



Viti i XVI-të i Botimit, Nr.1

Qershor 2024

APLIKIMI I TEKNIKËS SË STEGANOGRAFISË NË HARTA GJEOLGJIKE.

Ana Dindi*

**Departamenti i Inxhinierive, Fakulteti i Shkencave të Aplikuara dhe Ekonomike,
Albanian University*

Abstrakt

Të dhënat e ndjeshme nga studimet gjeologjike, si përshembull informacione mbi vendndodhjen e burimeve të pasura minerale mund të fshihen brenda hartës për t'u mbrojtur nga persona të paautorizuar. Ky artikull paraqet aplikimin e teknikës së steganografisë në hartë nëpërmjet një programi të quajtur MapSpace. Qëllimi është të ofrojë një mënyrë sa më të sigurt për të mbrojtur, menaxhuar dhe për të deshifruar të dhënat e përdoruesve të aplikacionit nëpërmjet imazheve. Përdorimi i steganografisë në hartë siguron që informacioni të jenë i padukshëm për të tjerët, ndërsa aftësia për ta menaxhuar dhe për ta lexuar atë brenda programit siguron një përvojë të sigurt për aplikuesit. Rezultati është harta e gjeneruar nga programi pa asnjë ndryshim të dukshëm në rezolucion nga origjinali.

Fjalë çelës: *bazë të dhënash, steganografia, hartë, fshehje, të dhënat.*

THE APPLICATION OF STEGANOGRAPHY TECHNIQUES IN GEOLOGICAL MAPS.

Abstract

Sensitive data from geological studies, such as information on the location of rich mineral resources, can be hidden within the map to protect them from unauthorized persons. This article presents the application of steganography techniques in maps through a program called MapSpace. The aim is to provide a secure way to protect, manage, and decrypt user data through images. The use of steganography in maps ensures that the information is invisible to others, while the ability to manage and read it within the program provides a secure experience for applicants. The result is a map generated by the program with no visible change in resolution from the original.

Key Words: *database, steganography, map, hiding, data.*

1. Hyrje

Steganografia është një nga mënyrat më të avancuara dhe më të efektshme për të fshehur informacionin. Në kohërat moderne, kur të dhënat në internet janë të rrezikuara për shkelje të privatësisë dhe përgjime, steganografia ofron një mjet të fuqishëm për mbrojtje të informacionit nga sytë e paautor-

izuar. Përveç shërbimit për qëllime të fshehta, ajo gjithashtu ka përdorime të ndryshme në fusha si computer science [8], kriptografia [9], si dhe inteligjenca artificiale [7].

Emri steganografi e ka origjinën e saj nga Greqishtja, duke u përkthyer fjalë për fjalë si "shkrim i mbuluar" [1]. Ky term përshkruan mirë funksionin e kësaj teknike, e cila është arti i kamuflimit të informacionit pa ngritur dyshime. Regjistrimi i parë i termit "steganografi" u gjet në librin *Steganographia* të Johannes Trithemius në 1499 [6]. Teknika e parë e dokumentuar e steganografisë raportohet të ketë ndodhur në shekullin V para erës sonë, kur njerëzit përdornin mesazhe të fshehta të mbuluara me dyll në pllaka. Historia përshkruan edhe raste si ai i Histiaeus, tiranit të Miletit nën mbretin Persian Darius I, që kërkonte të komunikonte me dhëndrin e tij. Për ta bërë këtë, ai përdori një skllav të besuar, duke tatuazhuar mesazhin në kokën e tij. Ky rast tregon përdorimin e steganografisë në kontekste të ndryshme historike për të fshehur informacionin. Sot, me rritjen e aktivitetit të shkaktuar nga interneti, nevoja për komunikim të sigurt dhe të fshehtë është më e rëndësishme se kurrë. Steganografia ofron një mjet efektiv për të siguruar komunikim të fshehtë, duke u bërë një pjesë e rëndësishme e mjeteve për mbrojtjen dhe sigurinë e informacionit.

Në këtë artikull është përdorur teknika LSB (Least Significant Bit) [4] për të fshehur informacionin në hartë. Metodë në të cilën bitet e fundit (më pak të rëndësishëm) të pixelave të hartës (imazhit) janë modifikuar për të mbajtur të dhënat e fshehura. Ky përdorim i LSB në steganografi është bërë për të kamufluuar informacionin në hartë duke e bërë të padukshme për një shikues të zakonshëm, dhe mundësinë e përdorimit për shkëmbime të sigurta të informacionit ose për të shtuar detaje të tjera në hartë. Informacioni mund të deshifrohet në çdo moment vetëm nga personat që kanë akses të hyjnë në aplikacion, të cilët kanë bërë të mundur fshehjen e atij mesazhi më parë. Parimi i sigurisë së informacionit të fshehur është shumë i rëndësishëm pasi siguron integritetin dhe besueshmërinë e të dhënave dhe mund të minimizojë rreziqet e shkeljes së privatësisë dhe sulmeve të mundshme të sigurisë.

2. Teknika Least Significant Bit (LSB) e steganografisë

Least Significant Bit (LSB) steganography [2] është një teknikë e përdorur në kontekstin e mbrojtjes dhe manipulimit të të dhënave në hartë përmes metodës së steganografisë. Kjo metodë përdor bitet e fundit (më pak të rëndësishëm) të pixelave të imazhit për të fshehur informacionin e dëshiruar. Në kontekstin e mbrojtjes dhe manipulimit të të dhënave në hartë, teknika LSB mund të përdoret për të fshehur informacione të ndryshme, siç janë shënime, udhëzime, apo edhe të dhëna të ndjeshme, brenda hartave. Kjo mund të jetë e rëndësishme për të ruajtur integritetin e të dhënave, për të mbrojtur privatësinë, ose për të dërguar informacione të fshehur në mënyrë të sigurt.

Për shembull, në një imazh me ngjyra RGB (ku përfaqësohen pixelat me ngjyrë të kuqe, jeshile, dhe blu), secili piksel ka tre vlera për të tre ngjyrat, të cilat janë të shprehura si numra binarë me 8 bite. Në LSB, për të fshehur një bit të dhënë të informacionit, vlera e pikselit në njërin ose në të gjitha ngjyrat modifikohet në mënyrë që biti i fundit i pikselit të përshtatet me vlerën e bitit të dhënë të informacionit për t'u fshehur. Për shembull, nëse do të fshehim bitin 1 (te fundit) të një informacioni në një piksel të caktuar në ngjyrën e kuqe të imazhit, dhe vlera binare e pikselit për këtë ngjyrë është 10101001, për të mbajtur shumë ngjashëm perceptimin vizual, mund të ndryshojmë vlerën e fundit të pikselit nga 1 në 0, duke bërë numrin të ndryshojë në 10101000.

Ky ndryshim i vogël nuk është perceptuar nga shikuesi, por mund të kodohet dhe dekodohet për të rikuperuar të dhënat e fshehura. Kështu, informacioni i fshehur është integruar në imazh në një mënyrë që nuk duket e dukshme për ata që shikojnë imazhin pa njohur një algoritëm të veçantë për ta zbuluar atë.

Për të zgjidhur disa nga sfidat dhe kufizimet e metodës bazë LSB u krijua LSB+, ku dallimi kryesor midis LSB dhe LSB+ është se metoda LSB+ përdor disa bite shtesë për fshehjen e informacionit, duke u përpjekur të minimizojë ndryshimet në imazh, duke bërë që ky i fundit të duket më natyral dhe më i vështirë për të zbuluar ndryshimet që mund të pësojë.

Në përgjithësi, LSB+ u krijua për të ofruar një alternativë më të sigurt dhe më të avancuar në krahasim me metodën bazë LSB, duke përmirësuar kështu rezistencën ndaj sulmeve dhe duke ofruar një performancë më të mirë.

3. Tipet e hartave ku aplikohet teknika LSB

Metoda e LSB mund të përdoret për të fshehur informacion në një gamë të gjerë të tipeve të imazheve.

- a) Tipi i parë janë ato imazhe hartash që përdorin vetëm ngjyrat bardhë e zi për të përfaqësuar informacionin.
- b) Tipi i dytë janë imazhe hartash që përdorin një gamë të ngjyrave për të përfaqësuar informacionin. Secili piksel ka një komponent të ngjyrës së kuqe (R), një komponent të ngjyrës së jeshile (G) dhe një komponent të ngjyrës së blu (B).
- c) Tipi i tretë janë imazhe hartash të mbushura me teksturë (uji, ndërtesa etj).

4. Aplikimet e Teknikave të Steganografisë në Hartat Gjeologjike

Aplikime potenciale të teknikave të steganografisë në kontekstin e mbrojtjes së të dhënave gjeologjike të ndjeshme në hartat përfshijnë:

- Mbrojtjen e Informacionit të Ndjeshëm: Informacioni i lidhur me burimet minerale të vlefshme dhe të rralla mund të fshehet në hartat gjeologjike për të mbrojtur ato nga personat e paautorizuar.
- Raportimi i Informacionit Konfidencial: Për projektet gjeologjike që përfshijnë të dhëna të ndjeshme për territorin apo burimet natyrore, steganografia mund të përdoret për të përcjellë raporte sekrete në mënyrë të fshehtë.
- Siguria në Komunikim: Për gjeologët që punojnë në terren, mund të krijojnë dhe të ndajnë mesazhe të fshehura në hartat gjeologjike për të koordinuar veprimet pa rrezikuar sigurinë e informacionit.

5. Parandalimi i rrezikut të manipulimit të të dhënave në hartë

Kohët e fundit, ekspertë në teknologjinë e informacionit kanë kuptuar se përdorimi i paligjshëm i steganografisë mund të bëhet një kërcënim për sigurinë e informacionit në të gjithë botën [5]. Steganografia mund të mundësojë terroristëve, për shembull, të komunikojnë në fshehtësi pa dijeni të autoriteteve ligjore për këtë komunikim. Ekziston rreziku që personat e paautorizuar të mund të përpiqen të zbulojnë ose të manipulojnë të dhënat e fshehura brenda imazheve. Nëse të dhënat e fshehura përdoren për qëllime të këqija, siç janë shpërndarja e informacionit të rremë, kryerja e krimeve të kibernetike, apo përgatitja e sulmeve terroriste, kjo mund të sjellë pasoja të rënda për sigurinë dhe stabilitetin e një sistemi ose një shoqërie.

Megjithatë, është e rëndësishme të përdoren teknika të ndryshme për të parandaluar këto rreziqe dhe për të siguruar integritetin dhe sigurinë e të dhënave të fshehura nëpërmjet steganografisë në harta. Këto teknika mund të përfshijnë përdorimin e algoritmeve të fuqishme të kriptografisë [9] për të fshehur dhe për të mbrojtur të dhënat, përdorimin e teknikave të monitorimit dhe zbulimit të sulmeve, si dhe implementimin e politikave të sigurisë të përshtatura në nivel organizativ për të mbrojtur integritetin e të dhënave.

6. Mbrojtja e të dhënave në hartë

Një nga mënyrat më efektive për të mbrojtur të dhënat është përdorimi i enkriptimit përpara se këto të dhënat të ruhen brenda hartave [5]. Gjithashtu janë të rëndësishme politikat dhe procedurat e qarta për menaxhimin dhe mbrojtjen e të dhënave të fshehura nëpërmjet steganografisë. Kjo përfshin procedurat për enkriptimin dhe dekriptimin e të dhënave, hartimin e rregullave për përdorimin, politikat për mbrojtjen dhe integritetin e të dhënave, politikat për autorizimin dhe access-in, si dhe trajnimin e personelit për të kuptuar rreziqet e mundshme dhe veprimet në rast të incidenteve të sigurisë.

6.1 Kufizimet dhe lejet për përdorimin e steganografisë

Në disa vende, mund të ketë kufizime ose leje për përdorimin e teknologjisë së steganografisë, veçanërisht nëse përdoret në kontekste të ndjeshme apo për qëllime të caktuara si siguria kombëtare. Përdorimi i steganografisë për të mbrojtur të dhënat duhet të përputhet me standartet etike dhe përgjegjësinë profesionale të përdoruesve. Kjo përfshin trajtimin e të dhënave me respekt, shmangien e përdorimit të tyre për qëllime të paligjshme dhe zbatimin e praktikave të sigurisë së përshtatshme. Është e rëndësishme që përdoruesit të informohen dhe të kenë transparencë lidhur me përdorimin e steganografisë, për mbrojtjen e të dhënave të tyre nëpërmjet hartave. Kjo përfshin informimin e tyre lidhur me teknikat e përdorura dhe qëllimin e fshehjes së të dhënave.

7. Implementimi i steganografisë në hartë duke përdorur teknikën LSB

Programi është ndërtuar në gjuhën JavaScript. Kodin në html (index.html), i cili është njëkohësisht frontend për programin. Backend – i është ndërtuar në gjuhën JavaScript (index.js) dhe (script.js). Libraria përkatese e përdorur për funksionimin e programit është steganography.dot.js. Ekzekutimi i programit bëhet në një browser të çfarëdoshëm. Emri i të cilit është MapSpace, mjaftueshëm lehtësi në përdorim dhe i aksesueshëm nga çdo përdorues.

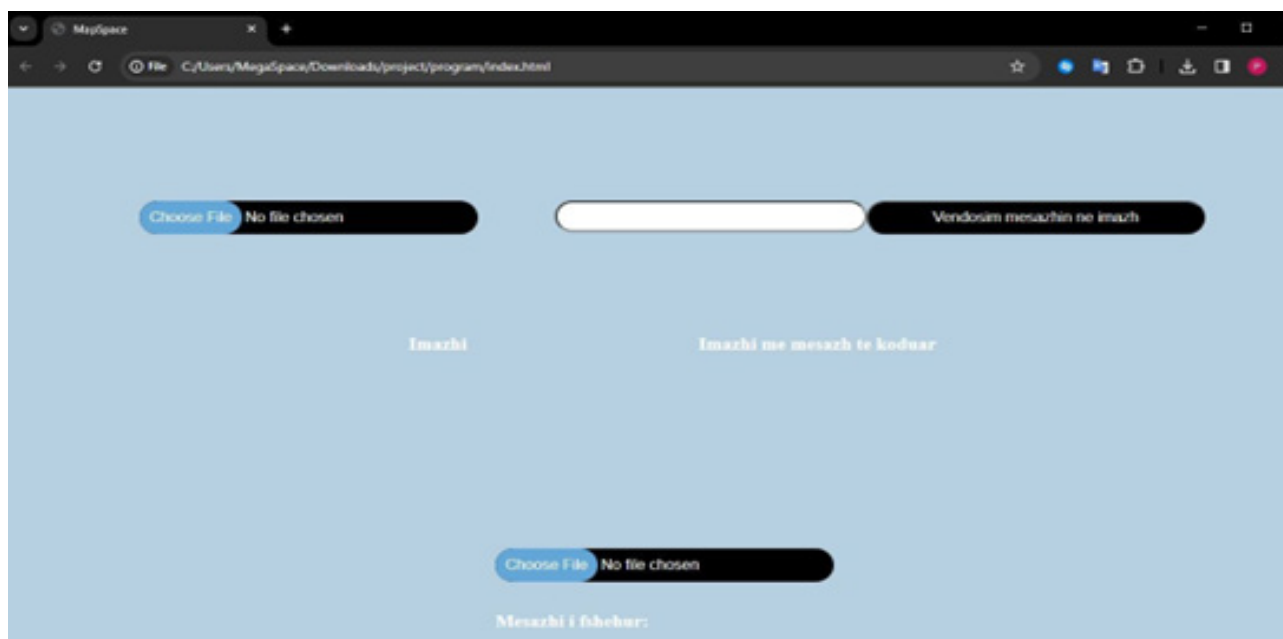


Figura 1: Paraqitja e programit

Në Choose file insertohet harta, më poshtë ku shkruhet imazhi do të shfaqet harta e thërritur. Tek butoni “Vendosim mesazhin në imazh” shkruhet mesazhi që duhet fshehur në hartë. Poshtë saj gjenerohet harta me mesazh të koduar. Pas kësaj duhet që imazhi i dytë të shkarkohet. Tek Choose file poshtë do të bëjmë të njëjtën gjë sic vepruam në fillim, insertojmë imazhin por këtë herë imazhin me mesazh të fshehtë dhe ndryshe nga hera e parë që na shfaqej harta tani na shfaqet mesazhi i fshehtë(dekodimi).

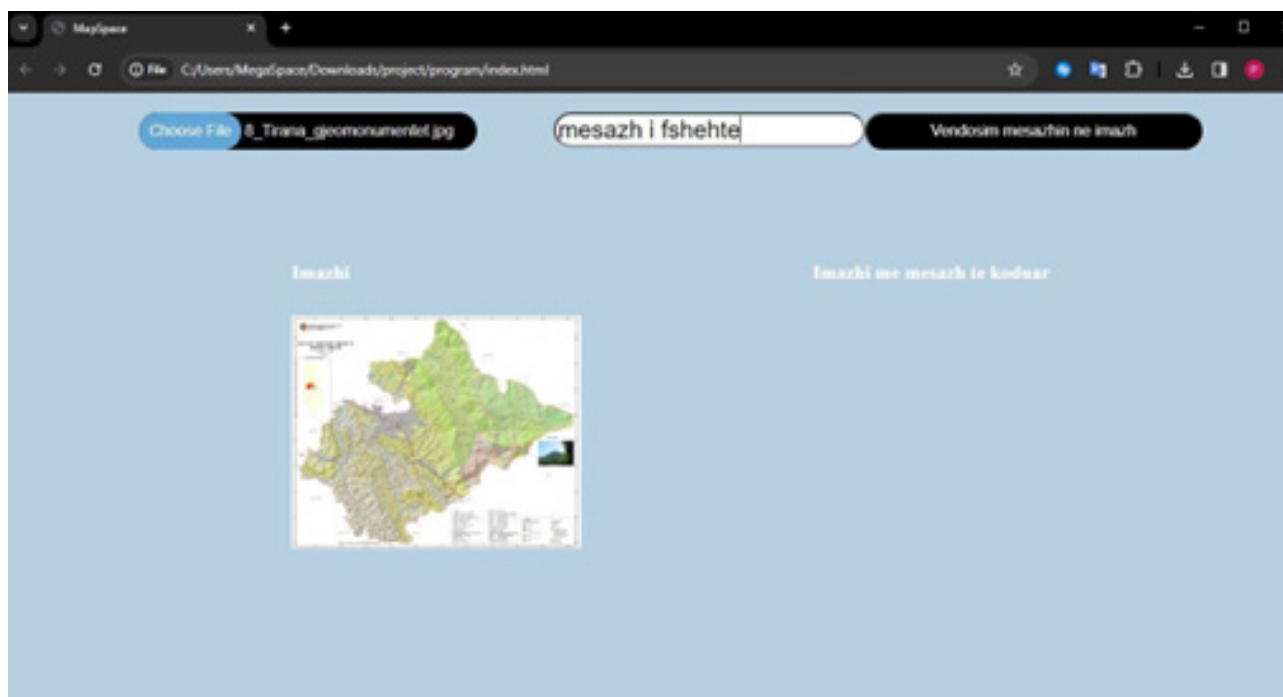


Figura 2: Marrim dhe insertojmë një hartë

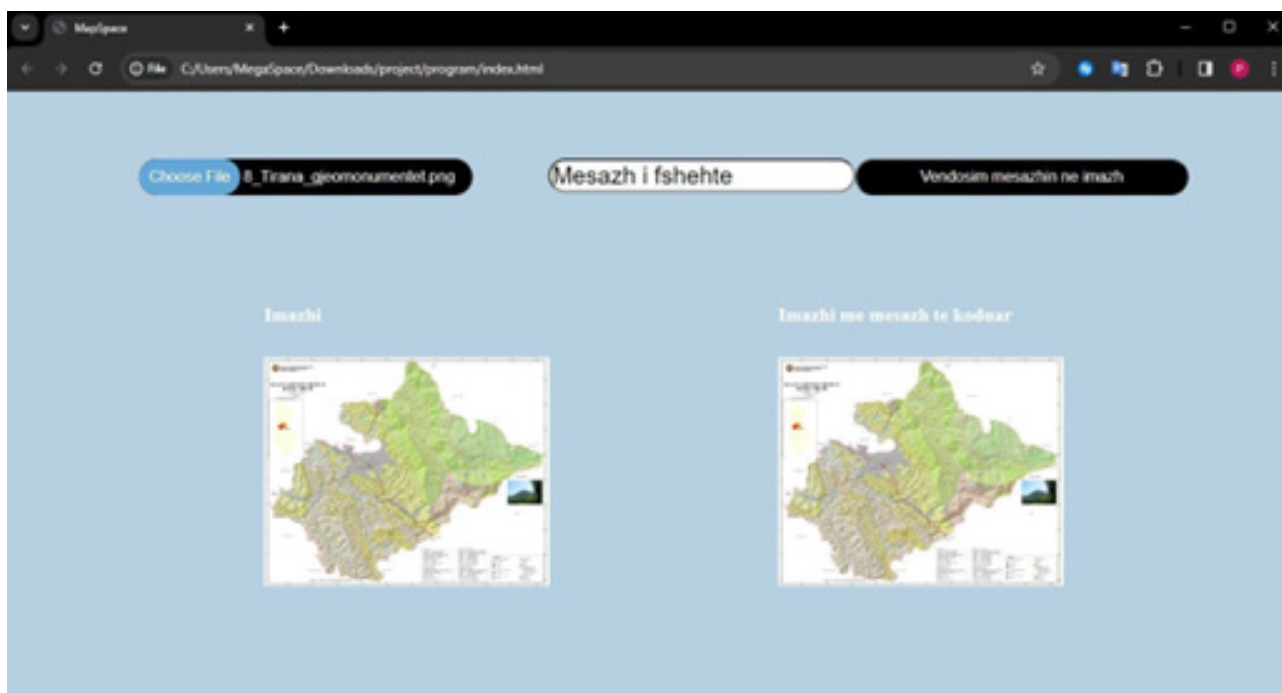


Figura 3: Shfaqja e imazhit me mesazh të koduar

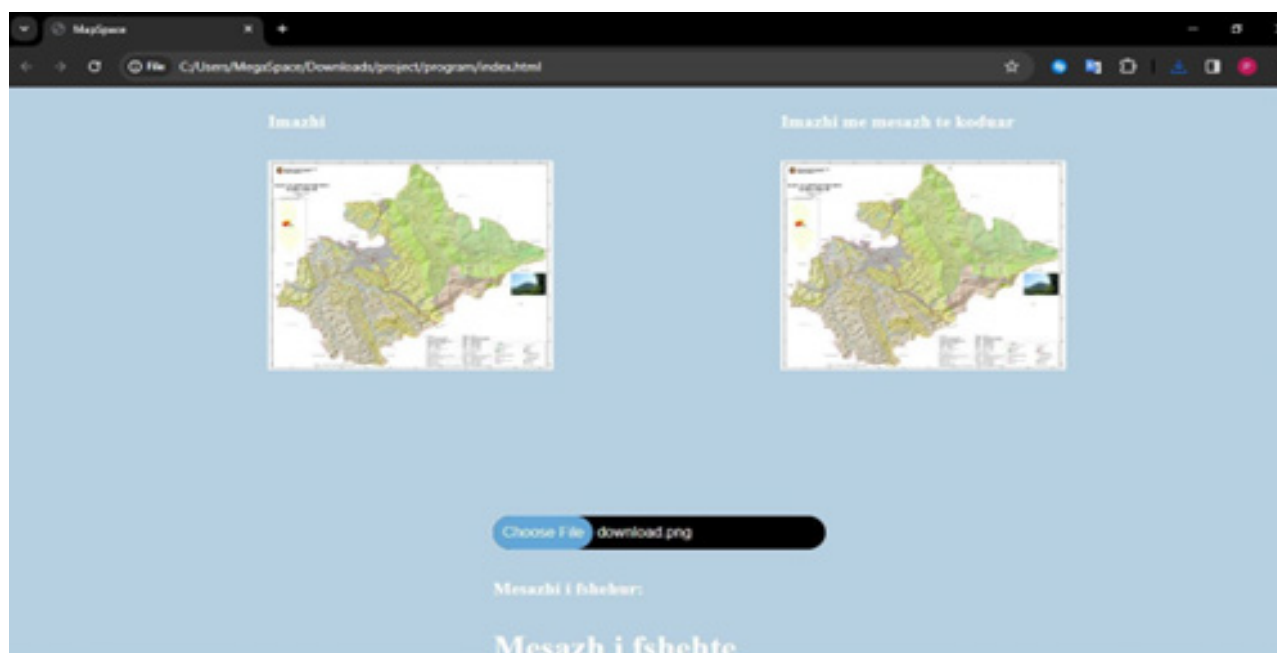


Figura 4: Insertimi dhe Shfaqja e mesazhit

8. Testime

Qellimi yne ka qene mbrojtja, menaxhimi dhe leximi i të dhënave të fshehura në hartë dhe me anë të programit të ndërtuar fshehja e informacione në hartë bëhet në mënyrë të përsosur, duke mos lënë vend për dyshime. Dihet që sa më i lartë rezolucioni i imazhit, prishja e qartësisë së hartës është e pa konsiderueshme edhe nëse ngarkesa e mesazhit është relativisht e madhe. Përkundrazi nëse rezolucioni i hartës është i ulët, qoftë edhe një e dhënë e vogël do të ndikonte drejtpërdrejtë në qartësinë e hartës. Me dy shembuj mund ta vërtetojmë lehtësisht atë që thamë më sipër.



(a)



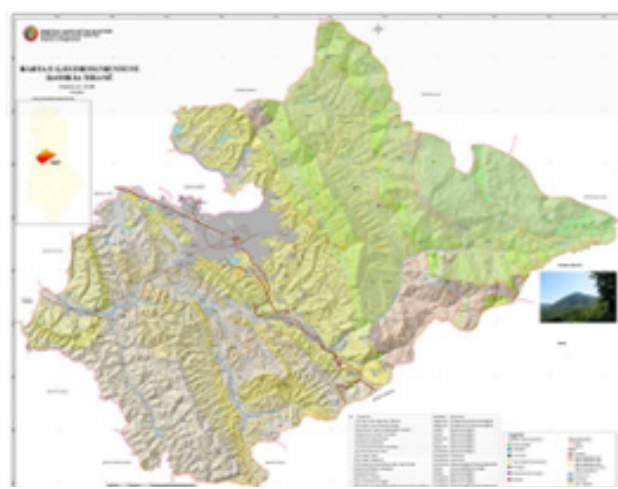
(b)

Figura 5: Harta origjinale (a), Harta me mesazh te fshehte (b)

Harta origjinale për shkak të rezolucionit të ulët që ka, do të mjaftonin shumë pak të dhëna dhe qartësia e hartës output do të ulej. Sigurisht që nuk kemi të bëjmë me një dallueshmëri të madhe por që është ekzistuese dhe që mund ta përmirësojmë mjafton të rrisim rezolucionin e hartës input dhe diferenca midis kësaj të fundit dhe hartës output do të jetë inekzistente.



(c)



(d)

Figura 6: Harta origjinale (c), Harta me mesazh te fshehte (d)

Diferenca mes dy hartave është e padukshme, kjo për shkak të rezolucionit shumë të lartë të hartës (c). Sic e përmendëm dhe më sipër rritja e rezolucionit e bën ndryshimin midis dy hartave të papërfillshëm, ky është një shëmbull që e pasqyron fare mirë këtë gjë.

9. Konkluzione dhe sfidat për të ardhmen

Në përfundim të artikullit vërejtëm se steganografia në hartë ofron një mundësi unike për mbrojtjen

e informacionit nëpërmjet fshehjes së të dhënave. Përdorimi i teknikave të avancuara si LSB+ kanë treguar se si informacioni mund të mbrohet nga sytë e paautorizuar duke ruajtur integritetin dhe privatësinë e të dhënave. Megjithatë, si çdo teknologji, steganografia përballlet me sfidat e saj, duke përfshirë rrezikun e zbulimit dhe manipulimit të të dhënave nga individë apo organizata kibernetike si dhe nevojën për mbrojtje të avancuar kundër këtyre kërcënimeve.

E rëndësishme është të merret parasysh balanca mes privatësisë dhe sigurisë, duke u përpjekur që përdorimi i steganografisë të mos shkelë të drejtat e individëve apo të përdoret për qëllime të paligjshme.

Një sfidë është rritja e ndërgjegjësimit rreth mënyrave të përdorimit të steganografisë si një mjet për mbrojtjen e të dhënave, si dhe zbatimin e politikave dhe procedurave të qarta për menaxhimin e rreziqeve të sigurisë.

Në të ardhmen, pritet që steganografia të vazhdojë të luajë një rol të rëndësishëm në mbrojtjen e të dhënave në një botë dixhitale. Propozimi i një metode të re për steganografinë e imazheve (hartë), e quajtur LSB++ [10]. Trajtimi i kësaj metode do të përmiresojë mbrojtjen e integritetit të informacionit të fshehure krahasuar me metoden LSB+.

Sfida që ngrihet është zhvillimi dhe implementimi i metodave që janë jo vetëm efektive në fshehjen e të dhënave, por që gjithashtu që mbështesin parimet e etikës dhe të drejtave të njeriut. Në këtë kontekst, bashkëpunimi ndërkombëtar dhe shkëmbimi i njohurive do të jenë thelbësorë për të përballuar sfidat e sigurisë dhe për të promovuar një përdorim të përgjegjshëm dhe të sigurt të steganografisë.

Referenca

- [1] Provos, N., & Honeyman, P. (2003, June). "Hide and seek: An introduction to steganography." *Privacy*, 1(3), 32-44.
- [2] Giarimpampa, D. (2019). Least significant bit steganography method for the digital data protection in the barcode. *AIP Conference Proceedings*, 2169(1), 040009. DOI: [DOI]
<https://pubs.aip.org/aip/acp/article/2169/1/040009/611081/Least-significant-bit-steganography-method-for-the>
- [3] Singh, A., & Kaur, A. (2019). "Spread spectrum image steganography." Retrieved from https://www.researchgate.net/publication/5583605_Spread_spectrum_image_steganography
- [4] "Blind Image Steganalytic Optimization by using Machine Learning". Halmstad 2018-08-05 Despoina Giarimpampa
<https://www.diva-portal.org/smash/get/diva2:1255395/FULLTEXT01.pdf>
- [5] "IMAGE STEGANOGRAPHY APPLICATIONS FOR SECURE COMMUNICATION" by Tayana Morkel, May 2012
<https://repository.up.ac.za/bitstream/handle/2263/29906/dissertation.pdf?sequence=1&isAllowed=y>
- [6] "Trithemius, Johannes", January 2017. DOI:10.1007/978-3-319-02848-4_570-1 In book: *Encyclopedia of Renaissance Philosophy* (pp.1-3)
https://www.researchgate.net/publication/314136305_Trithemius_Johannes
- [7] "Using Artificial Intelligence Approaches for Image Steganography: A Review". April 2020. DOI:10.1007/978-981-15-3075-3_16. In book: *Internet of Things—Applications and Future* (pp.239-247)
https://www.researchgate.net/publication/340422624_Using_Artificial_Intelligence_Approaches_for_Image_Steganography_A_Review

- [8] “Steganography Method Implementaiton in Computer Science”. November 2021
https://www.researchgate.net/publication/360671616_Steganography_Method_Implementaiton_in_Computer_Scien_ce
- [9] “Image Steganography in Cryptography”. 22 Aug, 2023 <https://www.geeksforgeeks.org/image-steganography-in-cryptography/>
- [10] “LSB++: An improvement to LSB+ steganography”. November 2011. DOI:10.1109/TEN-CON.2011.6129126 https://www.researchgate.net/publication/241634241_LSB_An_improvement_to_LSB_steganography