گزارش پایانی

سید علی یعقوب نژاد
محمد علی صدرایی
سید عارف جهانمیر
علی امیری نژاد

چکیده

تلگرام برنامه پیام‌رسان محبوبی که در رده‌ی پنج برنامه‌ی پیام‌رسان برتر دنیا قرار دارد و تمرکزش روی سرعت انتقال پیام و امنیت است. استفاده از این برنامه رایگان است. کاربران تلگرام امکان ارسال پیام، صدا، ویدیو و فایل‌های مختلف و رمزنگاری شده را تا حجم حدود دو گیگابایت دارند.تلگرام ۵۰ میلیون کاربر در ایران دارد، که ۵۶ درصد کل جمعیت این کشور را تشکیل می‌دهد. هدف ما رمزنگاری عکس هایی است که در تلگرام فرستاده میشوند. چالش اصلی رمزنگاری تلگرام این است که در هنگام ارسال عکس، تلگرام برای کاهش حجم عکس از تبدیل های مخصوص خود استفاده میکند که این باعث میشود فایل باینری عکس ورودی متفاوت از فایل باینری عکس خروجی در تلگرام باشد. همین امر سبب میشود که رمزنگاری های ساده به راحتی امکان پذیر نباشد. در ادامه راه حل پیشنهادی خود را ارائه میدهیم..

۱ مقدمه

با رشد تکنولوژی اطلاعات و شبکه ها و نیز توسعه انواع بسترهای ارتباطی، امروزه چالش اساسی در حوزه ارتباطات دیگر برقراری ارتباط محسوب نمیشود بلکه آنچه که باید در مرکز توجه قرار بگیرد امنیت این ارتباطات است. محیط اینترنت و نیز سایر زیرساختهای ارتباطی که در عصر کنونی به طور گستردهای جهت تبادل اطلاعات استفاده میشوند نیز از امنیت کافی برخوردار نیستند. پنهان نگاری اطلاعات یکی از سطوح امنیتی است که معمولا پس از انجام رمز نگاری به منظور پنهان ساختن وجود ارتباط استفاده میشود. پنهان نگاری کامپیوتری به معنای پنهان کردن اطلاعات در یک رسانه دیجیتال است به نحوی که هیچ ظنی مبنی بر وجود داده مخفی در رسانه دیجیتال برانگیخته نشود.

رمزگذاری یک ابزار موثر و محبوب در حفاظت از حریم خصوصی است. به منظور اشتراك ایمن تصویر رمز با دیگران، یک مالک محتوا ممکن است تصویر را قبل از انتقال رمزگذاری کند. در برخی از حالات، یک کارمند رده پایین تر و یا یک مدیر کانال امیدوار است که بتواند برخی از پیامهای اضافی، مانند اطلاعات مبدا، نماد تصویر یا اعتبار داده ها، را که در تصویر رمز شده است رمزگشایی کند، هر چند او از محتوای تصویر اصلی خبر ندارد. به عنوان مثال، تصاویر پزشکی ای که براي حفاظت از حریم خصوصی بیمار رمزگذاري شده است. یک مرکز بهداشتی دیگر ممکن است بخواهد اطلاعات دیگری را در تصاویر رمزگذاری شده مربوطه پنهان کند. ممکن است که محتوای اصلی را بتوان بدون هیچ گونه خطا، پس از رمزگشایی به دست آورد و بازیابی پیام هاي اضافی در سمت گیرنده انجام شود.

پنهان نگاری دیجیتال به عنوان روشی برای حفظ محرمانگی اطلاعات شناخته می شود.هدف از انجام این پروژه، ارائه روشی براي افزایش امنیت در ارسال تصویر بر پایه ی پنهان نگاری می باشد که در آن یک متن میتواند در تصویری پوششی مخفی شود. این رویکرد باعث میشود که در صورت استراق سمع از کانال امکان دسترسی به تصویر محرمانه به دلیل مخفی شدن آن در تصویر پوششی به سختی ممکن باشد.

۲ کارهای مرتبط / پیش‌زمینه

امروزه روش های متفاوتی در زمینه پنهان سازی معرفی شده اند که ما به مهم ترین آن ها اشاره میکنیم:

۱- روش LSB

یکی از روشهای شناخته شده در پنهان نگاری تصاویر، روش جایگزینی LSB یا جایگزینی در بیت دارای ارزش کمتر است. تصاویر دیجیتالی عموما از یک آرایه دو بعدی از پیکسلها ساخته شده که هر عضو این آرایه حاوی هشت بیت (در تصاویر سیاه و سفید) و ۲۴ بیت در (تصاویرنگی) هستند.روش کار LSB مخفی کردن اطلاعات در درست ترین بیت در هر پیکسل است. میزان تاثیر روش LSB در کیفیت یک تصویر، به تعداد بیتهایی که برای پنهان نگاری استفاده شده اند بستگی دارد. در این مقاله [۱] روشی را ارائه دادند که با مخفی کردن اطلاعات در لبه ها که بینایی انسان نمی تواند تغییرات کوچک را تشخیص دهد و با تغییر ترتیب صفحات RGB هنگام قراردادن پیام مخفی خطرات امنیتی را نسبت به دیگر روش ها کاهش دادند. در روشی دیگر [۲] با استفاده از تشخیص لبه هیبریدی که ترکیب دو روش canny و sobel می باشد بر روی سه پیکسل از مهم ترین پیکسل ها (MSB) علاوه بر افزایش ظرفیت پنهان نگاری، نیاز به ذخیره سازی لبه ها بر روی عکس اصلی را مرتفع کرد.

۲- روش های حوزه تبدیل

روشی ازدسته های پنهان نگاری که به طور مستقیم داده را درون رسانه اصلی جاسازی نمی کنند، روش های حوزه تبدیل نام دارند. در این روشها تصویر باید با استفاده از تبدیلات، از حوزه مکان به حوزه فرکانس برده شود و سپس عملیات جاسازی داده آغاز شود. این روش نسبت به روش های دامنه مکانی، روش های پیچیده تری محسوب می شوند. امروزه بیشتر سیستم های قوی پنهان نگاری در این حوزه توسعه داده شده است. گرچه ظرفیت پنهان سازی این روشها نسبت روشهای LSB کمتر است اما با استفاده از این تبدیل ها میتوان داده را در نواحی از تصویر پنهان ساخت که کمتر در معرض فشرده سازی،برش و پردازش قرار دارند. پرکاربردترین تبدیل DCT است و بیش تر روشها از افزونگی در دامنه DCT می برند. در این مقاله [۳] روش های لبه یابی در دامنه DCT پیاده سازی شدند که الگوریتم های Prewitt و Canny عملکرد بهتری نسبت به فیلترهای Sobel و Laplacian از نظر معیارهای SNR و PSNR داشتند. همچنین DCT نسبت به DWT کیفیت تصویر بهتر و PSNR بالاتری از خود نشان داد. در مقاله ای دیگر [۴] با انتخاب روش با استفاده از الگوریتم Hashing بیت های تصادفی انتخاب میشوند. این کار موجب افزایش امنیت در مقابل حملات میشود. با استفاده از بلوک های ۸*۸ تبدیل DCT اعمال میشود و با استفاده از الگوریتم ژنتیک (GA) مقادیر دامنه فرکانس بهینه شده تا بیت های بیشتری مورد استفاده قرار گیرد. در روشی دیگر [۵] با استفاده از تبدیل JPEG که از بلوک های n*n تبدیل DCT استفاده میکند، کانال های RGB عکس را به YCbCr تبدیل میکند. پیام ورودی با استفاده از الگوریتم رمزگذاری هافمن در ماتریس ورودی درج میشود. در این روش از دو بیت کم‌اهمیت پیکسل ضریب تبدیل کسینوس برای پنهان کردن بیت‌های پیام تعبیه‌شده استفاده می‌شود.

۳- روش های یادگیری عمیق

مدل های CNN پنهان نگاری اغلب به صورت یک encoder-decoder عمل میکنند بدین شکل که به عنوان ورودی دو عکس اصلی و رمزگذاری شده را ارسال می کنند. وظیفه encoder تولید عکسی است که از آن به عنوان عکس رمزگذاری شده stego image یاد میشود. همچنین image stego ورودی decoder می باشد. تفاوت مدل های متفاوت encoder-decoder در معماری شبکه های کانولوشن آن مانند تعداد لایه ها، تعداد فیلترها، اندازه فیلترها، تابع هزینه و دیگر پارامترهای مربوط به معماری شبکه های کانولوشن می باشد. مدل encoder-decoder که توسط این مقاله [۶] ارائه شد از معماری معروف شبکه ی U-Net برای بخش encoder استفاده شد. اندازه ی ورودی این شبکه ۲۵۶*۲۵۶ با ۶ کانال می باشد که عکس اصلی و عکس رمزگذاری شده را دریافت میکند. بخش decoder آن از ۶ لایه کانولوشن برای استخراج استفاده میشود. یکی دیگر از مدل های مبتنی بر شبکه های عصبی عمیق که امروزه در زمینه پنهان نگاری توجه زیادی را به خود جلب کرده شبکه های GANs می باشد.GAN ها نوعی از CNN های عمیق هستند که از نظریه بازی برای آموزش استفاده می کند. یک مدل تولیدی با فرآیند خصمانه وظیفه ی تولید تصویر را بر عهده دارد. یک شبکه ی دیگر که به عنوان شبکه ی ممیز شناخته میشود وظیفه ی بررسی عکس های تولید شده توسط شبکه ی مولد را بر عهده دارد. شبکه ها برای ایجاد یک خروجی عالی با یکدیگر رقابت می کنند.

در چارچوب تصویر پنهان نگاری، شبکه جدیدی به نام steganalyzer در برخی از روش ها معرفی شده است. توابع اصلی از این سه جزء عبارتند از:

- یک مدل مولد، G، برای تولید تصاویر stego ازتصویر اصلی و پیام تصادفی
- یک مدل تفکیک کننده، D، برای تشخیص جعلی یا واقعی بودن تصویر تولید از مولد

• یک Steganalyzer ،S برای بررسی اینکه آیا تصویر ورودی دارای داده های محرمانه است یا نه

سه مدلG، D و S .برای رقابت ساخته شده اند

۳ مدل پشینهاد شده

روش فشرده سازی در تلگرام به صورت JPEG می باشد. به همین سبب الگوریتم پیشنهادی ما نیز در فرمت JPEG پیاده سازی میشود. مراحل فشرده سازی JPEG به صورت زیر می باشد:

• تبدیلRGB به YCbCr

• تبدیل عکس به بلوک های ۸ پیکسل در ۸ پیکسل

• تبدیل مقادیر هر پیکسل به بازه ی -۱۲۸ تا ۱۲۷

• تبدیل گسسته کسینوس

• Quantization

• اسکن پیکسل های به صورت زیگ زاگ

• انجام تبدیلModulation Code Pulse Differential بر روی component DC

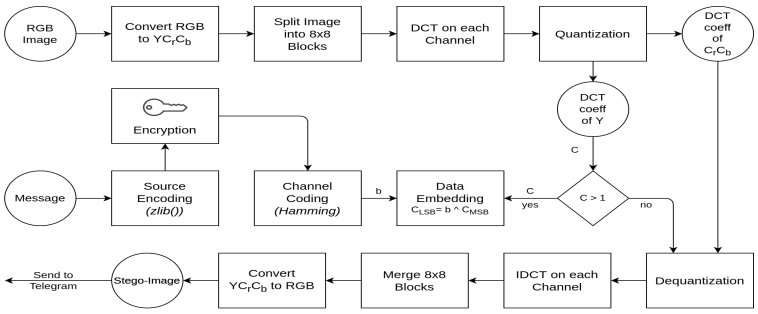
• انجام Encoding Length Run بر روی components AC

• انجام الگوریتم هافمن بر روی نتیجه ی نهایی

مرحله encoding

از آنجایی که در الگوریتم JPEG از (DCT) استفاده میشود، در الگوریتم خود از همین ضرایب برای پنهان سازی پیام استفاده میکنیم. عکس ورودی دارای فرمت RGB تبدیل به فرمت YCbCr می شود. در مرحله ی بعد تبدیل گسسته کسینوسی بر روی بلوک های ۸*۸ عکس اعمال میشود. سپس با استفاده از جدول تعریف شده ی گسسته سازی، quantizaion بر روی ضرایب کسینوسی اعمال میشود. برای مخفی کردن داده، ضرایبی از کانال luminance را که بزرگ تر از یک هستند در نظر میگیریم. برای کد کردن پیام رمز به منظور افزایش امنیت، از الگوریتم رمزنگاری استفاده می کنیم. ابتدا پیام را با استفاده از الگوریتم zlib ، encode میکنیم. سپس با استفاده از الگوریتم رمزنگاری کلید public و private ساخته میشود. در این پروژه الگوریتم رمزنگاری به کاربرده شده RSA می باشد. بیت های پیام کد شده و بیت MSB تصویر با هم xor میشوند و داخل بیت LSB قرار میگیرند. با برگرداندن ضرایب کسینوسی به ضرایب پیکسل های تصویر توسط تابع معکوس آن (IDCT) وتبدیل آن به فرمت RGB عکس خروجی آماده ی ارسال به تلگرام می شود. از آنجایی که در فایل خروجی احتمال خطا وجود دارد از روش کدگذاری Hamming برای تصحیح خطا استفاده می کنیم.

روند کلی الگوریتم در بخش encodeing تصویر به صورت زیر می باشد:



مرحله decoding

برای کدگشایی تصویر دریافت شده از تلگرام، ابتدا تصویر دریافت شده ی RGB را به فرمت YCbCr تبدیل میکنیم. سپس بر روی بلاک های ۸*۸ تبدیل گسسته کسینوسی اعمال میشود. با استفاده از جدول گسسته سازی ضرایب کسینوسی را گسسته می کنیم. به ازای ضرایب کانال luminance که بیشتر از یک می باشند، بیت LSB و MSB آن xor می شوند. سپس با

استفاده از الگوریتم Hamming بیت هایی که دارای خطا می باشند را اصلاح میکنیم و در نهایت با استفاده از کلید private ساخته شده توسط الگوریتم RSA پیام را رمزگشایی میکنیم. روند کلی الگوریتم decoding به صورت زیر می باشد:

۴ نتایج

برای ارزیابی تفاوت کیفیت عکس ورودی و خروجی از معیارهای زیر استفاده میکنیم:

۱- MSE خطای میانگین مربعات (MSE) روشی برای برآورد میزان خطاست که در واقع تفاوت بین مقادیر تخمینی و آنچه تخمین زده شده، است. MSE به دو دلیل تقریباً همه جا مثبت است (صفر نیست) یک اینکه تصادفی است و دوم به این دلیل که تخمین‌گر اطلاعاتی که قابلیت تولید تخمین دقیق تری دارد را حساب نمی‌کند. پس این شاخص که مقداری همواره نامنفی دارد، هرچقدر مقدار آن به صفر نزدیکتر باشد، نشان دهنده میزان کمتر خطاست. فرمول محاسبه ی MSE برای تصویر بدون نویز تک رنگ (خاکستری) با سایز m*n به صورت زیر می باشد:

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - K(i,j))]^2$$

PSNR -۲

PSNR معمولاً برای اندازه گیری کیفیت بازسازی تصاویر و ویدیوهایی که در معرض فشرده سازی با اتلاف هستند (lossy) استفاده می شود.

$$PSNR = 10 \log_{10} \frac{MAX_I^2}{MSE}$$

SSIM -۳

SSIM یک معیار مقایسه ای ساختاری دو تصویر است که براساس ساختار تصاویر طبیعی ارائه شده است. ساختار تصاویر طبیعی به این گونه است که پیکسلها وابستگی زیادی به پیکسلهای مجاور خود دارند و این وابستگی اطلاعات مهمی را درباره ساختار اشیاء در تصویر در بردارد. با محاسبه SSIM میزان مشابهت ساختاری در همسایگی هر پیکسل جداگانه محاسبه می شود .

$$SSIM(I, \widehat{I}) = \left(\frac{2\mu_I \mu_{\widehat{I}} + C_1}{\mu_I^2 + \mu_{\widehat{I}}^2 + C_1} \right)^{\alpha} . \left(\frac{2\sigma_I \sigma_{\widehat{I}} + C_2}{\sigma_I^2 + \sigma_{\widehat{I}}^2 + C_2} \right)^{\beta} . \left(\frac{\sigma_{I\widehat{I}} + C_3}{\sigma_I \sigma_{\widehat{I}} + C_3} \right)^{\gamma}$$

نتایج به دست آمده بر روی عکس بابون در جدول زیر آمده است:

	PSNR	MSE	SSIM
baboon	26.93	58.73	0.85

[1] R. Dumre and A. Dave, "Exploring LSB Steganography Possibilities in RGB Images", 12th International Conference on Computing Communication and Networking Technologies (ICCCNT), 2021, pp. 1-7, doi: 10.1109/ICCCNT51525.2021.9579588.

[2] De Rosal Ignatius Moses Setiadi, "Improved payload capacity in LSB image steganography uses dilated hybrid edge detection", Journal of King Saud University - Computer and Information Sciences,Volume 34, Issue 2,2022,Pages 104-114,ISSN 1319-1578,https://doi.org/10.1016/j.jksuci.2019.12.007.

[3] Nadish Ayub Arvind Selwal, "An improved image steganography technique using edge based data hiding in DCT domain", Journal of Interdisciplinary Mathematics, 2020, 23:2, 357-366, DOI: 10.1080/09720502.2020.1731949

[4] Biswas, R., Bandyapadhay, S.K., "Random selection based GA optimization in 2D-DCT domain color image steganography.", Multimed Tools Appl 79, 2020, 7101–7120., https://doi.org/10.1007/s11042-019-08497-x

[5] A. Darbani, M. M. AlyanNezhadi and M. Forghani, "A New Steganography Method for Embedding Message in JPEG Images," 2019 5th Conference on Knowledge Based Engineering and Innovation (KBEI), 2019, pp. 617-621, doi: 10.1109/KBEI.2019.8735054.

[6] Wu, Pin, Yang Yang, and Xiaoqiang Li., "StegNet: Mega Image Steganography Capacity with Deep Convolutional Network", Future Internet 10, 2018, no. 6: 54. https://doi.org/10.3390/fi10060054

[7] Subramanian, Nandhini Elharrouss, Omar Al-ma'adeed, Somaya Bouridane, Ahmed., "Image Steganography: A Review of the Recent Advances.", IEEE Access., 2021, PP. 1-1. 10.1109/ACCESS.2021.3053998.

[8] Shao-Ping Lu, Rong Wang, Tao Zhong, Paul L. Rosin, "Large-Capacity Image Steganography Based on Invertible Neural Networks", Conference on Computer Vision and Pattern Recognition, 2021.