**Алимжанова Жанна Муратбековна** – кандидат физико-математических наук,

Казахский национальный университет имени Аль-Фараби

**Аяшова Айзада Мақсұтқызы**- магистрант,

Казахский национальный университет имени Аль-Фараби

**Криптография және стеганография алгоритмдерін қолдана отырып, шифрлаудың және декодтаудың жаңа тәсілдері**

***Аңдатпа.*** *Бұл мақалада желілік ортада деректердің қауіпсіздігін арттыру үшін аффинді шифрлау алгоритмі бар Hash Least Significant bit (H-LSB) алгоритмі ұсынылды.*

***Аннотация****.В этой статье был предложен алгоритм Hash Least Significant Bit (H-LSB) с алгоритмом аффинного шифрования для обеспечения большей безопасности данных в сетевой среде.*

***Түйін сөздер:*** Криптография, стеганография, құпия хабарлама, хэш негізіндегі LSB, аффинді шифр, шифрлау процесі, дешифрлау.

***Кіріспе.*** Қазіргі уақытта желі деректерді көзден тағайындалған жерге дәл және жылдам жеткізуде маңызды рөл атқарады. Деректер құпиялылықтың жоғары деңгейімен беру үшін жеткілікті қауіпсіз емес. Ақпараттық қауіпсіздік компьютерлік желі арқылы деректерді беру кезінде ресурстарды бөлісудің негізгі мәселелерінің бірі болады. Криптография және стеганография - ашық арна желісі арқылы беру кезінде деректерді зиянкестерден қорғаудың екі әдісі болып табылады. Криптография - бұл деректерді шифрлау әдісі, ал стеганография - мұқабадағы құпия хабарламаны жасырудың өнері мен ғылымы.

Алдымен біз деректерді жаңа криптографиялық алгоритммен шифрлаймыз, содан кейін кескінге енгіземіз. Құпия хабарламаның сегіз биті 3, 3, 2 болып бөлінеді және сәйкесінше мұқабаның RGB пиксель мәндеріне енеді. LSB биттеріндегі кірістірудің нақты орнын таңдау үшін хэш функциясы қолданылады. Бұл жүйе хабарлама жіберушіге кескінге енгізбестен бұрын құпия хабарламаны шифрлау кілттерін таңдауға мүмкіндік береді, ал алушы хабарламаны шифрлау үшін кілттерді пайдаланады. Алушы шифрланған хабарламаны дұрыс емес кілттермен, бірақ бастапқы хабарламадан басқа нысанда шеше алады. Бұл жүйе құпия хабарламаны желілік ортада бір ұшынан екінші ұшына беру кезінде қауіпсіздікті жақсартуға қабілетті.

Телекоммуникация саласы өскен сайын желілер арқылы желілік сандық суреттердің әртүрлі түрлері беріледі. Қазіргі әлемнің әр дамып келе жатқан саласының негізгі қажеттілігі - байланыс. Барлығы ақпараттың құпия және қауіпсіз болуын қалайды. Интернеттің өсуі, ақпараттық технологиялар мен коммуникацияның маңызды факторлары ақпараттың қауіпсіздігі болады [1].

Күнделікті өмірде біз телефон арқылы немесе интернет арқылы ақпарат алмасу және беру үшін көптеген қауіпті жолдарды қолданамыз. Алайда, белгілі бір деңгейде бұл қауіпті. Криптография және стеганография - бұл ақпаратты өз өмірін шифрлау немесе жасыру үшін пайдаланатын екі әдіс. Оларды ақпаратты жасырын түрде бөлісу және беру үшін пайдалануға болады. Криптография - бұл байланыс құпиялығын қамтамасыз ету үшін хабарламаны өзгертуді қамтитын әдіс [2]. Қазіргі уақытта хабарлама құпиясын қорғау үшін деректерді шифрлау және дешифрлау үшін көптеген түрлі әдістер қолданылады.

Криптография. Криптографияда аралық тұлғаға хабарлама тек жіберуші мен алушыға белгілі шифрлау кілтімен шифрланғаны туралы түсінікті. Шифрлау кілтін пайдаланбай хабарламаға қол жеткізу мүмкін емес. Алайда, бұл әдістер хабарлама құпиясының мазмұнын қорғау үшін жеткіліксіз. Өйткені криптографияда стеганография деп аталатын басқа әдіс қолданылады [3].

Стеганография - бұл хабарламаны көрінбейтін түрде беру өнері мен ғылымы, ал құпия хабарлама оны мұқабада жасыру үшін жасалады және адам суретте жасырылған хабарламаны көре алмайды [4]. Мұқабаның құпия деректері бар суреті содан кейін алушыға беріледі. Алушы хабарламаны қабылдау процесі және жіберуші ұсынған құпия кілт арқылы ала алады.

Криптография - бұл хабарламаны рұқсат етілмеген пайдаланушылардың хабарламаларға қол жеткізуінен қорғау үшін құпия хабарламаларды кодтау және декодтау механизмі. Желілік ортада криптография жұмыс істейтін қосымшаларда деректерді қорғауда үлкен рөл атқарады. Грек тілінде криптография "жасырын құпия" дегенді білдіреді. Сонымен қатар, бұрын криптографияны барлау және қарулы күштердің саяси секторы қолданған. Ал қазіргі уақытта ол банкомат карталарында, электрондық коммерцияда, электрондық пошталарда, компьютерлік парольдерде және басқа қосымшаларда жиі қолданылады. Осы жылдар ішінде хабарламаны жіберуші мен алушыға белгілі шифрлау кілтімен өзгерту үшін әртүрлі алгоритмдер пайда болады [4].

Хабарламаны шифрлау кілтін пайдаланбай шифрлау мүмкін емес. Криптографиядан туындайтын мәселелердің бірі - бұл хабарлама әрдайым арадағы адамға түсінікті, өткені бұл хабарлама шифрланған. Бұл хабарлама жіберушінің бөтен адамның оқығанын қаламайтынын білдіреді. Бүгінгі таңда деректерді шифрлай алатын криптографияның көптеген әдістері бар. Ең көп таралған әдістердің бірі-аффиндік алгоритм. Аффиндік алгоритм ақпаратты шабуылдаушы үшін түсініксіз пішінге айналдыра алады.

Стеганография. Қазіргі уақытта пайдаланушылар арасында сандық кескінді бөлісу үшін әртүрлі желілер қолданылады. Компьютерлік желілердің түрлерінің көбеюімен сандық мәліметтердің үлкен көлемі желі арқылы жеткізіледі. Өйткені олардың көпшілігі құпия, жеке немесе екеуі де болуы мүмкін. Бұл деректерді зиянкестерден қорғау үшін шифрлаудың сенімді әдістеріне қажеттілік артады [5].

Стеганография - құпия хабарламаны кескінге енгізу үшін қолданылатын маңызды әдістердің бірі [6]. Бұл әдіс қолданушыға кескін ішіндегі ақпаратты жасыруға мүмкіндік беретін тамаша шифрлау қосымшасы болып табылады. Стеганография әдістері криптография арқылы құпия хабарламаны қосымша қорғауды қамтамасыз ете алады, осылайша ақпарат екі есе қорғалады [7].

Стеганография кескіннің ішіндегі ақпаратты жасырады, сондықтан кескіннің ішінде ешқандай ақпарат жасырмайтын сияқты болып тұрады. Осылайша, пайдаланушылар құпия ақпаратты қорғалмаған арна арқылы, мысалы, Интернет арқылы жібере алады. Стеганографияның әртүрлі әдістері қолданылады. Бұл мақалада біз кескінге құпия хабарламаны енгізу үшін ең аз маңызды бит (LSB) әдісін қолдандық.

**Шифрлау.** Бірінші кезеңде деректер жүйесіне кіру үшін пайдаланушыларға пайдаланушы аты мен пароль қажет. Жүйеге кіргеннен кейін пайдаланушы құпия кілттермен деректерді шифрлау үшін хабарлама жаза алады. Біздің жүйеде құпия ақпаратты шифрлау үшін Афина алгоритмін қолданамыз. Афина алгоритмі - деректерді шифрлау үшін қолданылатын алгоритмдердің бірі. Бұл процесте алфавиттегі әр әріп оның сандық эквивалентімен салыстырылады, математикалық функцияны қолдана отырып шифрланады және қайтадан әріпке айналады. Пайдаланылған формула әр әріп бір әріпке және артқа шифрланғанын білдіреді. Яғни шифр дегеніміз - бұл стандартты ауыстыру шифры, ол қай әріпке қалай жүретінін анықтайды.

Бұл әдіс деректерді пайдаланушыны желі арқылы рұқсатсыз кіруден қорғау үшін қауіпсіздікті қамтамасыз етеді. Сондықтан деректерді алушының кілтінсіз алу оңай болмайды. Қарапайым мәтінді шифрланған мәтінге айналдырғаннан кейін афина алгоритмнің көмегімен біз жоғары қауіпсіздікті қамтамасыз ету үшін шифр мәтінін алып, әр әріпті екілік кодтарға айналдырдық. Бұл ұсынылған әдіс шабуылдаушылардың оларды алуға тырысқанда нақты деректерді алуына жол бермеу үшін қолданылады. Бұл шифрланған деректер бастапқы кескіннің нөлдік бұрмалануымен кескінге енеді.

Мысалы:

Мәтін: Казахстан

Шифрланған мәтін: мигиузких

Бұл жерде әріптер А әрпінен Я әрпіне дейін алынған.

Шифрланатын ашық мәтінмен «Казахстан» алынды. Әр әріптің сандық мәндері үшін және әр әріпті шифрлау үшін келесі функция қолданылды:

***E(x) = (ax + b) mod m***(1)

мұндағы:

x: ашық мәтіндегі әріптің сандық мәні.

m: ашық мәтін әліпбиіндегі әріптер саны.

a және b - жіберуші мен алушы арасындағы құпия сандар.

E (x): түрлендіру нәтижесі.

Кесте 1 - X мәнін анықтау

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| мәтін | K | а | з | а | х | с | т | а | н |
| X | 11 | 1 | 8 | 1 | 22 | 18 | 19 | 1 | 14 |

Енді әр x мәнін алып, теңдеудің бірінші бөлігін орындаймыз (3x + 6). Әр таңба үшін (3x + 6) мәнін тапқаннан кейін нәтижені (3x + 6) 26-ға бөлген кезде қалдықты аламыз. Келесі кестеде шифрлау процесінің алғашқы төрт қадамы көрсетілген:

Кесте 2 – Мәтінді шифрлау

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| мәтін | K | а | з | а | х | с | т | а | н |
| X | 11 | 1 | 8 | 1 | 22 | 18 | 19 | 1 | 14 |
| (3x + 6) | 39 | 9 | 30 | 9 | 72 | 60 | 63 | 9 | 48 |
| (3x + 6)mod26 | 13 | 9 | 4 | 9 | 20 | 8 | 11 | 9 | 22 |
| Шифрленген мәтін | м | и | г | и | у | з | к | и | х |

Сандарды екілік түрінде көрсету үшін 6 екілік бит қажет, өйткені орыс алфавитінде 33 әріп қолданылады. Сондықтан бастапқы мәтін келесідей болады: 001101, 001001, 000100, 001001, 010100, 001000, 001011, 001001, 010110

Құпия хабарламаны шифрлағаннан кейін шифрланған хабарламаны кескінге ендіру әдісін қолдануға болады. Бұл процесс кіші мәнді битті алмастыратын хэш негізіндегі ең аз мәнді битті (HLSB) қолдану арқылы жүзеге асырылады. LSB-деректерді кескін файлына ендірудің ең танымал стеганография әдісі. Бұл әдіс суреттегі шифрланған хабарламаны жасыру үшін қолданылады, содан кейін суретті алушыға жібереді. Бірінші кезеңде біздің жүйеде пайдаланушылар логин мен парольді алу үшін тіркелгі жасауы керек. Тіркелгенде пайдаланушылар барлық өрістерді толтыруы керек.

Құпия хабарламаны шифрлағаннан кейін шифрланған хабарламаны кескінге ендіру әдісін қолдануға болады. Бұл процесс кіші мәнді битті алмастыратын хэш негізіндегі ең аз мәнді битті (HLSB) қолдану арқылы жүзеге асырылады. LSB-деректерді кескін файлына ендірудің ең танымал стеганография әдісі. Бұл әдіс суреттегі шифрланған хабарламаны жасыру үшін қолданылады, содан кейін суретті алушыға жібереді. Бірінші кезеңде біздің жүйеде пайдаланушылар логин мен парольді алу үшін тіркелуге жазылу керек. Жүйеге тіркелгеннен соң, пайдаланушылар 1-суретте көрсетілгендей кіру үшін логин мен парольді қолдана алады.



Сурет 1- Жүйеге кіру

Жүйеге кіргеннен кейін жүйелік пайдаланушылар екі қойындыны көре алады: біреуі - шифрлау деректерін кескінге шифрлау және ендіру үшін "деректерді кодтау", екіншісі - кескін ішіндегі деректерді шығару үшін "деректерді декодтау". Кескін туралы ақпарат, мысалы: сөздердің саны, кескіннің ішінде кодтауға болатын максималды өлшем. Суреттің өлшемі, биіктігі мен ені жоғарғы оң жақ панельде көрсетіледі. Сонымен қатар, кодтау қойындысындағы жоғарғы жолақта бізде бір мәтін өрісі бар. Ал батырма кескінді компьютердегі кез-келген жерден жүктеу үшін қолданылады.

Файлды ашудағы диалог терезесі келесідей көрсетіледі: пайдаланушы құпия суретті жасыру үшін кескін файлын таңдап, 2-суретте көрсетілгендей "ашу" түймесін басуы керек.



Сурет 2 - Суретті таңдау

Кодтау қойындысында үш мәтін өрісі бар: біріншісі - пайдаланушылар кескінде кодтағысы келетін құпия хабарлама жазуға арналған құпия хабарлама, екіншісі - хабарламаны шифрлау. Бұл мәтін өрісінде пайдаланушы шифрланған хабарламаны тікелей көре алады. Ал үшінші мәтін өрісі кескінді енгізбестен бұрын түрлендірілген шифрланған хабарламаны ASCII кодына көрсету үшін қолданылады.

Сонымен қатар, шифрланған хабарламаны кескін ішінде жасыру және қауіпсіздік үшін пароль қажет. Тексеру үшін парольді екі рет енгізу керек. Пайдаланушының паролі үшін алты таңбаны пайдалану керек. Бұл деректер паролі кескінге де енеді. Құпия хабарламаны шифрлау үшін пайдаланушыларға Affine cipher key таңдау керек.

Шифрланған деректерді енгізгеннен кейін пайдаланушылар 3-суретте көрсетілгендей шифрланған деректердің сәтті енгізілгеніне көз жеткізу үшін хабарлама терезесін алады.



Сурет 3 - Деректерді ендіру

Шифрланған деректерді сәтті енгізгеннен кейін жаңа stego\_image дерекқорда сақталады. Сонымен қатар, пайдаланушылар stego\_image-ді тікелей Интернет арқылы немесе мақсатты пайдаланушыларға электрондық пошта арқылы кескіннің ішіндегі құпия деректерді ашпай-ақ жібере алады. Бұл жүйеде деректерді шифрлау немесе алу үшін екінші қойынды қолданылады. Бұл қойынды жолағы екі мәтін өрісінен, кескін көрінісінен, екі тізім өрісінен және түймелерден тұрады. Алушы дерекқордан суретті сұрау үшін пароль енгізу үшін бірінші мәтін өрісін пайдаланады.

Дұрыс парольді енгізіп, "суретті қайтару" түймесін басқаннан кейін, кескін шифрлау жолағына бірден оралады. Бірақ алушылар a = 3 және b = 6 сияқты екі тізім өрісі арқылы аффиндік шифрлау кілттері дұрыс таңдалғанға дейін кескінге енгізілген деректерді шығарып, шеше алмайды. Бұл деректердің тұтастығы мен құпиялылығын қамтамасыз ету үшін қажет. Қате құпия кілтті кез-келген таңдау арқылы алушы мағынасыз хабарламаны қайтарады. Бұл желілік ортадағы зиянкестерге қарсы деректердің қауіпсіздігіне кепілдік береді.

Бұл мақалада көп деңгейлі қауіпсіздік әдістерін қолдана отырып, деректерді зиянкестерден қорғаудың жақсы қауіпсіздігін қамтамасыз ету үшін криптография және стеганография әдістері ұсынылған. Осы екі әдістің үйлесімі пайдаланушылар ашық арна арқылы деректерді беру кезінде басқалардан қорғағысы келетін кейбір маңызды деректердің арқасында деректерді енгізу қауіпсіздігін арттырады.

Бұл процестің басында шифрланған хабарлама алынады, ол мұқабаның кескініне енеді. Кез-келген шабуылдаушыға оны алушының жеке кілтінсіз шифрлау қиын болады. Содан кейін хэш функциясы позицияларды таңдау үшін қолданылады және ұсынылған әдіс сегіз бит алынады, құпия деректер сәйкесінше 3, 3, 2 ретпен LSB пиксель мәндеріне (қызыл, жасыл және көк) енеді. Әдістерге сәйкес, кескінге құпия деректерді енгізу үшін қызыл пиксельдің LSB-ге үш бит, жасыл пиксельге үш бит және көк пикселдердің LSB-ге 2 бит біріктірілген.

Бұл сегіз бит келесі ретпен енгізілген, өйткені көк түстің адам көзіне хроматикалық әсері қызыл және жасыл түстерге қарағанда үлкен. Сондықтан үлестіру үлгісі көк пиксельде жасырылатын 2 битті таңдайды. Осылайша, сурет сапасы жойылмайды. Бұл процесс барлық биттік хабарлама мұқаба кескініне енгенге дейін жалғасады. Әрбір RGB мұқаба кескінінің LSB-де деректерді жасыру позициясын анықтау үшін келесі формула қолданылады:

 ***K= p % n ………. (1)*** (2)

мұндағы K – пиксельдегі кіші бит позициясы, P – жасырын кескіндегі әр пиксельдің орны, ал n - LSB бит саны, біздің жағдайда ол - 4.





Сурет 4 (a) және (b). RGB пиксель мәнінің кіші екілік разрядын табу үшін хэштеу процесі

**ҚОРЫТЫНДЫ**

Бұл мақалада желілік ортада деректердің қауіпсіздігін қамтамасыз ету үшін криптография және стеганография әдістері ұсынылған. Біз ұсынатын жүйенің көмегімен деректерді жіберуші мен алушы арасында қорғалмаған желілік орта арқылы жіберуге болады. Желілік ортада бұл жүйе шабуылдаушылардан хабарлама құпиясын жасырудың ең жақсы тәсілдерінің бірі екені анық.

Мақалада қауіпсіздіктің қосымша функциялары бар жүйені дамытуға баса назар аударылады. Криптография әдісі, яғни аффиндік шифрлау алгоритмі құпия хабарламаны шифрлау үшін жүзеге асырылды және екілік кодқа түрленді. Сондықтан шабуылдаушыға кілтсіз және парольсіз шифрлауды бұзу оңай болмады.

**Қолданылған әдебиеттер**

1. Р. Пурнима и Исвария Р.Дж. «Обзор стеганографии цифровых изображений». Международный журнал компьютерных наук и инженерии 4.1 (2013): 23-31.

2. А. Анагоу и В. Шринивасарао. Модифицированный метод шифрования RSA на основе нескольких открытых ключей. Международный журнал инновационных исследований в области компьютерной и коммуникационной техники, Vol. 1, выпуск 4, июнь (2013): 859-864

3. Рашид, Акса, Малик Миссен и Надим Саламат. «Анализ методов стеганографии с использованием наименее значимого бит в изображениях в оттенках серого и его расширение на цветные изображения» Журнал научных исследований и отчетов (JSRR) 9.3 (2016): 1-14.

4. Ахмед Ласкар, Шамим. «Скрытие данных большой емкости с использованием стеганографии и шифрования LSB», Международный журнал систем управления базами данных (IJDMS) 4.6 (2012): 57-68.

5. Анил Кумар и Рохини Шарма. Защищенная стеганография изображений на основе алгоритма RSA и метода Hash-LSB. Международный журнал перспективных исследований в области компьютерных наук и программной инженерии. Том 3, выпуск 7, июль (2013): 363-372.

1. Романец Ю. В. Защита информации в компьютерных системах и сетях. /Под ред. В.Ф. Шаньгина. – М: Радио и связь 1999
2. Петраков А.В. Основы практической защиты информации. 2-е издание Учебн. Пособие. – М: Радио и связь 2010