطا انجام می شود.

۵- نتیجه

در این مقاله، با مقایســـه پیش بینی کننده های مختلف، نشـــان دادیم که پیش بینی کننده صفحه شطرنج بهترین پیش بینی کننده به منظور کاهش احتمال خطا در بازیابی تصویر اصلی است. با بررسی خطای پیش بینی، ما صرفاً MSB پیکسل های هدف رمز شده را به منظور تعبیه بیت های داده انتخاب می کنیم. این MSB ها تجمیع شـده و نسـبت به خطا در بازیابی مقاوم تر می گردند. با به کارگیری تغییر هیستوگرام مقادیر تجمیع شده، فضا به منظور تعبیه بیت های داده فراهم می شـود. در گیرنده با یک روش جداپذیر، بیت های داده اسـتخراج و تصـویر اصـلی بازیابی شـده و با تحلیل ریسـک، احتمال بازیابی بدون اتلاف م شخص می شود. نتایج آزمایش ن شان می دهد طرح پیشـــنهادی تنها طرح مطرح در **افبر** جدایی پذیر اســـت که بازیابی بدون اتلاف را صرفا با داشتن K_e محقق می کند.

مراجع

[1] Y.-Q. Shi, X. Li, X. Zhang, H.-T. Wu, and B. Ma, "Reversible data hiding: advances in the past two decades," *IEEE Access*, vol. 4, pp. 3210-3237, 2016.

[2] S. Xiang, and X. Luo, "Reversible data hiding in homomorphic encrypted domain by mirroring ciphertext group," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 28, no. 11, pp. 3099-3110, Nov. 2018.

[3] K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, "Reversible data hiding in encrypted images by reserving room before encryption," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 3, pp. 553-562, Mar. 2013.

[4] Z. Yin, Y. Xiang, and X. Zhang, "Reversible data hiding in encrypted images based on multi-MSB prediction and huffman coding," *IEEE Transactions on Multimedia*, Aug. 2019.

[5] Y.-C. Chen, T.-H. Hung, S.-H. Hsieh, and C.-W. Shiu, "A new reversible data hiding in encrypted image based on multi-secret sharing and lightweight cryptographic algorithms," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 12, pp. 3332-3343, Dec. 2019.

[6] X. Zhang, J. Long, Z. Wang, and H. Cheng, "Lossless and reversible data hiding in encrypted images with public-key cryptography," *IEEE Transactions on Circuits and Systems for Video Technology,* vol. 26, no. 9, pp. 1622-1631, Sep. 2016.
[7] X. Cao, L. Du, X. Wei, D. Meng, and X. Guo, "High capacity reversible data hiding in encrypted images by patch-level sparse representation," *IEEE Transactions on Cybernetics,* vol. 46, no. 5, pp. 1132-1143, May, May 2016.
[8] C.-W. Shiu, Y.-C. Chen, and W. Hong, "Encrypted image-based reversible data hiding with public key cryptography from difference expansion," *Signal Processing: Image Communication,* vol. 39, pp. 226-233, Nov. 2015.
[9] P. Puteaux, and W. Puech, "An efficient MSB prediction-based method for high-capacity reversible data hiding in encrypted images," *IEEE Transactions on Information Forensics and Security,* vol. 13, no. 7, pp. 1670-1681, Jul. 2018.
[10] A. Mohammadi, and M. Nakhkash, "Reversible data hiding in encrypted images using local difference of neighboring pixels," *arXiv preprint arXiv:1907.05123,* 2019.
[11] S. Yi, and Y. Zhou, "Separable and reversible data hiding in encrypted images using parametric binary tree labeling," *IEEE Transactions on Multimedia,* vol. 21, no. 1, pp. 51-64, Jan. 2019.
[12] D. Xu, and R. Wang, "Separable and error-free reversible data hiding in encrypted images," *Signal Processing,* vol. 123, pp. 9-21, Jun. 2016.
[13] Z. Yin, B. Luo, and W. Hong, "Separable and error-free reversible data hiding in encrypted image with high payload," *The Scientific World Journal,* vol. 2014, Apr. 2014.
[14] W. Zhang, K. Ma, and N. Yu, "Reversibility improved data hiding in encrypted images," *Signal Processing,* vol. 94, no. 1, pp. 118-127, Jan. 2014.
[15] F. Huang, J. Huang, and Y.-Q. Shi, "New framework for reversible data hiding in encrypted domain," *IEEE Transactions on Information Forensics and Security,* vol. 11, no. 12, pp. 2777-2789, Dec. 2016.
[16] H. Ge, Y. Chen, Z. Qian, and J. Wang, "A high capacity multi-level approach for reversible data hiding in encrypted images," *IEEE Transactions on Circuits and Systems for Video Technology,* vol. 29, no. 8, pp. 2285 - 2295, Aug. 2019.
[17] X. Zhang, "Commutative reversible data hiding and encryption," *Security and Communication Networks,* vol. 6, no. 11, pp. 1396-1403, 2013.
[18] X. Zhang, "Separable reversible data hiding in encrypted image," *IEEE Transactions on Information Forensics and Security,* vol. 7, no. 2, pp. 826-832, Apr. 2012.
[19] J. Zhou, W. Sun, L. Dong, X. Liu, O. C. Au, and Y. Y. Tang, "Secure reversible image data hiding over encrypted domain via key modulation," *IEEE Transactions on Circuits and Systems for Video Technology,* vol. 26, no. 3, pp. 441-452, Mar. 2016.
[20] Z. Qian, and X. Zhang, "Reversible data hiding in encrypted images with distributed source encoding," *IEEE Transactions on Circuits and Systems for Video Technology,* vol. 26, no. 4, pp. 636-646, Apr. 2016.
[21] X. Zhang, "Reversible data hiding in encrypted image," *IEEE Signal Processing Letters,* vol. 18, no. 4, pp. 255-258, Apr. 2011.
[22] W. Hong, T.-S. Chen, and H.-Y. Wu, "An improved reversible data hiding in encrypted images using side match," *IEEE Signal Processing Letters,* vol. 19, no. 4, pp. 199-202, Apr. 2012.
[23] X. Wu, and W. Sun, "High-capacity reversible data hiding in encrypted images by prediction error," *Signal Processing,* vol. 104, pp. 387-400, Nov. 2014.
[24] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Transactions on Circuits and Systems for Video Technology,* vol. 16, no. 3, pp. 354-362, Mar. 2006.
[25] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Transactions on Circuits and Systems for Video Technology,* vol. 13, no. 8, pp. 890-896, Aug. 2003.
[26] A. Mohammadi, and M. Nakhkash, "Sorting methods and adaptive thresholding for histogram based reversible data hiding," *arXiv preprint arXiv:1907.05129,* 2019.
[27] V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y. Q. Shi, "Reversible watermarking algorithm using sorting and prediction," *IEEE Transactions on Circuits and Systems for Video Technology,* vol. 19, no. 7, pp. 989-999, Jul. 2009.
[28] M. J. Weinberger, G. Seroussi, and G. Sapiro, "The LOCO-I lossless image compression algorithm: Principles and standardization into JPEG-LS," *IEEE Transactions on Image processing,* vol. 9, no. 8, pp. 1309-1324, Aug. 2000.
[29] M. Fallahpour, and M. H. Sedaaghi, "High capacity lossless data hiding based on histogram modification," *IEICE Electronics Express,* vol. 4, no. 7, pp. 205-210, 2007.
[30] X. Wu, and N. Memon, "Context-based, adaptive, lossless image coding," *IEEE Transactions on Communications,* vol. 45, no. 4, pp. 437 - 444, Apr. 1997.

زیرنویس‌ها

[1] Most significant bit
[2] Cloud computing
[3] Cloud storage
[4] Image owner
[5] Data hider
[6] Receiver
[7] Median edge detector
[8] Gradient-adjusted prediction
[9] Chessboard
[10] 1's complement
[11] Bold
[12] Peak signal-to-noise ratio
[13] Counter mode
[14] Lossless reconstruction