ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2024»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XIX Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2024»

PROCEEDINGS
of the XIX International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2024»

2024
Астана

УДК 001
ББК 72
G99

«ǴYLYM JÁNE BILIM – 2024» студенттер мен жас ғалымдардың XIX Халықаралық ғылыми конференциясы = XIX Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2024» = The XIX International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2024». – Астана: – 7478 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-7697-07-5

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов имолодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001
ББК 72
G99

ISBN 978-601-7697-07-5

меңгеру студенттер мен мамандарға жаңа мүмкіндіктер ашады және оларға еңбек нарығында бәсекелестік артықшылық береді.

Қолданылған әдебиеттер тізімі.

1. Таненбаум Э. Компьютерные сети. 4-е изд. – СПб.: Питер, 2006.- 992 с.
2. http://www.intuit.ru/studies/courses/8/8/lecture/126.
3. https://www.ps.kz/hosting/vpc?ad=57&gad_source=1&gclid=EAIaIQobChMIt9by9rmVhQMV6GWRBR16cAEhEAAYASAAEgK20fD_BwE.
4. Пелевин И.И., Маликова Е.Е. Разработка лабораторного практикума по изучению виртуальной телефонной станции IP-АТС Asterisk // Телекоммуникационные и информационные технологии, №2, 2018. С. 38-42.
5. https://www.3cx.ru/docs/manual/phonebook/.
6. Дэвидсон Д. и др. Основы передачи голосовых данных по сетям IP. Cisco Press. М.:Вильямс, 2007 - 400с.

УДК 004.056

СТЕГАНОГРАФИЯ КӨМЕГІМЕН «ҚҰПИЯ ЖАЗУ» ТУРАЛЫ

Серік Арсен Берікұлы[1], Алиева Гулжайна[2]

arsen4ik404@gmail.com

[1]Л.Н.Гумилев атындағы ЕҰУ Радиотехника, электроника және телекоммуникация кафедрасының студенті, Астана, Қазақстан

[2]Л.Н.Гумилев атындағы ЕҰУ Радиотехника, электроника және телекоммуникация кафедрасының инженері, Астана, Қазақстан

Ғылыми жетекшісі – Н. А. Бурамбаева

Ақпараттық технологияның дамуы соңғы он- он жарым жылдағы жаңалықтар өте көп. Жасай келе әр саланың маңызды (және ең маңызды) ақпараты, кәсіпорындар немесе ұйымдар қызметінің аспектілерін реттеулер, электронды түрде деректерді сақтау жүйелері тұтастығымен құпиялығын сақтау цифрлық жахандандыру негізгі бөлігі болып табылады. Ақпараттың бөгде тұлғалардың қолына түспеуі.

Сондықтан ерекше өткірлік ресурстадың сенімді қорғау мәселесі, сондай-ақ рұқсат етілмеген тұлғалардың мәтіндік құжаттар, бағдарламалық кодтар, деректер қорына қол сұқпау қадағалау. Мәліметтерді тасымалдаумен байланысты қауіпсіздік мәселелерінің негізгі шешімі деректерді шифрлауды қолдану болып табылады, оның ішінде симметриялы және асимметриялық криптографиялық шифрлау, онда деректер шифрлау кілті арқылы шифрленген мәтінге түрленеді. Содан кейін алушы бастапқы ашық мәтінді алу үшін шифрды шешу кілтін пайдаланып хабарламаның шифрын шеше алады.

Деректерді шифрлау құпия ақпаратты қорғаудың тиімді әдісі болғанымен, шифрланған деректер көбінесе түсініксіз және сыртқы түрі күдікті болып келеді, бұл қосымша тексеруге әкеледі. Нәтижесінде жасыруды қамтитын стеганография деп аталатын тағы бір зерттеу тақырыбы пайда болды сурет, бейне және мәтін жағдайында олар статистикалық түрде анықталмайтын және адам көзіне көрінбейтін етіп деректер тасымалдау, сондай-ақ аудио тасымалдаушылар жағдайында адамның есту жүйесіне сезілмейтіндей жасыру.

Бұл тәсіл күдік тудырмай немесе қажетсіз назар аудартпай деректерді қауіпсіз тасымалдауға мүмкіндік береді. Қазіргі уақытқа дейін деректерді қорғау толығымен шешілмеген тақырып және деректерді қорғауды жүзеге асырудың бір түрі – стеганография болып табылады.

Стеганография сөзбе-сөз "құпия жазу"-ды білдіреді. Ақпаратты қорғау әдістерінің бірі ретінде, оны әртүрлі салаларда қолдануға болады. Компьютерлік жүйелердің пайда болуы, Интернеттің дамуы және компьютерлік технологияны кеңінен қолдану цифрлық стеганография әдістерінің пайда болуына әкелді. Жасырын жіберу және жіберілген деректерді қорғау.

Стеганографияның дамуына серпін берген криптографияның мемлекеттер тарапынан шектеулер қойылуы: мысалы, шифрлау жүйесінде қолданыста жүрген “кілт- сөздер” мемлекетке тапсыру. Міндетті түрде тіркеу және олар аппараттық немесе басғдарламалық орта болғанына қарамастан, криптографиялық жүйелерді лицензиялау керек. Стеганография бұл реттілік қажет етпейді, және ақпаратты жасырудың тиімді тәсіл болып табылады.

Стеганография әдістері хабарламаларды жасырын жібер үшін ғана қолданылмайды, сонымен қатар авторлық немесе мүліктік құқықтарын фотосуреттер немесе басқа цифрланған өнер туындыларын қорғау үшін қолданылады. Ақпараттың ұрлануы, авторлық мағұлматтардың өзгертілуі интернет желісінде өте оңай және кен таралған. Деректерді қорғаудың бірден- бір түрі – цифрлық су белгелері.

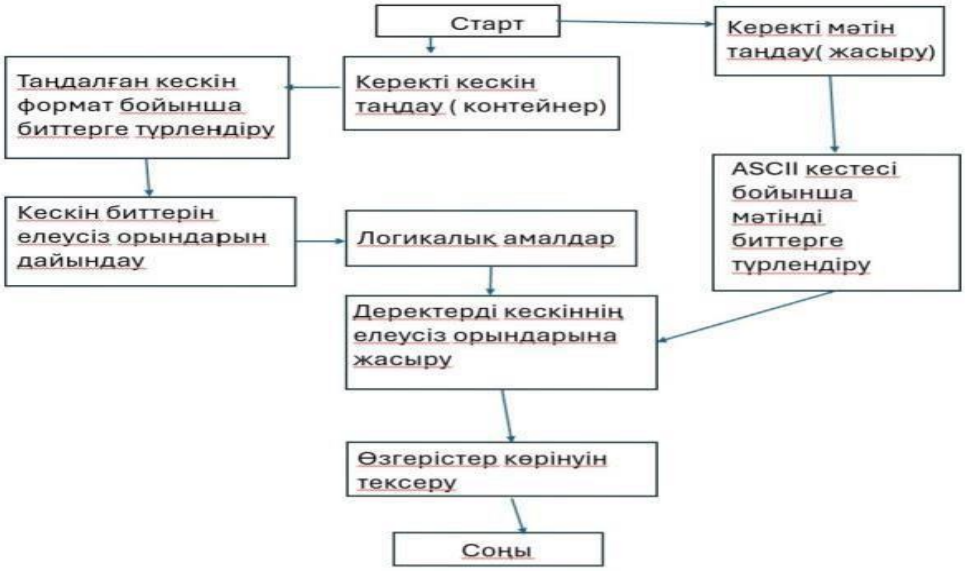
Цифрлық су белгілері деректер туралы көп ақпарат алуға болады: мысалға, файл қай уақытта жасағаны, авторлық құқық кімде екенін, автормен қала байланысқа шығу және т.б ақпаратты ұстай алады. Барлық енгізілген ақпарат сот алдында авторлық немесе дәлелдеу кезінде салмақты рөл атқарады.

Мысалы, ең қарапайым ақ-қара суретте әрбір пикселдің жарықтығын бір байтпен сипаттайды: нөл – қара, 255 - ақ, қалғанының бәрі - сұр түсті сипаттайды. Егер сіз файлдың кез келген байтын немесе жеке орналасқан байттарын өзгерткіңіз келсе, онда сәйкес келген пискел жарықтылығы өзгертеді. Сонымен қатар, писел битің өзгерту пикселдің түсің және жарығын өзгертеді: бірінші биті пикселді тұтас өзгертсе, екінші биті жартылай өзгертеді, ал сегізінші биті адамдың көру қабылеты басқамайтындай өзгерістертеді. Осы белгілерге сүйене отырып пикселдің сонгы биттарын өзгерте отырып деректерді жасырып, кескіндеріміздің бастапқы күйінен ауытқымауын қамтамасыз ете аламыз – сурет бірдей болып көрінеді. Бұл стеганографиялық әдістің аты LSB (Least Significant Bit). LSB әдісінің алгоритмдік түсіндірмесі келесідей:

Сурет пен деректерді таңдау: деректер жасырылатын кескінді және жасырылатын деректерді таңдаңыз. Деректер мәтін, басқа сурет немесе кез келген басқа деректер болуы мүмкін.

1. Деректерді түрлендіру: жасырғыңыз келетін деректерді биттер тізбегіне түрлендіру. Мәтін үшін бұл таңбаларды биттік реттілікке кодтау, ал кескіндер үшін пикселдерді биттерге түрлендіру болуы мүмкін.
2. Кескінді дайындау: Деректер жасырылатын кескіннің ажыратымдылығы мен сапасы жеткілікті жоғары екеніне көз жеткізіңіз, осылайша өзгерістер байқалмайды.
3. Деректерді жасыру: кескіннің әрбір пикселін аралаңыз. Жасырғыңыз келетін деректердің әрбір биті үшін сол пикселдің түсті арна мәнінің ең аз маңызды битін (әдетте қызыл, жасыл немесе көк) сәйкес деректер битімен ауыстырыңыз.
4. Өзгерістердің көрінуін тексеру: Суреттегі өзгерістер көзге көрінбейтініне көз жеткізіңіз. Мұны суретке қарау немесе кескінді талдау әдістерін қолдану арқылы жасауға болады.
5. Save Image: өзгертілген кескінді сақтаңыз.
6. Деректерді шығару: Жасырын деректерді шығару үшін суреттегі әрбір пиксель арқылы өтіп, әр түс арнасының ең аз маңызды биттерін шығарып алыңыз. Шығарылған бит тізбегін бастапқы деректерге қайтарыңыз.
7. Деректерді декодтау: Шығарылған деректерді бастапқы пішіміне қайтарыңыз (қажет болса).
9.

LSB алгоритм келесідей көрсетуге болады,



Сурет 1- LSB стеганографиялық әдісінің алгоритмдік түсіндірмесі

Негізгі анықтамалар

Стеганографияны 3 бөлімге бөлуге болады:

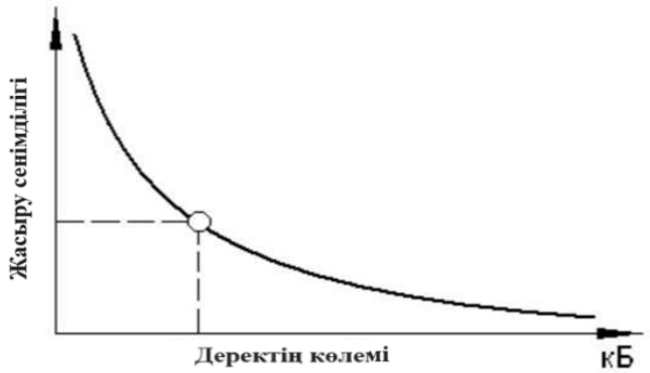
классикалық стеганография – барлық «компьютерлік емес әдістері».

- Компьютерлік стеганография классикалық стеганографияның бағыты, компьютерлік платформаның сипаттамаларына негізделген.
- цифрлық стеганография – классикалық стеганографияның бағыты;
- Ең үлкен қызығушылық сандық стеганография. Қызығушылық ақпаратты қорғау тұрғысынан ең перспективалы болып табылады.
- Стеганографияның негізгі ережелері:
- Жасыру әдістері шынайылық пен тұтастықты қамтамасыз етуі керек
- Әдістердің қауіпсіздігі стеганографияның сақталуына негізделген, жасырыға арналған ақпаратты жасырын кілт арқылы сақталуын қамтамасыз ету.
- Хабарды жасыру фактісі жауға белгілі болса да құнды мәліметтер шығарып алу қиын процесс болуы маңызды

Әдетте, стеганографиялық алгоритмдерді құру кезінде ең үлкен зерттеу көлемі құпиялылықты қамтамасыз етумен ерекше байланысты. Өндірілген бір немесе бірнеше бөліктің қалай өзгеретінін анықтауға арналған эксперименттер контейнер файлы алынған кескінге әсер етеді.

Стеганографиялық төзімділік алгоритм ендірілген хабардың өлшемі анықталады. Хабарлама өлшемін ендіру цифрлық кескінді сақтауды пайдалану тиімділігі құпия ақпарат негізінен максимуммен анықталады.

Әдетте, сандық түрде бұл критерий көлем арасындағы пайыздық қатынаспен, ендірілген хабарлама және бастапқы контейнер көлемі мен сипатталады. Алдын ала анықталған хабарлама контейнеріне ендірілген болса, сенімділік соғұрлым төмен болады



Сурет 2 – Ақпаратты жасыру сенімділігінің ақпараттың көлеміне тәуелділігі

Стеганография ақпаратты жасырын беру әдісі ретінде киберқауіпсіздік, барлау және деректерді қорғау салаларында маңызды рөл атқарады. LSB (Least Significant Bit) – адамның қабылдауында байқалатын өзгерістерді барынша азайта отырып, жасырын деректерді цифрлық медианың кескіндер немесе аудио файлдар сияқты төменгі ретті биттеріне енгізуге мүмкіндік беретін ең көп қолданылатын стеганография әдістерінің бірі.

Дегенмен, жасырын хабарламаларды талдау және анықтау әдістерінің дамуымен, соның ішінде машиналық оқытуды және цифрлық сигналды өңдеуді қолдану арқылы берілетін ақпараттың құпиялығын сақтау қиындай түсуде. Бұл стеганография әдістерін үздіксіз дамыту және жетілдіру, сондай-ақ деректерді қорғау үшін күшті шифрлау алгоритмдерін құру қажеттілігін көрсетеді.

Дегенмен, стеганография ақпараттың құпиялылығы мен қауіпсіздігін қамтамасыз етудің маңызды құралы болып қала береді, әсіресе үнемі өзгеретін киберқауіпті ортада. Оны тиімді пайдалану тек техникалық білімді ғана емес, сонымен қатар әдістеме қолданылатын әлеуметтік және мәдени контексттерді түсінуді талап етеді.

Қолданылған әдебиеттер тізімі

1. Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая Стеганография. - М.:Солон-Пресс, 2002 - 272 с
2. D. Volkhonskiy, I. Nazarov, B. Borisenko, and E. Burnaev. Steganographic generative adversarial networks. arXiv preprint arXiv:1703.05502, 2017.
3. Кувшинов С. С. Методы и алгоритмы сокрытия больших объемов данных на основе стеганографии: дис. … канд. тех. наук: 05.13.19. – СПб.: НИУИТМО, 2010. – 116 с
4. Урбанович П. П. Защита информации методами криптографии, стеганографии и обфускации. Минск: БГТУ, 2016. 220 с.