

# სტეგანოგრაფიის აპლიკაცია გრაფიკული ინტერფეისით (Whisper)

*მომხსენებელი: მარი ჭოხური*

*თანაავტორი: ნიკა მკრტიჩიანი*

*ელ-ფოსტა: [mari.tchokhuri101@ens.tsu.ge](mailto:mari.tchokhuri101@ens.tsu.ge)*

კომპიუტერულ მეცნიერებათა დეპარტამენტი

ზუსტ და საბუნებისმეტყველო მეცნიერებათა ფაკულტეტი

ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი

პროექტი ეხება ინფორმაციის უსაფრთხოებას, კერძოდ სტეგანოგრაფიასა და კრიპტოგრაფიას. დღესდღეობით, საკმაოდ მარტივია ინფორმაციასთან წვდომა, შესაბამისად, საჭიროდ ჩავთვალეთ მომხმარებლისთვის მიგვეცა ფაილების უსაფრთხოდ შენახვისა და გადაცემის საშუალება. ვცდილობთ, მომხმარებელს მივაწოდოთ შესაბამისი აპლიკაცია, ისეთი ფორმით, რომ მისთვის მარტივად გამოსაყენებელი იყოს. მიუხედავად იმისა, რომ უკვე არსებობს მსგავსი პროგრამული უზრუნველყოფა, Whisper-ი მომხმარებელთან ბევრად უფრო ახლოსაა და არ არის კიბერუსაფრთხოებისთვის შექმნილი მორიგი რთულად გამოსაყენებელი ხელსაწყო, როგორიცაა მაგალითად - StegHide. მომხმარებელს საშუალება აქვს სასურველი ფაილი (ტექსტი თუ ფოტო) “დამალოს” მეორე ფაილში (ტექსტში, ფოტოში, აუდიო ფაილში). ეს ხელს შეუწყობს ინფორმაციის საიმედოდ შენახვას/გაგზავნას/ატვირთვას. და დამატებით, ამ ტექნოლოგიით გამოირიცხულია, იმის დადგენა, რომ საბოლოო ფაილში არსებობს დამალული ინფორმაცია (ტექსტი, ფოტო).

პროექტისთვის გამოყენებულია შემდეგი ტექნოლოგიები: Python (Stegano, PyQt5, Qt Designer, Pillow, Shutil, Crypto.Cipher/AES, ჩვენი შექმნილი მოდული ImageSteganography). მაგალითად, ImageSteganography-ს კოდის მუშაობის პრინციპი მარტივად, რომ ავხსნათ განვიხილოთ ფოტოს ბიტების სტრუქტურა. ფოტო შედგება სამი ძირითადი ფერისგან (RGB). თითო არის 0-დან 255 ბტამდე. ჩვენი მოდული აანალიზებს თითოეულ ბიტს, აიდენტიფიცირებს ყველაზე უმნიშვნელო ბიტებს (ბიტებს, რომლებიც არ მოქმედებენ ფოტოს ხარისხზე და მის ვიზუალზე). ამის შემდეგ, ეს ბიტები ჩანაცვლდება “საიდუმლო ფაილის” ბიტებით.

## ლიტერატურა

(AES, n.d.)

(Pillow, n.d.)

(Qt Group, n.d.)

(chatGPT, n.d.)

(Youtube, n.d.)