RAQAMLI TASVIRLARDA LSB ALGORITMI ASOSIDA MA'LUMOTLARNI YASHIRISH SAMARADORLIGI TAHLILI

Rashidova Oydinoy Jo‘rabek qizi
TATU akademik litseyi

Annotatsiya. *Ushbu maqolada steganografiyaning eng keng tarqalgan usuli — Eng kichik ahamiyatli bit (LSB) algoritmi tadqiq etiladi. Tadqiqot davomida matnli ma’lumotlarni ko‘rinmas holda tasvirlarga joylashtirish mexanizmi, stego-ob’ektning vizual sifati va ma’lumot sig‘imi o‘rtasidagi bog‘liqlik o‘rganilgan. Natijalar PSNR (Peak Signal-to-Noise Ratio) koeffitsienti yordamida tahlil qilinib, usulning kiberxavfsizlikdagi o‘rni belgilangan.*

Kalit so‘zlar*: stenografiya, stepic, pil kutubxonasi, axborot xavfsizligi, shovqin*

Kirish

Axborot asrida ma’lumotlarning maxfiyligini ta’minlash faqatgina ularni shifrlash (kriptografiya) bilan cheklanib qolmaydi. Kriptografiya xabarni tushunarsiz holatga keltirsa-da, uning mavjudligi faktini yashira olmaydi, bu esa tajovuzkorlarda shubha uyg‘otishi mumkin. Steganografiya esa maxfiy aloqaning mavjudligini yashirish orqali ushbu muammoni hal qiladi. Raqamli tasvirlar o‘zining yuqori hajmli redundantligi (ortiqcha ma’lumotga egaligi) tufayli steganografik konteyner sifatida eng ko‘p foydalaniladigan ob’ektlar hisoblanadi.

Metodlar

Tadqiqotda LSB (Least Significant Bit) almashtirish usuli qo‘llanildi. Tasvirning har bir piksili RGB (Qizil, Yashil, Ko‘k) rang modelida 24 bitdan (har bir kanal uchun 8 bit) iborat. LSB usulida har bir rang kanalining eng kichik (oxirgi) biti maxfiy xabar bitiga almashtiriladi.

Algoritm qadamlari:

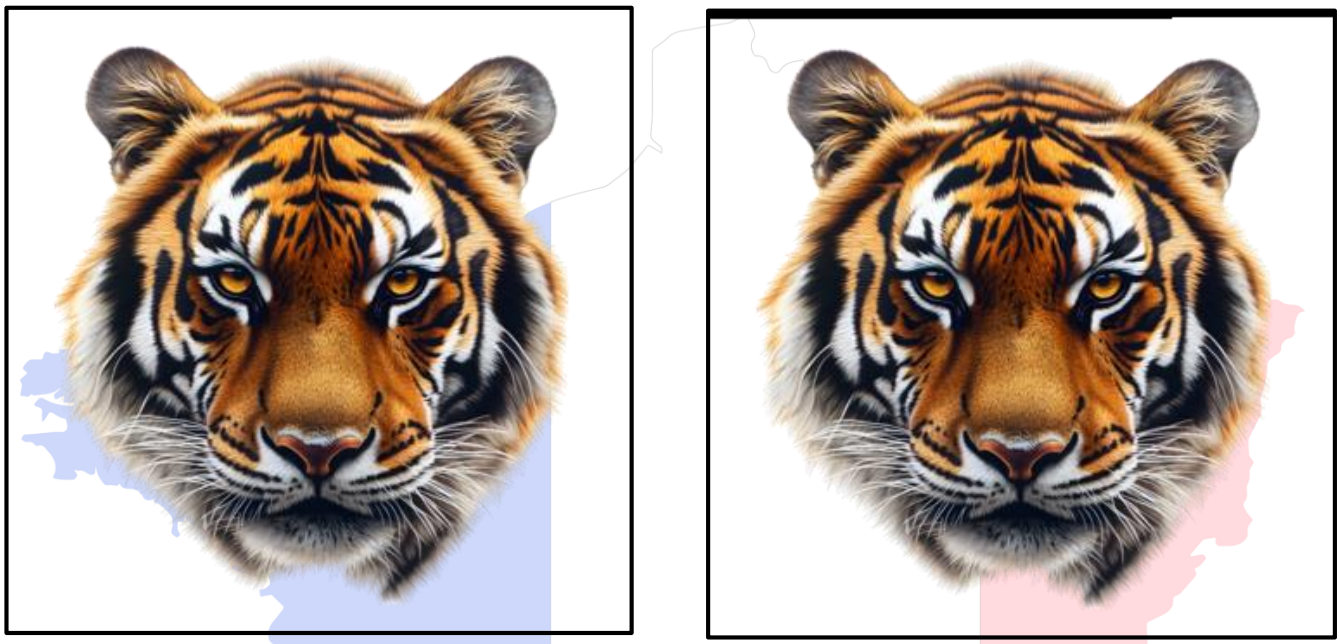
1. Maxfiy matnni ikkilik (binary) ko‘rinishga o‘tkazish.
2. Konteyner tasvirni piksellar massiviga ajratish.
3. Har bir pikselning oxirgi bitini xabar bitlari bilan ketma-ket almashtirish.
4. Olingan natijani yangi fayl (stego-ob’ekt) sifatida saqlash.

stepic moduli Python-da tasvir steganografiyasi bilan shug'ullanish uchun yaratilgan eng sodda va samarali kutubxonalardan biri hisoblanadi. Uning asosiy vazifasi — har qanday ixtiyoriy ma'lumotni (matn, fayl yoki boshqa ma'lumotlar) PNG yoki BMP kabi rasm formatlari ichiga ko'rinmas holatda yashirishdir.

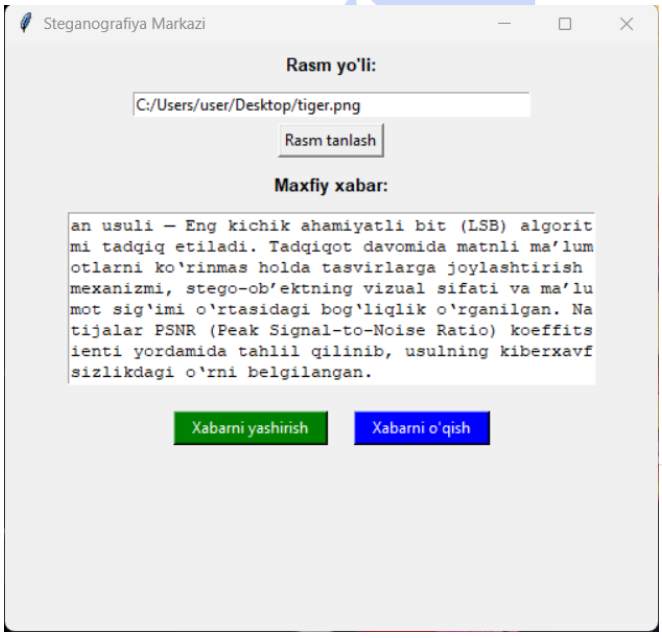
Natijalar

Natijalarga keladigan bo‘lsak,visual o‘xshashlik original va kodlangan rasm o‘rtasida 0.01% farqdan ham kam.Piksel qiymatlari unchalik o‘zgarmagani hisobida, ranglar sezilarli darajada o‘zgarmaydi.

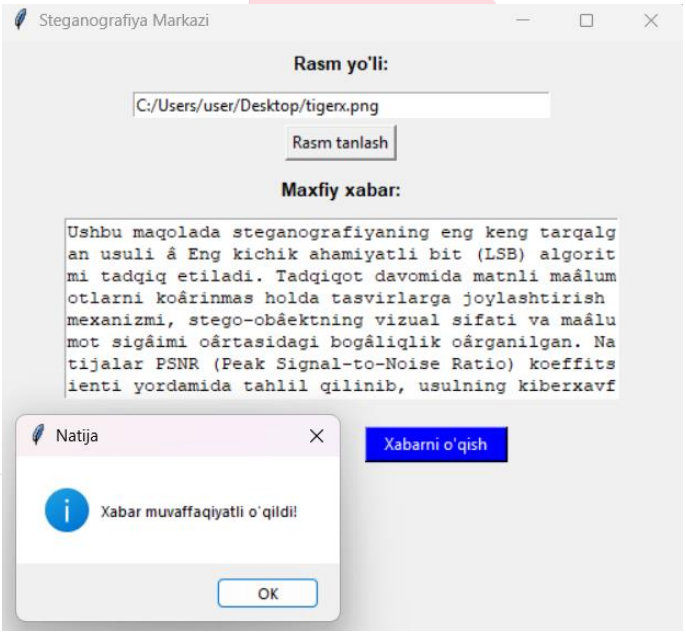
Rasmlar PNG formatida. Shuni hisobidan rasmda shovqin paydo bo‘lmaydi.



1-rasm. Chapdagi rasm haqiqiy rasm, o‘ngdagi rasm stenografiya bilan kodlangan rasm



2-rasm. Matnni rasm ichiga joylashtirish



3-rasm. Rasmdan matnni qayta o‘qish jarayoni

Xulosa. Ushbu tadqiqot doirasida ishlab chiqilgan steganografik dasturiy vosita va olingan natijalar tahlili shuni ko'rsatadiki, LSB (Eng kichik ahamiyatli bit) usuli raqamli ma’lumotlarni yashirin uzatishda hamon eng samarali metodlardan biri bo'lib qolmoqda. Python tilining stepic va PIL kutubxonalari yordamida amalga oshirilgan ushbu loyiha, steganografiyaning asosiy tamoyili — ma’lumot mavjudligi faktining o‘zini yashirish vazifasini muvaffaqiyatli bajardi.

Tahlillar natijasida aniqlandiki, LSB usuli konteyner-tasvirning vizual yaxlitligiga deyarli ta’sir ko‘rsatmaydi. Inson ko‘zi piksellarning quyi bitlaridagi o‘zgarishlarni farqlash qobiliyatiga ega emasligi sababli, stego-tasvir va asl nusxa o‘rtasidagi farqni sub’ektiv baholash imkonsizdir. Bu esa tizimning vizual xavfsizlik darajasi yuqori ekanligidan dalolat beradi. Biroq, texnik tahlil shuni ko‘rsatadiki, usulning asosiy zaifligi statistik hujumlarda namoyon bo‘ladi. Tasvir gistogrammasidagi "juft piksellar"ning sun’iy tenglashishi kabi g‘alati o‘zgarishlar professional steganaliz asboblari orqali maxfiy kanalni fosh qilishi mumkin.

Shu sababli, tizimning kriptografik bardoshliligini oshirish uchun faqatgina steganografiya bilan cheklanib qolmasdan, gibrid himoya usullarini qo‘llash zarur. Xabarni konteynerga joylashdan avval uni AES (Advanced Encryption Standard) kabi zamonaviy algoritmlar yordamida shifrlash, ma’lumot fosh bo‘lgan taqdirda ham uning mazmunini daxlsiz saqlashni kafolatlaydi.

Foydalanilgan adabiyotlar

1. Cheddad, A., et al. (2010). Digital image steganography: Survey and analysis of current methods. Signal Processing.
2. G‘aniyev, S. K. (2019). Kriptografik usullar va axborot xavfsizligi. Toshkent.
3. Johnson, N. F., & Jajodia, S. (1998). Exploring Steganography: Seeing the Unseen. IEEE Computer.
4. Cox, I., et al. (2007). Digital Watermarking and Steganography. Morgan Kaufmann.