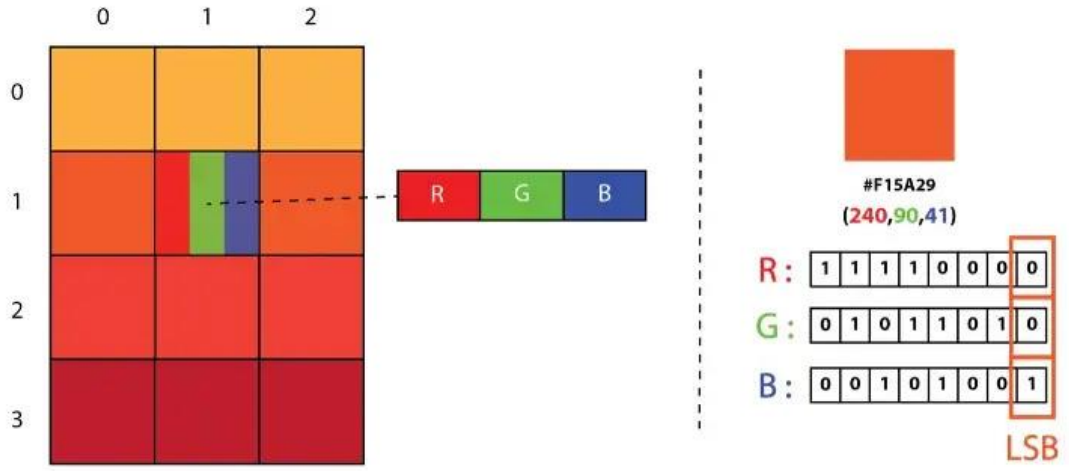
مقاله پارت دوم پروژه الگوریتم

امیرحسین تسلیمی، رضا نعمت اللهی

استاد : جناب آقای دکتر زیارتی

مقدمه :

Least Significant Bit (LSB) یک تکنیک در Image Steganography است، پیامی که قرار است در عکس مخفی شود، به صورت باینری هر بیت آن با کم ارزش ترین بیت مولفه های رنگی پیکسل عکس جایگزین میشود.



پنهان‌نگاری (Steganography) :هنر و علم برقراری ارتباط پنهانی است و هدف آن پنهان کردن ارتباط به وسیله قرار دادن پیام در یک رسانه پوششی است به گونه‌ای که کمترین تغییر قابل کشف را در آن ایجاد نماید و نتوان موجودیت پیام پنهان در رسانه را حتی به صورت احتمالی آشکار ساخت. پنهان‌نگاری شاخه‌ای از دانشی به نام پنهان‌سازی اطلاعات (Information Hiding) است .

تاریخچه :

استگانوگرافی از واژه یونانی "Stego" به معنای "پوشیده" و "Graphia" به معنای "نوشتن" گرفته شده است. استگانوگرافی یک تکنیک باستانی برای برقراری ارتباط پنهان است. اولین شکل استگانوگرافی توسط چینی ها گزارش شده است. پیام مخفی را با ابریشم یا کاغذ بسیار ظریف می نوشتند و سپس به شکل توپ در می آوردند و با موم می پوشاندند. در نتیجه مخفی کردن آن راحت تر بود.هرودوت در یکی از آثار مهم تاریخ خود به نام «تاریخ در طول 400 سال قبل از میلاد» به سنت مخفی نویسی اشاره کرده است. او در نوشته های خود به درگیری های یونان و ایران اشاره کرده است. پادشاهی به نام هیستیائوس آریستاگوراس میلتوس را به شورش علیه پادشاه ایران تشویق کرده است. او عادت داشت سر مورد اعتمادترین خدمتکاران خود را کامل بتراشد و پوست سر را با پیامی مخفیانه خالکوبی کند و منتظر رشد موها بماند. خادم میتوانست بدون اینکه توجه کسی جلب شود بین مرزها رفت وآمد کند و پیام را با خود حمل کند. در پایان وقتی پیش شخص مورد نظر میرسید میتوانستند سر او را دوباره بتراشند و پیام منتقل میشد. به طور مشابه در طول جنگ جهانی دوم، آلمانی ها استفاده از ریز نقطه ها را ابداع کردند. تصویر حاوی جزئیات عالی به اندازه ریز نقطه ها کوچک میشد. استفاده آلمانی ها از استگانوگرافی برای به اشتراک گذاری رمزها بین افراد به عنوان تکامل اخیر استگانوگرافی در نظر گرفته می شود. نمونه دیگری از استگانوگرافی در طول جنگ ویتنام است که نیروهای مسلح اسیر شده ایالات متحده برای انتقال برخی از اسرار نظامی در طول جلسات عکس، حرکات دست های خودشان را نشان میدادند تا بتوانند پیام را منتقل کنند. در طول جنگ جهانی دوم، ارتش مقاومت فرانسه در پشت فرستندگان با جوهر نامرئی پیام مخفی مینوشتند. همچنین در طول جنگ سرد، سازمان اطلاعات مرکزی ایالات متحده از دستگاه های مختلفی برای مخفی کردن پیام ها استفاده می کرد. به عنوان مثال، آنها یک لوله تنباکو ساختند که فضای کوچکی برای پنهان کردن میکروفیلم داشت. اما هنوز هم میشد از آن استفاده کرد و مصرف کرد. رشته استگانوگرافی نامحدود است و از هر نوع رسانه پوششی می توان برای انتقال پیام های مخفی استفاده کرد. رسانه های پوششی می توانند متن، تصاویر (خاکستری، باینری، رنگی)، صدا، ویدئو و غیره باشند.

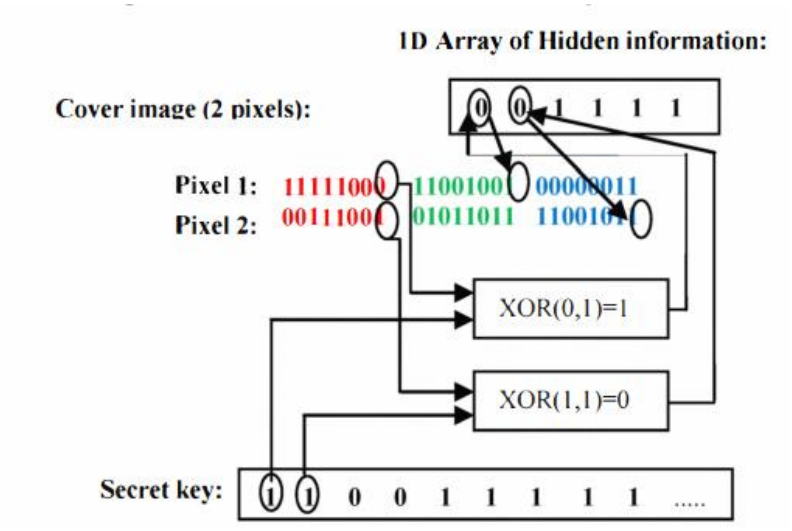
عملکرد :

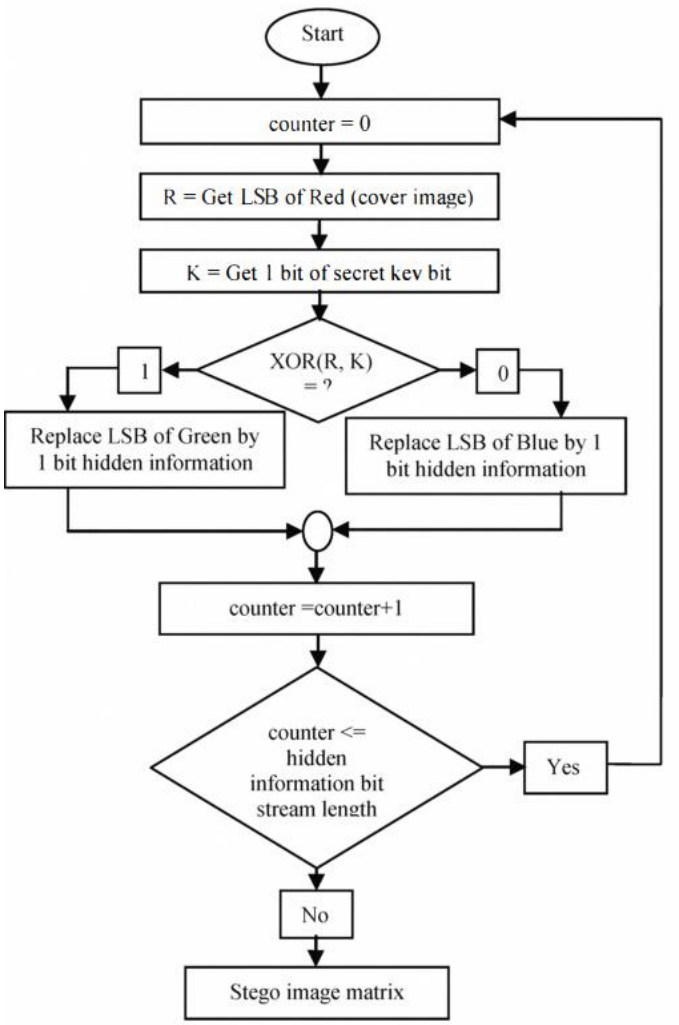
در این بخش به بررسی الگوریتم انجام شده میپردازیم.

در روش معمولی استفاده از LSB ،بیت های پیام با کم ارزش ترین بیت های مولفه های رنگی پیکسل ها جایگزین میشود. در این حالت با فرض اینکه هر حرف 8 بیت باینری باشد، برای هر حرف به 3 پیکسل نیاز داریم. هر پیکسل 3 مولفه ی رنگی قرمز ،آبی و سبز دارد که کم ارزش ترین بیت هر کدام را با بیت پیام عوض میکنیم. تغییر عکس بسیار کم است و قابل تشخیص برای چشم انسان نیست.در نتیجه پیام مخفی میماند.

مشکل این روش در آن است که استخراج بیت های پیام راحت است و نیاز به کلید ندارد. برای تقویت این روش میتوانیم از یک کلید استفاده کنیم. تا شخص بدون داشتن کلید نتواند پیام را استخراج کند.

کلیدی به طول خود پیام ایجاد میکنیم. هر کدام از بیت های کلید را با بیت کم ارزش مولفه قرمز پیکسل ها xor میکنیم. در صورتی که حاصل 0 بود، بیت پیام را در بیت کم ارزش مولفه آبی مینویسیم و اگر حاصل 1 بود، در بیت کم ارزش مولفه سبز مینویسیم.





- مزیت این رویکرد:

بدست آوردن پیام بدون کلید بسیار سخت است. به طور مثال اگر پیام 5 حرف داشته باشد، یعنی کلیدی به اندازه 40 بیت باینری داریم، که در بدترین حالت باید 2^40 رشته از صفر و یک ها تست شود، تا به کلید صحیح رسید !.

- عیب این رویکرد:

فضای ذخیره سازی عکس کاهش می یابد، زیرا در این حالت هر حرف 8 پیکسل اشغال میکند به جای 3 پیکسل، در واقع حداکثر پیام ممکن 33 درصد حالت معمولی میشود تقریبا.

در نهایت برای پیامی به طول n حرف به عکسی با 8n پیکسل نیاز داریم.

```
    for i in range(852):
        for j in range(1280):
            if ((i+1)*(j))%8 == 0 and len(str(massage))-1>((i+1)*(j)):  #sentinel val
                temp = bin(img[i][j][2]).replace("0b", "")
                temp = temp[:-1] + '1'
                img[i][j][2] = str(int(temp, 2))

            elif ((i+1)*(j))%8 == 0 and (len(str(massage))+2>((i+1)*(j))):  #sentinel val
                temp = bin(img[i][j][2]).replace("0b", "")
                temp = temp[:-1] + '0'
                img[i][j][2] = str(int(temp, 2))
                break

            if len(str(massage))>((i+1)*(j)) and ((int(key[(i+1)*(j)]) ^ int(bin(img[i][j]
[2]).replace("0b", "")[-1])) == 0): #blue
                temp = bin(img[i][j][0]).replace("0b", "")
                temp = temp[:-1] + massage[(i+1)*(j)]
                img[i][j][0] = str(int(temp, 2))

            elif (len(str(massage))>((i+1)*(j))) and ((int(key[(i+1)*(j)]) ^ int(bin(img[i]
[j][2]).replace("0b", "")[-1])) == 1) : #green
                temp = bin(img[i][j][1]).replace("0b", "")
                temp = temp[:-1] + massage[(i+1)*(j)]
                img[i][j][1] = str(int(temp, 2))
            else :
                break
        else:
            continue
        break
}
```

code for encrypt massage

برای استخراج پیام از عکس، باید بدانیم که پیام تا کجا است. برای این منظور هر سری که یک حرف را میخوانیم(8 بیت باینری)، بیت کم ارزش مولفه قرمز را در پیکسل هشتم یک قرار میدهیم. به این معنا که پیام تمام نشده. وقتی به حرف آخر رسیدیم این بیت را صفر میگذاریم به این معنا که پیام تمام شده است. حال برای استخراج بیت های کم ارزش مولفه قرمز پیکسل های مضرب 8 را چک میکنیم اگر صفر بود، پیام به پایان رسیده است.

کاربردها:

اکثر برنامه های جدیدتر از استگانوگرافی مانند یک واترمارک برای محافظت از حق چاپ بر روی اطلاعات استفاده می کنند. مجموعه‌های عکس، که بر روی سی‌دی فروخته می‌شوند، اغلب پیام‌های مخفی در عکس‌ها دارند که امکان تشخیص استفاده غیرمجاز را فراهم می‌کند. تکنیک مشابهی که برای DVD اعمال می‌شود حتی مؤثرتر است، زیرا شرکت ها، ضبط‌کننده‌هایی را برای شناسایی و ممنوع کردن کپی کردن DVD های محافظت شده می‌سازند.

در دنیای تجارت می توان از استگانوگرافی برای پنهان کردن یک فرمول شیمیایی مخفی یا برنامه هایی برای یک اختراع جدید استفاده کرد.

فرض کنیم دیتابیس بزرگی از داده ها داریم. برای پیدا کردن یک فایل خاص(عکس مثلا) میتوانیم به در آن فایل اطلاعاتی را از طریق استگانوگرافی قرار دهیم(meta data). مثلا در عکس ها عنوان و تاریخ را جایگذاری کنیم. به طور کلی از استگانوگرافی برای ترکیب کردن دیتاهای مختلف استفاده میکنیم.

در پرینترها ،از استگانوگرافی استفاده میشود تا یک واترمارک دیجیتالی روی کاغذ ایجاد شود. که میتواند نقاطی مخفی رو کاغذ باشد. این کار امکان شناسایی دستگاهی را که برای چاپ یک سند استفاده می‌شود را به استفاده کننده از آن میدهد.

منابع:

https://www.ukessays.com/essays/english-language/background-of-steganography.php

https://en.wikipedia.org/wiki/Steganography

http://datahide.org/BPCSe/applications-e.html

https://www.researchgate.net/publication/261421805_A_new_approach_for_LSB_based_image_steganography_using_secret_key

William (Chuck) Easttom - Penetration Testing Fundamentals_ A Hands-On Guide to Reliable Security Audits-Pearson It Certification (2018)