یک روش پایه‌ای برای توسعه‌ی الگوریتم‌های نهان‌نگاری مبتنی بر LSB با تأکید بر مقاومت

محمدعلی شمع‌علیزاده بایی*[1]، زین‌العابدین نوروزی[2]، محمد سبزی‌نژاد[3]، محمدرضا کرمی[4]

[1و2]اعضای هیئت‌علمی دانشگاه امام‌حسین(علیه‌السلام)، [3]دانشگاه خوارزمی تهران، [4]دانشگاه صنعتی نوشیروانی بابل

(تاریخ دریافت: ۹۴/۷/۲۸ ؛ تاریخ پذیرش: ۹۵/۴/۶)

چکیده

نهان‌نگاری، علم و هنر مخفی کردن اطلاعات در یک رسانه، مثل تصویر و صوت است و هدف از آن پنهان کردن هرگونه ارتباط بین فرستنده و گیرنده‌ی یک پیام است. امروزه، اینترنت و شبکه‌های ارتباطی الکترونیکی به‌سرعت در حال پیشرفت است و این در حالی است که مسائل و مشکلات زیادی در مسیر استفاده از آنها وجود دارد. مهم‌ترین این مسائل، مسئله‌ی امنیت پیام ارسالی از طریق این شبکه‌های ارتباطی است؛ بنابراین، یک روش ارتباطی امن، برای انتقال اطلاعات از طریق این شبکه‌ها موردنیاز است. یک روش برای این کار، رمزنگاری است. ولی از آنجایی‌که رمزنگاری پیام اصلی را به یک متن نامرتب و نامفهوم تبدیل می‌کند، باعث تشکیک و سوءظن معارضان و ناظران بر این شبکه‌های ارتباطی می‌گردد. روش‌های پنهان‌نگاری اَمن، با نهان کردن پیام محرمانه‌ی رمزشده در یک رسانه مثل تصویر، می‌توانند بر این مشکل غلبه کنند. در این مقاله، با بررسی بعضی از فن‌های جاسازی پیام در تصویر، به‌خصوص روش‌های معروف به LSB و LSB2، فن جدیدی برای این کار پیشنهاد می‌کنیم که آن را ELSB2 می‌نامیم. این الگوریتم را به‌گونه‌ای طراحی کردیم که در مقابل پردازش‌های پُراتلافی نظیر فیلترینگ و فشرده‌سازی که به‌آسانی اطلاعات جاسازی‌شده در تصویر را تخریب می‌کنند، از مقاومت بیشتری برخوردار است. پس از معرفی روش‌های مذکور، به پیاده‌سازی و مقایسه آنها می‌پردازیم.

واژه‌های کلیدی

جاسازی پیام، امنیت، مقاومت، نهان‌نگاری.

A Basic Approach in Developing LSB-based Steganographic Algorithm Emphasizing on Robustness

Mohammad Ali Shamalizadeh Bayi[1], Zein-al-abedin Nowroozi[2], Mohammad Sabzi Nezhad[3], Mohammadreza Karami[4]

[1,2]Faculty Member of Imam Hossein University, [3]Tehran Khwarizmi University, [4]Babol Nowshirvani University.

(Submitted: 2015/Oct/19; Accepted: 2016/Jun/26)

Abstract

Steganography is the science and art of hiding communication in a media like image, audio, and so on in order to hide any communication between the transmitter and receiver of a message. Nowadays internet and electronic communication networks are rapidly progressing. However, there are many issues and problems in the course of their employment. The most important of these is the security of sent message through these communication channels. So, we need a secure network to send data through these channels. Cryptography is one method for this purpose. But, as Cryptography transforms the main message into a disordered and imperceptible one, it causes doubt and suspicion to the opponents and supervisors of these networks. Secure approaches of watermarking, by hiding encrypted secret message in a media like image, can overcome this problem. In this article by reviewing some of the techniques of embedding message into image, especially those known as LSB and LSB2 ones, we propose a new technique for this work which is known as ELSB2. We have designed this algorithm in such a way that it shows more resistance against lousy processing such as filtering and compression, which easily destroy information embedded into image. After introducing the above mentioned techniques, we implement and compare them.

Keywords

Message embedding, Security, Robustness, Steganography.

۱- مقدمه

نهان‌نگاری[1] یا استگانوگرافی، هنر برقراری ارتباط پنهانی افراد است و هدف از آن پنهان کردن ارتباط بین فرستنده و گیرنده‌ی پیام با قرار دادن آن در یک رسانه مثل صوت، تصویر یا ویدئو است به‌گونه‌ای که کمترین تغییر قابل‌کشف را در آن ایجاد نماید و نتوان موجودیت پیام پنهان‌شده در رسانه را، حتی به‌صورت احتمالی آشکار ساخت[۱]. پنهان‌نگاری خود شاخه‌ای از دانشی به نام ارتباطات پوشیده است. تفاوت اصلی رمزنگاری و پنهان‌نگاری آن است که در رمزنگاری هدف، اختفاء محتویات پیام است و نه وجود پیام، اما در پنهان‌نگاری هدف مخفی کردن هرگونه نشانه‌ای از وجود پیام است. در مواردی که تبادل اطلاعات رمزشده مشکل‌آفرین باشد، باید وجود ارتباط، پنهان گردد. به‌عنوان‌مثال، اگر شخصی به متن رمزنگاری‌شده‌ای دسترسی پیدا کند، به‌هرحال دسترسی به متن اصلی برای وی غیرممکن نیست؛ اما در پنهان‌نگاری شخص سوّم هرگز از وجود پیام مخفی در متن اطلاعی حاصل نمی‌کند[۲].

به‌طورکلی، در سیستم‌های اختفاء اطلاعات، سه عنصر اصلی ظرفیت[2]، امنیت[3] و مقاومت[4] دخیل هستند. در دنیای امروز، جوهر نامرئی و کاغذ که در گذشته برای برقراری ارتباطات پنهانی به کار برده می‌شد، به‌وسیله‌ی رسانه‌های عملی‌تر مثل تصویر، ویدئو و فایل‌های صوتی جایگزین شده‌اند. به دلیل اینکه این رسانه‌های دیجیتال دارای افزونگی اطلاعاتی زیادی هستند، می‌توانند به‌عنوان یک پوشش مناسب برای پنهان کردن پیام استفاده شوند[۲و۳]. تصاویر، مهم‌ترین رسانه مورداستفاده، به‌خصوص در اینترنت هستند و درک تصویری انسان از تغییرات در تصاویر محدود است. الگوریتم‌های پنهان‌نگاری متعددی، برای ساختارهای مختلف تصاویر ارائه‌شده است. هیچ‌یک از این الگوریتم‌ها، تاکنون امنیت را به‌طور کامل تأمین نکرده‌اند. ب طور کلی، روش‌های پنهان‌نگاری در تصویر، از الگوریتم‌های جاسازی و الگوریتم‌های استخراج بیت‌های پیام تشکیل شده‌اند. به تصویر مورداستفاده برای پنهان‌نگاری، پوشانه یا تصویر پوششی[5] و به تصویری که با قرار دادن پیام به‌وسیله‌ی الگوریتم جاسازی در تصویر پوششی به دست می‌آید، تصویر میزبان[6] یا گنجانِه می‌گوییم. الگوریتم‌های پنهان‌نگاری در حالت کلی در فضای مکان یا در فضای تبدیل [۴] که فضای فرکانس نامیده می‌شود، پیاده‌سازی می‌شوند. در هر یک از این فضاها به شیوه‌های گوناگونی می‌توان داده‌ها را پنهان کرد که یکی از ساده‌ترین روش‌ها، استفاده از بیت‌های کم‌ارزش در فضای موردنظر است. در پنهان‌نگاری نیز همانند رمزنگاری، فرض بر آن است که الگوریتم‌های به کار رفته، برای همه آشکار است. معروف‌ترین الگوریتم‌ها در فضای تبدیل، الگوریتم‌های F_3، F_4 و F_5 هستند که همگی مبتنی بر بیت کم‌ارزش می‌باشند[۴].

پنهان‌نگاری در حوزه‌ی مکان، ساده‌تر و پُرکاربردتر از بقیه است. در این حوزه، از ضعف بینایی انسان در تفکیک دقیق رنگ‌ها و تشخیص تغییرات استفاده می‌شود. در واقع، در روش‌های موجود در این حوزه، پیام درون بخشی از فضای بیتی تصویر پنهان‌شده و در نتیجه امکان کشف آن به‌سادگی میسر نخواهد بود. معروف‌ترین الگوریتم‌ها در این حوزه الگوریتم‌ها LSB یا LSB1، LSBM، LSBMR، EAMR، I-EAMR هستند که اساس همگی بر اولین بیت کم‌ارزش است[۵و۶و۷و۸]. الگوریتم‌های پنهان‌نگاری در این حوزه، مستقیماً بر روی مقادیر پیکسل عمل می‌کنند. اگرچه فن‌های موجود در این حوزه، به‌راحتی قابل‌اعمال بر روی اغلب تصاویر هستند، اما در مقابل نسبت به پردازش‌هایی نظیر فیلترینگ و فشرده‌سازی که اَعمال پُراتلافی هستند، حساسیت زیادی دارند و به‌آسانی تخریب می‌شوند و به‌علاوه از ظرفیت جایگذاری کمتری نیز برخوردارند. فن LSB1 همان فن سنتی برای جاسازی بیت های پیام در کم‌ارزش‌ترین بیت[7] پیکسل‌های تصویر پوششی است. فن LSB2 که توسط A.E.Mustafa و Elgamal در سال 2011 طراحی شده است[۹]، با جاسازی بخشی از بیت‌های پیام در دومین بیت از پیکسل‌های تصویر پوششی، اندکی مقاومت آن را تقویت می‌کند. در بخش‌های دوم و سوم این مقاله، الگوریتم‌های LSB1 و LSB2 را موردبررسی قرار داده، سپس در بخش

---

[1] Steganography
[2] Capacity
[3] Security
[4] Robustness
[5] Cover image
[6] Stego image
[7] Least Significant Bit

چهارم، به توسعه‌ی روش LSB2 می‌پردازیم و در بخش پنجم، با پیاده‌سازی آنها، سه روش را مقایسه می‌کنیم.

۲- روش LSB1

روش جاسازی در بیت کم‌ارزش، یکی از متداول‌ترین روش‌های نهان‌نگاری در حوزه‌ی مکانی تصویر هست. این روش بسیار ساده است به‌طوری‌که هر بیت پیام، در یک بیت کم‌ارزش از هر پیکسل تصویر پوششی جاسازی می‌گردد. این عمل باعث تغییر ناچیزی (۰ یا ± 1 واحد) در مقدار دستمالی شدت پیکسل موردنظر می‌شود. برای درک بهتر موضوع به جدول۱ نگاه کنید. در این جدول مشاهده می‌کنید که مقدار داده‌های مکانی ما برابر است با ۱۳۵،۹۸،۲۲۱ که در رشته‌بیتی آنها، داده‌ها در مکان کم‌ارزش جاسازی می‌شوند. پس از جاسازی پیام در آن به این روش، از مورد اول یک واحد کم، به مورد دوم یک واحد اضافه و مورد سوم بدون تغییر باقی می‌ماند. در نتیجه، شدت‌های ۱۳۴، ۹۹ و ۲۲۱ به دست می‌آید.

جدول۱. جاسازی پیام در پیکسل‌های تصویر پوششی به روش LSB1.

شدت پیکسل‌های تصویر پوششی به اسکی	۱۳۵	۹۸	۲۲۱
شدت پیکسل‌های تصویر پوششی به باینری	۱۰۰۰۰۱۱۱	۰۱۱۰۰۰۱۱	۱۱۰۱۱۱۰۱
بیت‌های پیام	۰	۱	۱
شدت پیکسل‌های تصویر پوششی به باینری پس از جاسازی بیت‌های پیام به روش LSB1	۱۰۰۰۰۱۱۰	۰۱۱۰۰۰۱۱	۱۱۰۱۱۱۰۱
شدت پیکسل‌های تصویر پوششی به اسکی پس از جاسازی بیت‌های پیام به روش LSB1	۱۳۴	۹۹	۲۲۱

واضح است که اگر داده‌ها در مکان‌هایی باارزش بالاتری از پیکسل‌های تصویر پوششی جاسازی شوند، این عمل باعث تأثیرگذاری بیشتری بر روی داده‌های میزبان و بالا رفتن نرخ نویز در آن می‌گردد. از طرفی روش جاسازی پیام در بیت کم‌ارزش در مقابل عملیاتی نظیر فیلترینگ و فشرده‌سازی بسیار ضعیف عمل می‌کند و هیچ‌گونه مقاومتی در برابر آنها ندارد؛ به عبارت دیگر، پیام جاسازی‌شده با کوچک‌ترین حمله‌ای از این نوع از دست می‌رود یا آسیب می‌بیند.

۳- روش LSB2

در این روش، یک تصویر $m\times n$ به‌عنوان تصویر پوششی استفاده می‌شود، به‌طوری‌که بتوانیم یک پیام حداکثر با همین تعداد بیت (h) را در آن پنهان کنیم. این پیام با استفاده از روش LSB2 به‌منظور افزایش مقاومت سیستم و محافظت در برابر نفوذهای بیرونی مثل فیلترینگ، فشردگی یا هر نوع نویز دیگری در تصویر پوششی پنهان می‌شود. این فرایند جاسازی به‌آسانی با اجرای الگوریتم زیر که آن را الگوریتم LSB2 می‌نامیم، صورت می‌گیرد. در این فرایند، بعضی از بیت‌های پیام در دوّمین بیت از پیکسل‌های تصویر پوششی متناظر، جاسازی می‌شود.

۳-۱- الگوریتم روش LSB2

به‌منظور کم کردن تفاوت بین مقادیر شدت پیکسل‌ها در تصویر پوششی و تصویر میزبان، گام‌های زیر را تعریف می‌کنیم[۹]:

گام۱: استخراج بیت‌های پیام:

$$Bit = \{M_0, M_1, \dots و M_h\}$$

گام۲: استخراج پیکسل‌های تصویر پوششی:

$$Pixel = \{pixel_0, pixel_1, \dots, pixel_{m\times n}\}$$

گام۳: استخراج اولین بیت‌های کم‌ارزش تصویر پوششی:

$$LSB1 = \{A_0, A_1, \dots, A_{m\times n}\}$$

گام۴: استخراج دومین بیت کم‌ارزش از پیکسل‌های تصویر پوششی:

$$LSB2 = \{B_0, B_1, \dots, B_{m\times n}\}$$

گام۵: اجرای حلقه زیر:

for i = 0 to Message length(h) do
{ if $M_i == B_i$ Then
do nothing
Else
{
If($M_i == 1$ and $B_i == 0$) Then
{ $B_i = M_i$; $A_i = 0$;
$pixel_i = pixel_i - 1$;}
else if ($M_i == 0$ and $B_i == 1$) Then
{ $B_i = M_i$; $A_i = 1$;
$pixel_i = pixel_i + 1$; }
}

۳-۲- پیاده‌سازی الگوریتم LSB2

برای بکارگیری الگوریتم، فرض کنید بخواهیم کاراکتر A را در یک تصویر پنهان کنیم. گام‌های عملیات را به‌صورت زیر تعریف می‌کنیم:

گام۱: تبدیل داده‌های پیام از ده‌دهی به دودویی:

[پیام] —دهدهی به دو دویی→ [1000001]

گام ۲: خواندن فایل پوششی و تبدیل آن به آسکی

گام۳: تبدیل فایل پوششی به دودویی

گام ۴: استخراج بیت‌های پیام

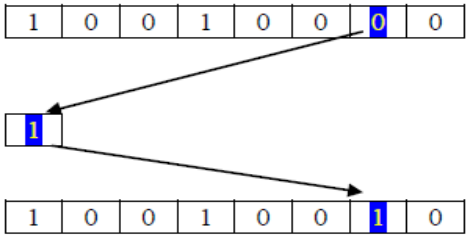
[10000001] —تبدیل به 8 بیت→ [1 0 0 0 0 0 0 1].

گام ۵: نخستین بایت از هشت بایت انتخابی از فایل پوششی را در نظر بگیرید:

1	0	0	1	0	0	0	0

گام۶: ELSB2 را با یک بیت از بیت‌های پیام به‌صورت زیر جایگزین می‌کنیم:

اولین بیت پیام یعنی ۱ است که به‌صورت زیر در ELSB2 جاسازی می‌شود.



مطابق روش پیشنهادی اگر بیت داده‌ای که باید پنهان شود برابر ۱ باشد و LSB2=0، آنگاه:

۱. LSB1 تصویر را به صفر تغییر می‌دهیم که بعد از جایگزینی آن داریم:

1	0	0	1	0	0	1	0

۲. حال ۱ را از آن کم می‌کنیم، لذا داریم:

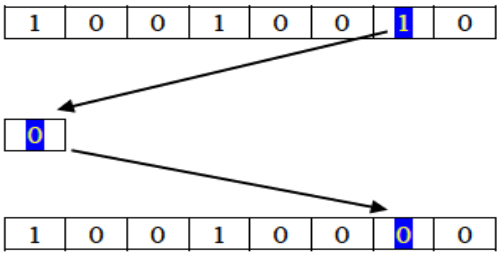
1	0	0	1	0	0	0	0

بنابراین، هیچ تغییری در اولین بایت تصویر پوششی و میزبان مشاهده نشد.

حال، بایت دوّم تصویر پوششی را در نظر می‌گیریم:

1	0	0	1	0	0	1	0

ملاحظه می‌شود که بیت دوّم پیام صفر است که با جایگزینی به روش LSB2 داریم:



که مطابق روش پیشنهادی اگر بیت داده پنهان‌شونده برابر صفر باشد و LSB2=1 آنگاه:

۱. بیت اول تصویر پوششی، یعنی LSB1، به ۱ تغییر می‌کند.

1	0	0	1	0	0	1	1

۲. حال مقدار آن را ۱ واحد افزایش می‌دهیم:

1	0	0	1	0	0	1	0

که باز هم هیچ تغییری در تصویر پوششی نداریم و با تکرار این فرایند، همه‌ی بیت‌های پیام پنهان خواهند شد.

۴. روش پیشنهادی

می‌دانیم جاسازی پیام به روش LSB1 ساده‌ترین روش است که در مقابل اعمالی چون فیلترینگ، فشرده‌سازی و اَعمال مشابه، مقاومتی ندارد و به‌آسانی آسیب‌پذیر است. روش LSB2 با جاسازی بعضی از بیت‌های پیام در دوّمین بیت کم‌ارزش از پیکسل‌های تصویر پوششی متناظر، اندکی به مقاومت بیت‌های مخفی‌شده در مقابل حملات یادشده می‌افزاید. در اینجا، به طراحی الگوریتم ELSB2 با انگیزه‌ی افزایش مقاومت بیت‌های پیام جاسازی‌شده می‌پردازیم. لذا، با توسعه‌ی الگوریتم LSB2 این الگوریتم را طوری طراحی می‌کنیم که همه‌ی بیت‌های پیام در دوّمین بیت پیکسل‌های تصویر پوششی جاسازی شوند. البته، با در نظر گرفتن این موضوع که تغییرات در هر پیکسل به‌اندازه‌ی تغییرات در روش‌های یادشده یعنی ۰ یا ± 1 واحد بماند (با مقایسه‌ی جداول (۱) و (۲) این موضوع ملاحظه می‌شود) که این موضوع متضمن تغییر کیفیت تصویر میزبان به‌اندازه‌ی الگوریتم‌های LSB1 و LSB2 است.

۴-۱- الگوریتم ELSB2

در این روش یک تصویر سیاه‌وسفید $N = m \times n$ به‌عنوان تصویر پوششی استفاده می‌شود، به‌طوری‌که ما می‌توانیم با استفاده از الگوریتم زیر، یک پیام h بیتی که حداکثر آن N است را در آن جاسازی یا پنهان کنیم[۱۰].

گام۱. استخراج بیت‌های پیام:

$Bit = \{M_0, M_1, \dots و M_N\}$

گام۲. با فرض اینکه پیکسل‌های تصویر پوششی LSB1 و LSB2 عبارت باشند از:

$Pixel = \{Pixel_0, Pixel_1, \dots و Pixel_N\}.$

$Pixel_i$

H_i	G_i	F_i	E_i	D_i	C_i	B_i	A_i

$LSB1 = \{A_0, A_1, \dots و A_N\}.$

$LSB2 = \{B_0, B_1, \dots, B_N\}.$

گام۳. اجرای حلقه زیر:

```
for i = 0 to Message length (h) do
{
        if (Bi == Mi) Then
            do nothing
Else If (Mi == 0 and Bi == 1)
        {
    If ( (Ai = 0)
{ Bi = 0; Ai = 1; }
    Else If (Ai = 1 and Ci = 0)
            {Ci = 1;
            Bi = Ai = 0 ; }
    Else If (Ai = 1 and Di = 0)
            {Di = 1;
        Ci = Bi = Ai = 0 ; }
    Else If (Ai = 1 and Ei = 0)
{Ei = 1;
        Di = Ci = Bi = Ai = 0 ; }
    Else If (Ai = 1 and Fi = 0)
{Fi = 1; Ei = Di = Ci = Bi = Ai = 0 ; }
 Else If (Ai = 1 and Gi = 0)
{Gi = 1;
    Fi = Ei = Di = Ci = Bi = Ai = 0 ; }
    Else If (Ai = 1 and Hi = 0)
            {Hi = 1;
  Gi = Fi = Ei = Di = Ci = Bi = Ai = 0 ; }
            }
    Else If (Mi == 1 and Bi == 0)
        {
    If ( (Ai = 1)
    { Bi = 1; Ai = 0; }
    If (Ai = 0and Ci = 1)
        {Ci = 0;    Bi = Ai = 1 ; }
      Else If (Ai = 0 and Di = 1)
        {Di = 0; Ci = Bi = Ai = 1 ; }
      Else If (Ai = 0 and Ei = 1)
{Ci = 0;
        Di = Ci = Bi = Ai = 1 ; }
      Else If (Ai = 0 and Fi = 1)
{Fi = 0;
        Ei = Di = Ci = Bi = Ai = 1 ; }
      Else If (Ai = 0 and Gi = 1)
{Gi = 0;
    Fi = Ei = Di = Ci = Bi = Ai = 1 ; }
    Else If (Ai = 0 and Hi = 1)
{Hi = 0;
  Gi = Fi = Ei = Di = Ci = Bi = Ai = 1 ; }
            }
    }
```

به‌عنوان‌مثال، جدول ۲ را در نظر بگیرید که در سمت چپ آن، بیت‌های ۱۰ پیکسل از تصویر پوششی و در تک ستون سمت راست آن، بیت‌های پیام برای جاسازی در آن نشان داده شده است. همچنین، در جدول۳ مقادیر متناظر تصویر میزبان را ملاحظه می‌کنید. با مقایسه‌ی این دو جدول، همان‌طوری‌که قبلاً بیان شد، ملاحظه می‌شود، با وجود اینکه همه‌ی بیت‌های پیام در دوّمین بیت پیکسل‌های تصویر پوششی یعنی ستون $\mathbf{B_i}$ جاسازی شدند ولی تغییرات در ستون decimal برابر **0** یا $\pm\mathbf{1}$ است. این یعنی با وجود اینکه کلیه‌ی بیت‌های پیام در دوّمین بیت پیکسل‌های تصویر پوششی جاسازی شده است، کاهش چندانی در کیفیت تصویر پوششی نداشتیم این مطلب عملاً روی سه تصویر پیاده‌سازی‌شده و نتایج در جدول۴ نشان داده شده است که تائیدکننده‌ی موضوع است.

جدول ۲. پیکسل‌های تصویر پوششی و بیت‌های پیام قبل از جاسازی بیت‌های پیام.

	Cover image $pixel_i$									
i	H_i	G_i	F_i	E_i	D_i	C_i	B_i	A_i	decimal	Mi
۱	۱	۰	۰	۱	۱	۰	۱	۰	۱۵۴	۰
۲	۱	۱	۱	۰	۱	۱	۰	۱	۲۲۷	۱
۳	۱	۰	۰	۰	۱	۱	۱	۱	۱۴۳	۱
۴	۰	۱	۱	۱	۰	۱	۱	۰	۱۱۸	۱
۵	۱	۱	۰	۱	۰	۰	۰	۱	۲۰۹	۰
۶	۱	۰	۰	۰	۱	۱	۱	۱	۱۴۳	۰
۷	۱	۱	۱	۰	۰	۱	۱	۱	۲۲۱	۱
۸	۰	۰	۰	۱	۱	۱	۰	۰	۲۸	۰
۹	۱	۱	۰	۰	۱	۱	۰	۱	۲۰۶	۱
۱۰	۱	۰	۱	۱	۱	۱	۱	۱	۱۹۱	۱

جدول۳. پیکسل‌های تصویر پوششی بعد از جاسازی بیت‌های پیام.

$Stego\ image\ pixel_i$								
H_i	G_i	F_i	E_i	D_i	C_i	B_i	A_i	decimal
۱	۰	۰	۱	۱	۰	۰	۱	۱۵۳
۱	۱	۱	۰	۱	۱	۱	۰	۲۳۸
۱	۰	۰	۰	۱	۱	۱	۱	۱۴۳
۰	۱	۱	۱	۰	۱	۱	۰	۱۱۸
۱	۱	۰	۱	۰	۰	۰	۱	۲۰۹
۱	۰	۰	۱	۰	۰	۰	۰	۱۴۴
۱	۱	۱	۰	۱	۰	۰	۰	۲۳۲
۰	۰	۰	۱	۱	۱	۰	۰	۲۸
۱	۱	۰	۰	۱	۱	۱	۰	۲۰۶
۱	۰	۱	۱	۱	۱	۱	۱	۱۹۱

۴-۲- شبیه‌سازی

برای پیاده‌سازی الگوریتم‌های **LSB1**، **LSB2** و **ELSB2** و مقایسه‌ی نتایج آن‌ها، عکس‌های ۱،۲و۳ را در نظر می‌گیریم. جاسازی به روش‌های فوق را در این سه تصویر اعمال می‌کنیم سپس با در دست داشتن پوشانه و نهانه، این الگوریتم‌ها را با استفاده از نرم‌افزار MATLAB مورد ارزیابی کیفی مرسوم در نهان‌نگاری و پردازش تصویر قرار می‌دهیم. نتایج را در جدول ۴. ثبت می‌کنیم

شکل ۱. تصویر رضا

شکل ۲. تصویر محمد

شکل ۳. تصویر نخل.

با مقایسه‌ی سه ستون جدول۴، به‌خصوص برای روش ELSB2 که هر یک از بیت‌های پیام در دوّمین بیت پیکسل‌های آن جاسازی شده است، ملاحظه می‌کنید که پارامترهای ارزیابی محاسبه‌شده برای سه تصویر، بسیار به مقادیر به‌دست‌آمده از روش‌های دیگر، نزدیک است. این یعنی الگوریتم **ELSB2** با وجود اینکه بیت‌های پیام را در دومین بیت کم‌ارزش پیکسل‌های تصاویر پوشانه جاسازی کرد (افزایش مقاومت)، میزان تخریب در این تصاویر از تصاویر نهانه به‌دست‌آمده از دو روش دیگر یعنی **LSB1** و **LSB2** بدتر نشده است.

جدول ۴. نتایج محاسبه چند پارامتر ارزیابی تصاویر پوششی.

		LSB1	LSB2	ELSB3
رضا	SNR	۶۶.۷۰۵۸	۶۷.۰۸۶۷	۷۰.۳۹۶۷
	MSE	۶.۶۶۳۰e.۰۴	۶.۱۰۳۵e.۰۴	۲.۸۳۸۲e.۰۴
	PSNR	۷۹.۸۹۴۱	۸۰.۲۷۵۰	۸۳.۵۸۴۹
محمد	SNR	۶۹.۵۱۷۵	۷۲.۰۷۷۰	۶۸.۷۳۲۶
	MSE	۰.۰۰۲۰	۰.۰۰۱۱	۰.۰۰۲۲
	PSNR	۷۵.۲۲۲۵	۷۷.۷۸۳۰	۷۴.۴۴۸۷
نخل	SNR	۶۹.۳۱۷۷	۷۲.۷۷۷۷	۶۷.۳۰۳۲
	MSE	۰.۰۰۱۹	۸.۳۹۲۳e.۰۴	۰.۰۰۳۰

۵- نتیجه‌گیری و پیشنهاد

فن جاسازی پیام مرسوم در حوزه‌ی مکان، یعنی LSB1 که بیت‌های پیام را در کم‌ارزش‌ترین بیت پیکسل‌های تصویر پوششی، یعنی اولین بیت، جاسازی می‌کند، در مقابل عملیاتی چون فیلترینگ یا فشرده‌سازی و عملیات مشابه بسیار آسیب‌پذیر است و این عملیات باعث بیشترین تخریب در تصویر پوششی می‌گردد. در این مقاله، با توسعه‌ی الگوریتم LSB2 یک روش جدید برای پنهان‌سازی پیام، در یک تصویر ارائه شده است. الگوریتم LSB2 به دلیل جاسازی بعضی از بیت‌های پیام در بیت دوّمین بیت کم‌ارزش تصویر پوششی، از مقاومت بیشتری نسبت به LSB1 برخوردار است. روش ELSB2 که در این مقاله پیشنهاد شد به دلیل اینکه همه‌ی بیت‌های پیام را در بیت دوّم پیکسل‌های تصویر پوششی جاسازی می‌کند، احتمال تخریب در تصویر پوششی، پس از عملیات یادشده را بسیار کم می‌کند. به عبارت دیگر، این فن مقاوم‌تر از بقیه است. نتایج به‌دست‌آمده در جدول ۴ هم با برآورد پارامترهای متفاوت ارزیابی شفافیّت تصویر، نشان می‌دهد که پیاده‌سازی این الگوریتم تأثیری روی کیفیت تصویر پوششی در مقایسه با روش‌های پیشین ندارد. درحالی‌که مقاومت را در مقابل برخی از حملات عمدی یا غیرعمدی افزایش داده است. در مقالات بعدی می‌توان روی توسعه امنیتی **ELSB2** کار کرد.

منابع:

[1]. I. Cox, M. Miller, J. Bloom, J. Fridrich, T.Kalker, "Digital Watermarking and Steganography", Second edition. Morgan Kaufmann, Burlington, 2007.

[2]. R. Bohem, "Advanced Statistical Steganalysis ", Springer-Verlag Berlin Heidelberg 2010.

[3]. D.C. Wu., Tsai, and W.H., "A steganographic method for images by pixel value differencing", Pattern Recognition Letters24, pp. 1613–1626, 2003.

[4]. Westfield, A., and Pfitzman, A., “Attacks on steganographic systems,” Information Hiding, Springer-Verlage Berlin Heidelberg, LNCS 1768, pp. 61-76, 1999.

[5]. L. Bin et al, "A Survey on Image Steganography and Steganalysis", Ubiquitous International Journal of Information Hiding and Multimedia Signal ProcessingVol. 2, 2073-4212, 2011.

[6]. J. Mielikainen, Lsb matching revisited, IEEE Signal Processing Letters, vol. 13, no. 5, 285-287, 2006,

[7]. Luo, W., Huang, F., Huang, J." Edge adaptive image steganography based on LSB matching revisited" IEEE Trans. Inf. Forensics Secure, Vol.5, No.2, 201–214, 2010.

[8].F. Huang, Y.Zhong , J.Huang, "Improved Algorithm of Edge Adaptive Image Steganography Based on LSB Matching Revisited Algorithm" , Springer-Verlag Berlin Heidelberg. 19–31, 2014.

[9] Mustafa, A. E., Elgamal, A. M. F., Almi, M. E. E., and Ahmed, B. D., “A proposed algorithm for steganography in digital image based on least significant bit,” Research Journal Specific Education Faculty of Specific Education, Mansoura University, No. 21, 2011.

[10]. M.A shamalizade, Z Norozi, M.R Karami, "A New Algorithm for Embedding Message in Image Steganography International Journal of Engineering Research and Technology Vol. 3 (02), ISSN 2278 – 0181, February-2014.