სტეგანოგრაფია და მისი გამოყენების პერსპექტივები ინფორმაციის დაცვაში

ბესიკ ბერიძე, მიხეილ დონაძე

ბათუმის შოთა რუსთაველის სახელმწიფო უნივერსიტეტი
b.beridze@bsu.edu.ge, mikheil.donadze@bsu.edu.ge

რეზიუმე

ნაშრომში განხილული და დახასიათებულია კომპიუტერული სტეგანოგრაფია - როგორც ინფორმაციის დაცვის კრეატიული და ერთერთი პერსპექტიული კომპონენტი თანამედროვე ციფრულ ეპოქაში. ნაშრომში აღწერილია სტეგანოგრაფიის არსი, წარმოდგენილია მისი ზოგადი დახასიათება და მოყვანილია ძირითადი ცნებები. ნაშრომი მოიცავს კომპიუტერული სტეგანოგრაფიის მეთოდების დეტალურ კლასიფიკაციასა და ანალიზს, მათ შორის ციფრული სტეგანოგრაფიის LSB, DCT და Spread Spectrum ტექნოლოგიების შედარებას. პრაქტიკულ ნაწილში წარმოდგენილია პროგრამული აპლიკაცია „BSU_Stegano_v.1“, რომელიც ვიზუალურად აჩვენებს სტეგანოგრაფიული მეთოდების მუშაობის პრინციპებს. ნაშრომი მიზნად ისახავს სტეგანოგრაფიის პერსპექტივების გააზრებას, როგორც ლეგიტიმური გამოყენების, ისე კიბერუსაფრთხოების გამოწვევების კონტექსტში, რაც ხელს უწყობს მონაცემთა უსაფრთხოების პრაქტიკის გაუმჯობესებას.

საკვანძო სიტყვები: უსაფრთხოება, ინფორმაციის დაცვა, სტეგანოგრაფია, Phyton

1. შესავალი.

თანამედროვე ციფრულ ეპოქაში, როდესაც ინფორმაციული ტექნოლოგიები ჩვენი ყოველდღიური ცხოვრების განუყოფელი ნაწილია, ინფორმაციის უსაფრთხოებას და კონფიდენციალურობის უზრუნველყოფას განსაკუთრებული მნიშვნელობა ენიჭება. გლობალიზაციის და ციფრული კომუნიკაციების განვითარებასთან ერთად, მატულობს კიბერდამნაშავეობის რისკები და ინფორმაციის არაავტორიზებული წვდომის საფრთხეები.

თანამედროვე ციფრულ ეპოქაში ინფორმაციის დაცვა კრიტიკულ მნიშვნელობას იძენს. ყოველდღიურად მილიარდობით მონაცემი გადაიცემა ინტერნეტის საშუალებით, დაწყებული პირადი მიმოწერებიდან, დამთავრებული კონფიდენციალური კორპორაციული ინფორმაციითა თუ სახელმწიფო საიდუმლოებებით. ამ ინფორმაციის უსაფრთხოებაზე ზრუნვა კომპლექსური ამოცანაა, რომელიც მოიცავს მონაცემთა მთლიანობას, კონფიდენციალურობასა და ხელმისაწვდომობას. ტრადიციული დაცვის მეთოდები, როგორიცაა კრიპტოგრაფია, მიზნად ისახავს ინფორმაციის შინაარსის გაშიფვრას, შეუძლებელი გახადოს არაავტორიზებული პირებისთვის. თუმცა, კრიპტოგრაფიული მეთოდები, მიუხედავად მათი სიმძლავრისა, მაინც ტოვებს კვალს - დაშიფრული შეტყობინების არსებობა თავისთავად იწვევს ეჭვს და შეიძლება მიიქციოს თავდამსხმელის ყურადღება. სწორედ აქ შემოდის თამაშში სტეგანოგრაფია, რომელიც ინფორმაციის დაფარვის ხელოვნებასა და მეცნიერებას წარმოადგენს, ისე რომ მისი არსებობა არ იყოს აშკარა გარე დამკვირვებლისთვის [1].

21-ე საუკუნეში, ციფრული მედიის ფართო გავრცელების ფონზე - სურათები, ვიდეო ფაილები, აუდიო ჩანაწერები და ტექსტური დოკუმენტები - სტეგანოგრაფიული ტექნიკების

გამოყენების შესაძლებლობები მნიშვნელოვნად გაფართოვდა. მალტიმედია ფაილების მასობრივი გამოყენება ინტერნეტ სივრცეში ქმნის იდეალურ გარემოს ფარული კომუნიკაციისთვის.

თანამედროვე კიბერუსაფრთხოების ლანდშაფტში, სადაც კორპორაციული და სახელმწიფო დონეზე ინფორმაციის გაჟონვა სერიოზულ ეკონომიკურ და რეპუტაციულ ზარალს იწვევს, სტეგანოგრაფია წარმოადგენს ინფორმაციის დაცვის ინოვაციურ მექანიზმს. განსაკუთრებით მნიშვნელოვანია მისი როლი სენსიტიური ინფორმაციის ტრანსმისიის დროს, რომელიც მოითხოვს მაქსიმალურ კონფიდენციალურობას.

ხელოვნური ინტელექტის და მანქანური სწავლების ტექნოლოგიების განვითარება ახალ შესაძლებლობებს ქმნის როგორც სტეგანოგრაფიული მეთოდების გაუმჯობესებისთვის, ისე მათი გამოვლენისთვის. ეს ტენდენცია აქტუალურს ხდის სფეროს კვლევის გაღრმავებას და ახალი ხერხების შემუშავებას.

მიუხედავად იმისა, რომ კრიპტოგრაფია წარმატებით იცავს მონაცემთა შინაარსს, იგი ვერ მალავს კომუნიკაციის ფაქტს. სტეგანოგრაფია ამ მიმართულებით სრულიად განსხვავებულ შესაძლებლობას იძლევა: მისი მეშვეობით შესაძლებელია ინფორმაციის გადაცემა ისე, რომ მისი არსებობა შეუმჩნეველი დარჩეს. თანამედროვე რეალობაში, როდესაც მონაცემთა დაცვა ერთ-ერთი მთავარი პრიორიტეტია, როგორც სახელმწიფო, ისე კერძო სექტორისთვის, სტეგანოგრაფიის კვლევა და პრაქტიკული გამოყენება განსაკუთრებით აქტუალურია [1,2].

2. ძირითადი ნაწილი

როგორც შესავალში აღვნიშნეთ სტეგანოგრაფია - ეს არის კავშირის (შეტყობინებების გადაცემის) ორგანიზების მეთოდი, რომლის მიზანიც არის თვითონ კავშირის არსებობის დაფარვა. კრიპტოგრაფიისგან განსხვავებით, სადაც მხარეს ზუსტად შეუძლია განსაზღვროს, არის თუ არა გადაცემული ინფორმაცია დაშიფრული ტექსტი, სტეგანოგრაფიის მეთოდები საშუალებას იძლევა საიდუმლო შეტყობინებები ჩაშენდეს ღია მესიჯებში ისე, რომ შეუძლებელი გახდეს მათი არსებობის ეჭვიც კი.

გამოთვლითი ტექნიკის და ინფორმაციის გადაცემის ახალი არხების განვითარებამ წარმოშვა სტეგანოგრაფიის ახალი მეთოდები, რომლებიც ეფუძნება ინფორმაციის წარმოდგენის თავისებურებებს კომპიუტერულ ფაილებში, გამოთვლით ქსელებში და სხვ. ამ მიმართულებას კომპიუტერული სტეგანოგრაფია წარმოადგენს [3].

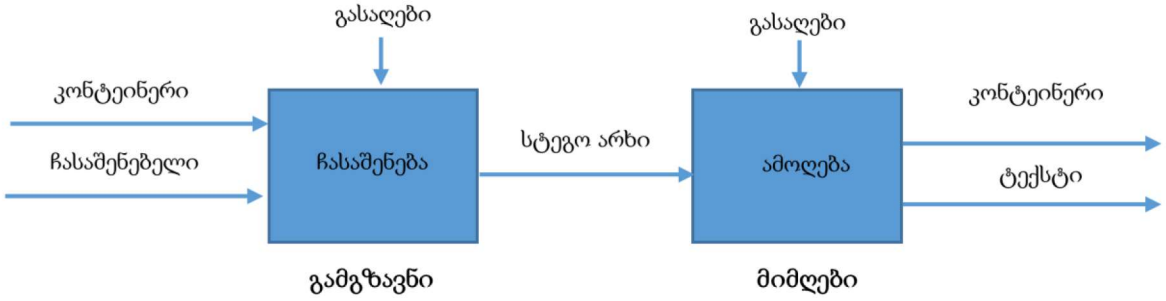
კომპიუტერული სტეგანოგრაფია ორი ძირითადი პრინციპის საფუძველზე მოქმედებს:

1. ფაილები, რომლებიც შეიცავენ ციფრულ გამოსახულებას ან ხმას, გარკვეულ დრომდე შეიძლება შეიცვალოს ფუნქციური დანიშნულების დაკარგვის გარეშე, განსხვავებით სხვა ტიპის მონაცემებისა, რომლებიც აბსოლუტურ სიზუსტეს საჭიროებენ.
2. ადამიანის გრძნობითი ორგანოები ვერ ამჩნევენ უმნიშვნელო ცვლილებებს გამოსახულების ფერში ან ხმის ხარისხში. ეს პრინციპი განსაკუთრებით ეფექტურია იმ გამოსახულებისა ან ხმის შემთხვევაში, რომელიც შეიცავს ზედმეტ (redundant) ინფორმაციას.

იმის გამო, რომ კომპიუტერული სტეგანოგრაფია არის ინფორმაციის დაცვის შედარებით ახალი სფერო და აქამდე არ არსებობდა ერთიანი ტერმინოლოგია, მეცნიერების მიერ შემოთავაზებულ იქნა ტერმინების სისტემატიზაცია. სტეგანოგრაფიული სისტემა ანუ სტეგოსისტემა, რომელიც წარმოადგენს იმ საშუალებებისა და მეთოდების ერთობლიობას, რომლებიც გამოიყენება ფარული საკომუნიკაციო არხის შესაქმნელად. სტეგოსისტემის აგებისას უნდა გათვალისწინებულ იქნას შემდეგი პირობები [1,3]:

- დამალვის მეთოდებმა უნდა უზრუნველყოს იმ ინფორმაციის ავთენტურობა და მთლიანობა, რომელშიც შეტყობინება იმალება;
- მოწინააღმდეგემ შეიძლება სრულად იცოდეს სტეგანოგრაფიული სისტემა და მისი დეტალები. ერთადერთი, რაც მისთვის უცნობია, არის საკვანძო ინფორმაცია (key), რომლის მეშვეობითაც მხოლოდ მფლობელს შეუძლია ფარული შეტყობინების არსებობისა და შინაარსის დადგენა;
- თუკი მოწინააღმდეგეს როგორიც არ უნდა იყოს, შეეტყო ფარული შეტყობინების არსებობა, ეს არ უნდა აძლევდეს მას საშუალებას, ამოიღოს ფარული ინფორმაცია სხვა მონაცემებიდან მანამ, სანამ კლავიში დაცულია საიდუმლოდ;
- პოტენციური მოწინააღმდეგე უნდა იყოს მოკლებული ნებისმიერ ტექნიკურ თუ სხვა უპირატესობას ფარული შეტყობინებების ამოცნობასა და გაშიფვრაში.

სტეგოსისტემის სტრუქტურული სქემა (იხილეთ. სურ. 1).



სურ. 1 სტეგანოგრაფიის სტრუქტურული სქემა

საიდუმლო გასაღების მქონე სტეგოსისტემაში გამოიყენება ერთი გასაღები, რომელიც ან წინასწარ უნდა იყოს განსაზღვრული, ან უნდა გადაეცეს დაცული არხით. ღია გასაღების მქონე სტეგოსისტემაში შეტყობინების ჩასაშენებლად და ამოსაღებად გამოიყენება სხვადასხვა გასაღებები, რომელთა შორის კავშირის დადგენა გამოთვლითაც შეუძლებელია. ამგვარად, ღია გასაღების თავისუფლად გადაცემა შესაძლებელი ხდება დაუცველი არხის მეშვეობით.

სტეგანოგრაფიის მეთოდებს შორის ყველაზე გავრცელებულია სამი მეთოდი, ესენია: LSB (ყველაზე ნაკლებად მნიშვნელოვანი ბიტი), DCT (დისკრეტული კოსინუსური ტრანსფორმაცია) და Spread Spectrum (გაშლილი სპექტრი). სამივე მეთოდი არის ციფრული სტეგანოგრაფიის საშუალებების. ისინი შექმნილია ციფრული მედიისთვის და მუშაობს კომპიუტერული ალგორითმების საშუალებით. თითოეულ მათგანს აქვს თავისი უპირატესობები და ნაკლოვანებები, რაც განსაზღვრავს მათ გამოყენების სფეროებს [6,7].

სტეგანოგრაფიის ტექნოლოგიის არჩევა დამოკიდებულია კონკრეტულ მოთხოვნებზე, როგორიცაა მონაცემთა ტევადობა, უსაფრთხოების დონე და მდგრადობა შეტევების მიმართ. დასკვნის სახით შეიძლება ითქვას, რომ LSB საუკეთესოა მაშინ, როდესაც საჭიროა დიდი რაოდენობით მონაცემების სწრაფად დამალვა და არ არის მაღალი მოთხოვნები სიმყარეზე (მაგალითად, მოკლე ვადით გადაცემა მეგობრებს შორის). DCT უზრუნველყოფს უკეთეს ბალანსს ტევადობასა და სიმყარეს შორის, განსაკუთრებით JPEG გამოსახულებების შემთხვევაში. ის ხშირად გამოიყენება წყლის ნიშნების (watermarking) დასამატებლად. Spread Spectrum არის ყველაზე ძლიერი და უსაფრთხო მეთოდი, რომელიც უზრუნველყოფს მაქსიმალურ სიმყარეს სხვადასხვა სახის შეტევების მიმართ, თუმცა მონაცემთა დაბალი

ტევადობით. ის იდეალურია აპლიკაციებისთვის, სადაც ინფორმაციის დამალვის ფაქტი თავისთავად უნდა დარჩეს საიდუმლოდ და უსაფრთხოება უმთავრესია [6,7].

თანამედროვე სტეგანოგრაფიაში ხშირად გამოიყენება ამ მეთოდების კომბინაციები, რათა გაუმჯობესდეს როგორც სიმტკიცე, ასევე მონაცემთა ტევადობა და შეუმჩნევადობა. ნაშრომში განხილული მიდგომების გათვალისწინებით Phyton-ის პლატფორმაზე რეალიზებული იქნა პროგრამული აპლიკაცია „BSU_Stegano_v.1“. აპლიკაცია შეიქმნა ნაშრომში განხილული სტეგანოგრაფიული და კრიპტოგრაფიული მეთოდების და ალგორითმების კომბინაციით, ანუ შემოთავაზებულია ჰიბრიდული მიდგომა. პროგრამა იყენებს LSB (Least Significant Bit) სტეგანოგრაფიას, საიდუმლო ტექსტის სურათში დამალვისთვის და Fernet შიფრაციას უშუალოდ ტექსტის დაშიფვრისათვის.

იმპლემენტაციის პროცესში გამოყენებული იქნა Phyton-ის ძირითადი ბიბლიოთეკები:

ბიბლიოთეკა	**დანიშნულება**
PyQt6	მომხმარებლის გრაფიკული ინტერფეისის შესაქმნელად
stepic	ტექსტის სტეგანოგრაფიული დამალვა გამოსახულებაში
Pillow (PIL)	გამოსახულებების ჩატვირთვა, შენახვა და რედაქტირება
cryptography.fernet	ტექსტის უსაფრთხო დაშიფვრა და გაშიფვრა
codecs, os, sys	სისტემური ოპერაციები და ფაილური მენეჯმენტი

ცხრილი 1. აპლიკაციაში გამოყენებული Phyton-ის ბიბლიოთეკები

ეს ბიბლიოთეკები დაფუძნებულია ღია კოდზე და pip ინსტრუმენტი საშუალებას გაძლევს აღნიშნული პაკეტები (ბიბლიოთეკები) ადვილად დავაინსტალიროთ, განვაახლოთ ან წავშალოთ.

კრიპტოგრაფიული გასაღების ავტომატური დაგენერირება ჩვენს მიერ შემუშავებული მეთოდის საშუალებით.

პროექტის რეალიზაციისათვის საჭიროა სისტემის მოთხოვნები: Python 3.7 ან უფრო მაღალი ვერსია, Windows/Linux/macOS მხარდაჭერა, მეხსიერება მინიმუმ 4GB RAM და 100MB თავისუფალი ადგილი დისკზე.

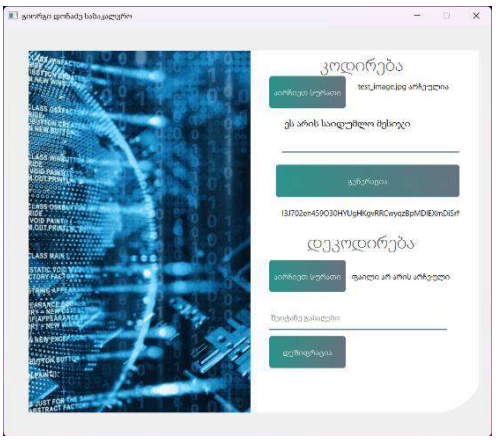
სისტემა შემუშავებულია მოდულური პრინციპებით და შედგება შემდეგი ძირითადი კომპონენტისგან:

- main.py – პროგრამის შესასვლელი ფაილი, რომელიც აერთიანებს UI-სა და ფუნქციურობას.
- stegano_encryptor.py – პასუხისმგებელია კოდირებაზე (დაშიფვრა და სტეგანოგრაფია).
- stegano_decryptor.py – პასუხისმგებელია გაშიფვრაზე (სტეგანოგრაფიიდან ამოღება და გაშიფვრა).

ენკოდინგის მოდული შედგება შემდეგი კომპონენტებისაგან: გრაფიკული ინტერფეისი საიდუმლო ტექსტის შესაყვანად, სურათის ფაილის არჩევის ფუნქციონალი, კრიპტოგრა-ფიული გასაღების გენერაცია, სტეგანოგრაფიული ენკოდინგი.

დეკოდინგის მოდული აერთიანებს შემდეგ კომპონენტებს: შიფრაციული გასაღების შეყვანის ინტერფეისი, სტეგანო-სურათის არჩევის ფუნქციონალი, ტექსტის აღდგენა და დეშიფრაცია.

როგორ მუშაობს სისტემა. ვპროგრამის ინტერფეისი მარტივი და მოსახერხებელია. მომხმარებელი ირჩევს სასურველ სურათს (test_image.jpg), შესაბამის ველში შეგვყავს ტექსტი "ეს არის საიდუმლო მესიჯი", შემდეგ დავაჭიროთ ღილაკს "გენერაცია".



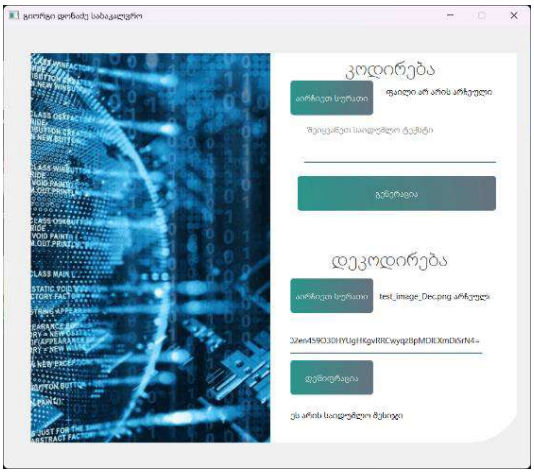
სურ. 2 სტეგანოგრაფიული ენკოდინგი - პროგრამის ძირითადი სამუშაო ფანჯარა

პროგრამა შექმნის ორ ფაილს test_image_Dec.png და test_image.txt

სურ. 3 სტეგანოგრაფიული ენკოდინგის შედეგი

სურათში დაშიფრული საიდუმლო ტექსტის წაკითხვა/აღდგენა.

1. ავირჩიეთ ენკოდირებული სურათი
2. შევიყვანეთ გასაღები
3. დავაჭირეთ "დეშიფრაცია" ღილაკს



სურ. 4 შედეგი: თავდაპირველი ტექსტი აღდგა

განვიხილოთ სისტემის უსაფრთხოების ანალიზი, პროგრამული პაკეტი აერთიანებს როგორც სტეგანოგრაფიული ასევე კრიპტოგრაფიული უსაფრთხოების მეთოდებს და ალგორითმებს.

სტეგანოგრაფიული უსაფრთხოება იყენებს **LSB** მეთოდის პრინციპს, რაც უზრუნველყოფს შემდეგ ბენეფიტებს:

- მონაცემების დამალვა უმნიშვნელო ბიტებში
- არ შეიმჩნევა ვიზუალური ცვლილებები
- სტატისტიკური ანალიზი რთულია

კრიპტოგრაფიული უსაფრთხოება იყენებს **Fernet** სიმეტრიული შიფრაციის მეთოდს, რომელიც შედის Python-ის cryptography ბიბლიოთეკაში. იგი არის უსაფრთხო და მარტივი გზა მონაცემების დაშიფვრისა და გაშიფვრისთვის. Fernet იდეალურია მონაცემების, ფაილების, პაროლების დაშიფვრისთვის, რადგან უზრუნველყოფს მაღალ უსაფრთხოებას და ადვილია გამოსაყენებელი. კვლევის სიახლეა Fernet შიფრაციის ჩვენს მიერ შერჩეული მახასიათებლები:

- AES 128-bit ენკრიფცია CBC რეჟიმში
- ჩაშენებული authentication (HMAC) - ამოწმებს მონაცემების მთლიანობას
- გასაღების მდგრადობა - 256-bit
- შიფრაციის ტიპი - სიმეტრიული შიფრაცია

პროგრამის ბენეფიტები და უპირატესობა მსგავსი პროდუქტებისგან განსხვავებით არის:

- ყოველ ახალ ენკოდინგზე გენერირდება ახალი გასაღები
- ტექსტი ჯერ იშიფრება და შემდეგ იმალება გრაფიკულ ფაილში
- წყარო ფაილი უცვლელი რჩება, არ ხდება მისი დაზიანება (დამახინჯება)

დაშიფვრა: Fernet ბიბლიოთეკა აკმაყოფილებს თანამედროვე უსაფრთხოების სტანდარტებს (AES-128 CBC + SHA256 HMAC).

სტეგანოგრაფია: ვიზუალურად ვერ შეიმჩნევა ცვლილება, ასევე მავნე სუბიექტისთვის PNG ფაილის ბიტური ანალიზი შეუძლებელია.

პროგრამას აქვს მცირე შეზღუდვაც, იგი მუშაობს მხოლოდ PNG/JPG ფორმატების გრაფიკულ ფაილებთან და არ აქვს სხვა ტიპის ფაილების მხარდაჭერა. სამომავლოდ რეკომენდებულია გაუჯობესება, რომ შესაძლებელი იყოს მეტი, განსხვავებული ფორმატის ფაილის ფორმატის მხარდაჭერა, „ბენჩმარკინგი“ - პროცესის ანალიზი სხვადასხვა ტიპის ფაილებისთვის და QR კოდის მხარდაჭერა გასაღებისთვის.

პროგრამამ გაიარა შემდეგი ტიპის ტესტირება:

ტესტი	აღწერა	სტატუსი
სწორი დაშიფვრა-გაშიფვრა	ტექსტი სრულად აღდგენილი	☑
არასწორი გასაღები	გაშიფვრა უარყოფილია	☑
დიდი ტექსტი	შეტყობინება შეზღუდვის შესახებ	☑
არასწორი გამოსახულება	შეცდომის დაფიქსირება	☑
გამოსახულების გარეგნული კონტროლი	უცვლელი ვიზუალი	☑

3. დასკვნა

ნაშრომი მიზნად ისახავდა ინფორმაციის დაცვაში სტეგანოგრაფიის პერსპექტივების განხილვას, მისი არსიდან და ზოგადი დახასიათებიდან დაწყებული, თანამედროვე მეთოდებისა და ტექნოლოგიების შედარებითი და ანალიზით დამთავრებული. შესრულებული კვლევის ფარგლებში, დეტალურად იქნა გაანალიზებული ციფრული სტეგანოგრაფიის ძირითადი ცნებები, მისი მეთოდების კლასიფიკაცია და თითოეული მათგანის სპეციფიკა.

კვლევა ადასტურებს, რომ სტეგანოგრაფია რჩება ინფორმაციის დაცვის აქტუალურ და მზარდ მიმართულებად. მიუხედავად იმისა, რომ იგი შეიძლება გამოყენებულ იქნას როგორც ლეგიტიმური მიზნებისთვის (მაგალითად, ინტელექტუალური საკუთრების დაცვა, ცენზურის გვერდის ავლა), ის ასევე წარმოადგენს საფრთხეს კიბერუსაფრთხოებისთვის (მაგალითად, მავნე პროგრამების დამალვა). შესაბამისად, სტეგანოგრაფიის პრინციპების, მეთოდებისა და ტექნოლოგიების სიღრმისეული გაგება კრიტიკულია, როგორც მონაცემთა უსაფრთხოების სპეციალისტებისთვის, ისე ზოგადად ციფრული სამყაროს მომხმარებლებისთვის. ნაშრომში წარმოდგენილი კვლევა ხელს უწყობს ამ სფეროს უკეთ გააზრებასა და პოტენციური საფრთხეების დროულად იდენტიფიცირებასა და მათზე რეაგირებას.

გამოყენებული ლიტერატურა:

1. Hassaballah, M., & Ali, A. A. (2020). Digital Media Steganography: Principles, Algorithms, and Advances. Academic Press
2. Wayner, P. (2008). Disappearing Cryptography: Information Hiding: Steganography and Watermarking (3rd ed.). Publisher Morgan Kaufmann
3. Fridrich, J. (2009). Steganography in Digital Media: Principles, Algorithms, and Applications. Cambridge University Press.
4. Zhang, X., & Wang, S. (2006). Efficient Steganographic Embedding by Exploiting Modification Direction. IEEE Communications Letters, 10(11), 781-783
5. Holub, V., & Fridrich, J. (2012). Designing Steganographic Distortion Using Directional Filters. IEEE Workshop on Information Forensics and Security (WIFS), 234-239
6. Luo, W., Huang, F., & Huang, J. (2010). Edge Adaptive Image Steganography Based on LSB Matching Revisited. IEEE Transactions on Information Forensics and Security, 5(2), 201-214.
7. Subramanian, N., Elharrouss, O., Al-Maadeed, S., & Bouridane, A. (2021). Image Steganography: A Review of the Recent Advances. IEEE Access, 9, 23409-23423.

Steganography and its application prospects in information protection

Besik Beridze, Mikheil Donadze

Batumi Shota Rustaveli State University

b.beridze@bsu.edu.ge, mikheil.donadze@bsu.edu.ge

Abstract

The paper discusses and characterizes computer steganography - as a creative and one of the promising components of information protection in the modern digital era. The paper describes the essence of steganography, provides its general characterization and presents the main concepts. The paper includes a detailed classification and analysis of computer steganography methods, including a comparison of digital steganography technologies LSB, DCT and Spread Spectrum. The practical part presents the software application **"BSU_Stegano_v.1"**, which visually demonstrates the principles of steganographic methods. The paper aims to understand the perspectives of steganography, both in the context of legitimate uses and cybersecurity challenges, which contributes to improving data security practices.

Keywords: Security, Information Protection, Steganography, Phyton