ӘОЖ 004.932 **DOI 10.52167/1609-1817-2022-122-3-376 -383**

Э.Н. Дайырбаева[1,2], А.С. Еримбетова[2,3], А.Ж. Тұрғанбаев[2], А.Ж. Тойгожинова[1], А.Д. Нұрланбек[1]
[1]Логистика және көлік академиясы, Алматы, Қазақстан
[2]Ақпараттық және есептеуіш технологиялар институты ҚР БҒМ ҒК, Алматы, Қазақстан
[3]Satbayev University, Алматы, Қазақстан
E-mail: nurbekkyzy_e@mail.ru

ИНТЕРПОЛЯЦИЯ АРҚЫЛЫ СУРЕТТЕРДЕ АҚПАРАТТАРДЫ ЖАСЫРУ ЖОЛДАРЫНА ТАЛДАУ

Аңдатпа. Бұл мақалада белгілі стеганографиялық агоритмдерді талдай отырып, олардың тиімділігі мен заман талабына сай ақпараттарды қорғау, авторлық құқықты қорғау сияқты өзекті мәселелерді шешу барысында қолданылу жолдарын зерттедік. Сонымен бірге, стеганографияда контейнер ретінде қолданылатын: мәтін, сурет, аудио/видо файлдар және хаттамалар қарастырылды. Жасырын ақпараттарды жіберу барысында контейнер ретінде – суреттер қолданылды. Суреттер стеганография саласында ең көп қолданысқа ие объект ретінде белгілі болғандықтан, осы мақалада тағы да бір рет оның тиімді екенін анықтадық.

Жұмыстың мақсаты: жасырын ақпараттарды арналар арқылы беру тәсілдерін бикубтік интерполяцияның көмегімен орындау және оған стеготалдау жүргізу жолдарына талдау жасау болып табылды. Мақсатқа жету үшін мақалада стеганографиялық үш әдіс қарастырылды. Интерполяцияның бикубтік деп аталатын түрін пайдалана отырып, арнайы жасырын ақпаратты енгізу алгоритмін қолданып, Phyton тілінде бағдарлама жазылып, өз кезегінде 300 дана суреттер тесттен өткізілді. Бос және жасырын ақпараты бар контейнерлер RS стеготалдауының көмегімен қаншалықты жасырын түрде болуы мүмкін екендіктері зерттелді және эксперимент түрінде жасалып, тиісті нәтижелер алынды.

Сонымен қатар, жұмыста қолданылған контейнерлердің екі түрінің, яғни бос және жасырын ақпараттары бар контейнерлер көлемі кездейсоқ түрде таңдалынған архивтеу бағдарламаларының көмегімен салыстырылды және алынған нәтижелер қойылған эксперименттің дұрыстығын дәлелдей түсті. Алынған нәтижелер зерттеу барысында пайдаланылған жұмыс нәтижелерімен салыстырылды. Стеганография бағытында интерполяцияның басқа да түрлерін пайдалан отырып, болашақта басқа да зерттеулер жасау жоспарда бар.

Түйінді сөздер. Стеганография, интерполяция, LSB әдіс, RS талдауы, суреттер, стегоконтейнер.

Кіріспе.

Қазіргі уақытта мультимедиалық деректерді интернет арқылы бөгде адамдардың көшіруі немесе жоюы оңай болып тұрған кезеңде өмір сүрудеміз. Сондықтан деректерді жасырын түрде беру маңызды болып табылады. Хабарламаны жіберу фактісін жасырудың құралдары мен әдістерін әзірлеуді *стеганография* [1]. Оның ең тиімді қолданылуы криптографиялық әдістермен бірге қолданылады. Әдетте стеганография екі бағытқа бөлінеді: классикалық және компьютерлік. Соңғы уақытта деректерді жасыру әдістерін қолдану көптеген салаларда маңызды болды. Мысалы, көптеген цифрлық кескіндер, аудио және бейнелер қазір авторлық құқық туралы жасырын ескертуді немесе рұқсатсыз

көшіруді болдырмауға көмектесетін ерекше, бірақ анық емес белгілерді қамтиды [2]. Деректерді қалпына келтіргеннен кейін бастапқы кескінмен не болатынына байланысты деректерді жасырудың қайтымсыз және қайтымды әдістері бар. Деректерді қайтымсыз жасыру стеганография деп аталады.

Стеганография үшін сандық файлдардың барлық форматтарын қолдануға болады, бірақ жоғары дәрежелі форматтар қолайлы. Суреттер мен аудио файлдар бұған ерекше сәйкес келеді. 1 – суретте стеганография үшін қолдануға болатын төрт негізгі санатын көрсетілген:

1 сурет - Стеганография түрлері

Мәтіндегі ақпаратты жасыру стеганографияның маңызды әдісі болып табылады. Айқын әдіс құпия хабарламаны әр мәтіндік хабарламаның әр n әрпінде жасыру болды. Бұл тек алдымен Интернет және цифрлық файлдардың барлық форматтары, олардың маңыздылығын төмендетті [3]. Цифрлық файлдарды қолданатын мәтіндік стеганография жиі қолданылмайды, өйткені мәтіндік файлдарда артық мәліметтер өте аз.

Цифрлық суреттердің таралуын, әсіресе Интернетте және сандық кескін көрінісінде көп мөлшерде артық биттерді ескере отырып, суреттер стеганографияға арналған ең танымал қамту объектілері болып табылады.

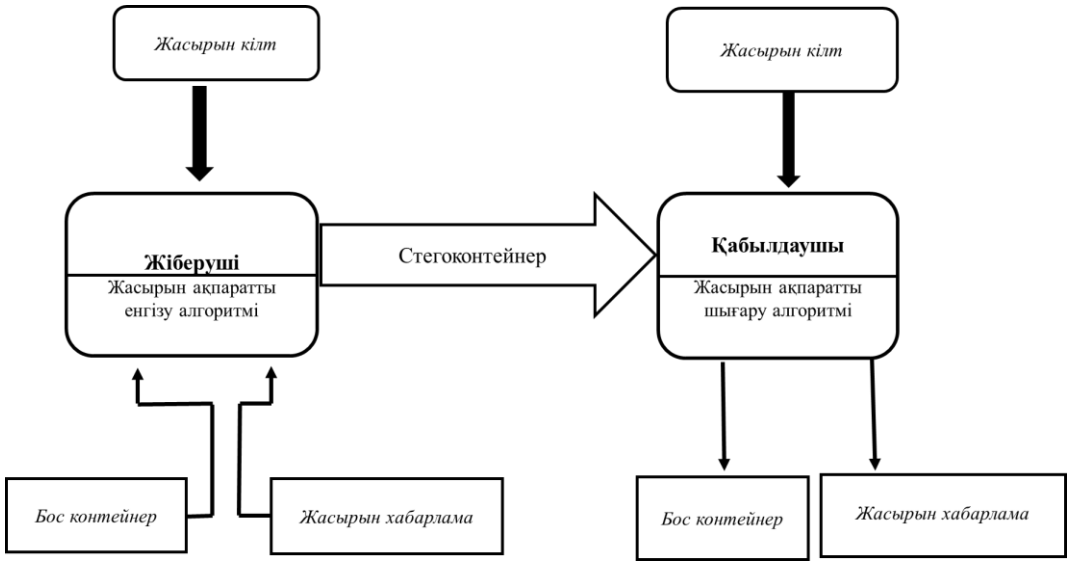
Аудио файлдардағы ақпаратты жасыру үшін кескін файлдарымен бірдей әдістер қолданылады. Стеганографиялық потенциал бойынша олар суреттерге тең болғанымен, маңызды аудио файлдардың үлкен мөлшері оларды суреттерге қарағанда азырақ танымал етеді [4].

«Хаттамалық стеганография» термині желі арқылы беру кезінде пайдаланылатын хабарламалар мен желіні басқару хаттамаларына ақпаратты енгізу техникасын білдіреді [5].

Стеганографияның басты мақсаты – хабарламаларды *контейнерлер* деп аталатын зиянсыз нысандарға енгізу арқылы байланыстың болу фактісін жасыру. Контейнер бос болып саналады, егер оның құрамында құпия деректер болмаса және тиісінше, толтырылған контейнер деп қандай да бір қол жетімсіз ақпаратты жасыратын объектіні атаймыз. Сандық стеганографиясындағы контейнерлер ретінде әр түрлі суреттерді, бейне файлдарды, аудио файлдарын, мәтіндік файлдарды және тіпті орындалатын файлдарды пайдалануға болады. Электрондық құжаттарда артық ақпарат болса, олар құпия хабарламаларды жасыру үшін объект ретінде пайдаланылады [6].

Құпия хабарламаны контейнерге орналастыру үшін элементтерді белгілі бір жолмен өзгертетін енгізудің алгоритмі қолданылады нәтижесінде толтырылған контейнер пайда болады, оны стегоконтейнер деп те атайды. Іске асыру процесі, әдетте, алгоритмнің барысын басқаратын және жасырын хабарлама алу үшін қажет секундтық стего-ключпен байланысты. Деректерді беру қауіпсіздігін арттыру үшін ендірмес бұрын хабарлама

«деректерді шифрлаудың кез-келген сенімді алгоритмі» көмегімен шифрланады. Стегоконтейнерден хабарламаны кері алу үшін қабылдаушы тарап тиісті енгізу алгоритмімен тығыз байланысты ақпаратты тарту алгоритмін пайдаланады. Құпия деректерді беруді ұйымдастыратын стегожүйе деп аталады және 2 – суретте бейнеленген.



2 сурет - Стегожүйенің сұлбасы

Суреттер – стеганография үшін қолданылатын ең танымал объект болып табылады. Цифрлық кескіндер саласында сурет файлдарының көптеген форматтары бар, олардың көпшілігі нақты қосымшаларға арналған. Бұл әртүрлі кескін файл пішімдері үшін әртүрлі стеганографиялық алгоритмдер бар. Компьютер үшін сурет – бұл кескіннің әртүрлі аймақтарындағы жарықтың әртүрлі қарқындылығы болып табылатын сандар жиынтығы. Интернеттегі суреттердің көпшілігі әр пиксель мен оның түсі орналасқан тікбұрышты кескін пиксель картасынан тұрады (бит түрінде ұсынылған) [7].

Суреттер негізінде ақпараттарды жасыру бойынша стеганографияның арнайы әдістері қолданылады.

Стеганография ғылымының дамуына үлес қосқан ғалымдар: Джанг (Zhang,H), Ф. Лию (Liu, F), К. Кашена (Cachin, C), Н. Провоса (Provos N.), К. Салливана (Sullivan, К.), Х. Фарида (Farid, H.), Дж. Фридрич (Fridrich, J,), А. Кера (Кег, А.).

Жұмыстың мақсаты: жасырын ақпараттарды арналар арқылы беру тәсілдерін бткубтік интерполяцияның көмегімен орындау және оған стеготалдау жүргізу жолдарына талдау жасау.

Материалдар мен тәсілдер.

Интерполяция арқылы суреттерде ақпараттарды жасыру экспериментін жасау үшін стеганографияның бірнеше әдістері қолданылды.

Бірінші әдіс ретінде стеганографияның LSB әдісі қарастырылды. Стеганографияның ең көп таралған және кеңінен қолданылатын әдістерінің бірі – кіші биттерге (LSB) ену әдісі [8]. Бүгінгі күні ол жасырын деректерді сандық суреттерге, фильмдерге және аудио жазбаларға енгізу үшін қолданыла береді. LSB әдісін қолданған ең алғашқы стеганографиялық сұлбалар бастапқы кескінге аздап бұрмалану енгізу арқылы ақпаратты енгізуге назар аударды, эвристикалық болжамды ескере отырып, ақпаратты енгізу кезінде бұрмаланулар неғұрлым аз енгізілсе, стеганографиялық сұлба соғұрлым қауіпсіз болады.

LSB енгізу әдістерінің қарқынды дамуы суреттер үшін стегоанализ әдістерінің пайда болуына себеп болды, яғни құпия хабарламаның берілу фактісін анықтау әдістері. Нәтижесінде, құпиялылықтың қолайлы деңгейін қамтамасыз ету үшін енгізу барлық пикселдерде емес, тек бір бөлігінде жүзеге асырылады және бұл пикселдер жалған кездейсоқ түрде таңдалады.

Екінші әдіс ретінде интерполяцияның бикубтік әдісі – фотосуреттерді өңдеу кезінде жақсы нәтижелер береді, себебі жақын аралықтағы сегіз пиксельдің мәндері қолданылады. Бикубтік интерполяция есептеу математикасында [9] екі айнымалы функция жағдайында мәні екіөлшемді жүйелі торда көрсетілген кубтық интерполяцияны кеңейту болып табылады.

Бикубтік интерполяция жағдайында $[0,1]\times[0,1]$ шаршының ішінде орналасқан $P(x,y)$ нүктесіндегі $f(x,y)$ функциясының мәні, f функциясының (i,j), $i=-1...2$, $j=-1...2$ он алты көрші нүктелердегі интерполяцияланған қабатты көрсететін функцияның жағдайындағы жалпы түрі төмендегідей болады:

$$P(x,y)=\sum_{i=0}^{3}\sum_{j=0}^{3}a_{ij}x^{i}y^{j}. \quad (1)$$

Мақалада қолданылатын үшінші әдіс ретінде стеготалдау әдісі пайдаланылды. Стеганоталдаудың негізгі мақсаты – стеганографиялық жүйелерді зерттеу және стегоақпаратты қолданудың сенімділігіне сапалы және сандық баға алу үшін оларды зерттеу, сондай-ақ контейнерде жасырылған ақпаратты анықтау, оны өзгерту немесе жою әдістерін құру. Стеготалдаудың негізгі міндеттерінің бірі – стеганографиялық құралдарды қолданудың ықтимал іздерін зерттеу және оларды қолдану фактілерін анықтауға мүмкіндік беретін әдістерді әзірлеу. Біздің жұмыста RS стеготалдауы қолданылды.

Статистикалық стеготалдаудың негізгі әдістерінің бірі –2001 жылы J.Friedrich және басқалар ұсынған RS (regular–singular) әдісі [10].

Нәтижелер.

Интерполяция арқылы суреттерде ақпараттарды жасыру эксперименті төмендегідей жүзеге асырылды:

- интерполяция үшін бикубтік интерполяция әдісін таңдау;
- интерполяция процесін жүзеге асыру;
- суреттерге жасырын хабарламаны енгізу процесі;
- жасырын хабарламаны суреттен қалпына келтіру процесі;
- декодтау нәтижесі;
- бос контейнерлер жиынтығы бойынша RS талдауын жүргізу;
- жасырын ақпараты бар контейнерлер жиынтығы бойынша RS талдауын жүргізу.

1 кесте - Бос контейнерлер жиынтығы бойынша RS талдауының нәтижелері

L		0%	1-4%	5% және одан көп
Файлдар үлесі	225x225	50	49,6	0,4

2 кесте - Жасырын ақпараты бар контейнерлер жиынтығы бойынша RS талдауының нәтижелері

L		0%	1-4%	5% және одан көп
Файлдар үлесі	225x225	33,6	64,2	2,2

3-кестеден көріп тұрғанымыздай бос және жасырын ақпараты бар контейнерлердің көлемдері тиісінше айырмашылықтарға ие. Екі түрлі контейнерлердің көлемін анықтау үшін төрт архиваторлар пайдаланылды және архиваторлар кездейсоқ таңдалды.

3 кесте - Бикубтік интерполяция әдісі арқылы 12%-ға толтырылған контейнерлердің көлемі

Архиватор	**Бос контейнерлер көлемі**	**Жасырын ақпараты бар контейнерлер көлемі**
RAR	107MB	141MB
ZIP	187MB	198MB
GZIP	188MB	199MB
BZIP2	156MB	174MB

Талқылау.

Біз бикубтік интерполяция әдісін жүзеге асырдық және зерттедік. Бұл енгізу әдісінің стегоанализі жүргізілді, нәтижелер алынды, оларды [8] қарастырған әдістердің стегоанализімен салыстыруға болады.

Қарастырылған әдіске сүйене отырып, біз контейнердің максималды сыйымдылығы 12% және суретке байланысты екенін анықтадық. 225x225 көлеміндегі 300 сурет тесттен өткізілді. Бірінші типтегі қателіктерді есептеу нәтижелері қатенің 0% екенін көрсетті.

RS талдауының қорытынды нәтижелері 1-кестеде көрсетілген, оған сәйкес бұл әдіс RS әдісіне төзімді екені анықталды. Сондай-ақ, зерттеуде біз бос және толтырылған контейнерлерді салыстырып көрдік.

Болашақта интерполяцияның басқа әдістерін қолдана отырып, растрлық файлдарға ақпаратты енгізудің тұрақты стеганографиялық әдістерін жасау, сондай-ақ оларды әртүрлі әдістермен талдау жоспарлануда.

Қорытынды.

Бұл мақалада стеганографиялық алгоритмдер зерттеліп, суреттер арқылы жасырын ақпараттарды тарату үшін қолданылатын үш стеганографиялық әдіс қолданылды. Мақаланың мақсаты жүзеге асырылды. Интерполяция арқылы суреттерде ақпараттарды жасыру алгоритмі Phyton бағдарламалау тілінің көмегімен жүзеге асырылды. Алынған нәтижелердің стеготалдауы RS стеготалдауының көмегімен жүзеге асырылды. Байланыс арналары арқылы жасырын ақпараттарды тарату барысында стегоконтейнерлер ретінде суреттерді пайдалану тиімді екені расталды.

Бұл зерттеуді Қазақстан Республикасы Білім және ғылым министрлігінің Ғылым комитеті қаржыландырды (Грант №AP08857179).

ӘДЕБИЕТТЕР

[1] Настинов Э.О. Сокрытие информации в изображениях с помощью стеганографии и LSB метода / Э.О. Настинов, В.Ю. Сергиенко, Н.Е. Шейдаков // Современные проблемы проектирования, применения и безопасности информационных систем:Материалы XVI Международной научной конференции, Кисловодск, 19–21 октября 2015 года. – Кисловодск: Ростовский государственный экономический университет "РИНХ", 2015. – С. 95-100. – EDN DOKAAX.

[2] Свищенко М. Е. Сравнение методов стеганографии в изображениях / М.Е. Свищенко, Р.А.Томакова // Программная инженерия: современные тенденции развития и применения (ПИ-2020):Сборник материалов IV всероссийской научно-практической конференции, посвященной 30-летию создания кафедры программной инженерии, курск, 12–13 марта 2020 года. – курск: Юго-западный государственный университет, 2020. – с. 189-193. – EDN ZUNFYE.

[3] Zhang, H., Song, Z., Feng, B., Zhou, Z., Liu, F. Technology of Image Steganography and Steganalysis Based on Adversarial Training (2020) Proceedings - 2020 16th International Conference on Computational Intelligence and Security, CIS 2020, pp. 77-80. DOI: 10.1109/CIS52066.2020.00025

[4] Дайырбаева Э.Н., Липская М.А., Тойгожинова А.Ж. Суреттерді өңдеуде стрип-әдісті пайданалу жолдары мен нәтижелері. Вестник КазНИТУ, №5 (2020). –бб. 279-284

[5] Дайырбаева Э.Н., Липская М.А., Тойгожинова А.Ж, Нугуманов Ш.Е. Сандық және компьютерлік стеганографиялардың сипаттамалары мен мүмкіншіліктеріне шолу. Вестник КазАТК №3 (114) 2020. -бб. 246-252

[6] Гонсалес Р., Вудс Р. Цифровая обработка изображений. Издание 3-е, исправленное и дополненное Москва: Техносфера, 2012. – 1104 с

[7] В.Т. Фисенко, Т.Ю. Фисенко, Компьютерная обработка и распознавание изображений: учеб. пособие. - СПб: СПбГУ ИТМО, 2008. – 192 с.

[8] Мерзлякова Е.Ю. Построение стеганографических систем для растровых изображений, базирующихся на теоретико-информационных принципах: дисс. … канд.тех.наук: 05.13.19. – Новосибирск: СибГУТИ, 2011. – 161 с.

[9] Lee C.-F.(2012). An efficient image interpolation increasing payload in reversible data hiding. Expert Systems with Applications. -Volume 39, Issue 8. – P. 6712-6719. https://doi.org/10.1016/j.eswa.2011.12.019

[10] Грачев Я.Л., Сидоренко В.Г. Стегоанализ методов скрытия информации в графических контейнерах. *Надежность*. 2021;21(3):39-46. https://doi.org/10.21683/1729-2646-2021-21-3-39-46https://doi.org/10.21683/1729-2646-2021-21-3-39-46

Elmira Daiyrbayeva, master's degree, research associate, Academy of Logistics and Transport, Institute of Information and Computing Technologies KN MES RK, Almaty, Kazakhstan, nurbekkyzy_e@mail.ru

Aigerim Erimbetova, senior researcher, associate professor, Institute of information and computing technologies of the Ministry of education and science of the Republic of Kazakhstan, Satbayev University,Almaty, Kazakhstan, aigerian@mail.ru

Aynur Toigozhinova, PhD, associate professor, Academy of logistics and transport, Almaty, Kazakhstan, aynur_t@mail.ru

Almas Turganbayev, software engineer, Institute of information and computing technologies of the Ministry of education and science of the Republic of Kazakhstan, Almaty, Kazakhstan, m1challenge@inbox.ru

Aigerim Nurlanbek, master's degree, senior lecturer, Academy of logistics and transport, Almaty, Kazakhstan, aika9008@mail.ru

ANALYSIS OF WAYS TO HIDE INFORMATION IN IMAGES BY INTERPOLATION

Abstract. In this article, analyzing well-known steganographic agorhythms, we studied their effectiveness and ways of their use in solving topical issues of modern information protection, copyright protection. At the same time, the following protocols were considered: text, image, audio/video files and protocols used as containers in steganography. In the process of sending hidden information, images were used as containers. Since images are known as the most widely used object in the field of steganography, in this article we once again found that they are effective.

The purpose of the work is to analyze the methods of transmitting hidden information through channels by means of bicubic interpolation and methods of stegotalization. To achieve this goal, three steganographic methods were considered in the article. Using the so-called bicubic form of interpolation, a program was written in the phyton language, in turn, 300 images were tested. The extent to which containers with empty and hidden information can be hidden using RS stegotalization has been studied and experimentally developed and relevant results have been obtained.

In addition, the volumes of two types of containers used in the work, i.e. Containers with empty and hidden information, were compared using randomly selected archiving programs, and the results obtained proved the correctness of the experiment. The results obtained were compared with the results of the work used in the study. In the direction of steganography, it is planned to conduct other studies in the future using other types of interpolation.

Keywords. Steganography, interpolation, LSB method, RS analysis, images, stegocontainer

Эльмира Дайырбаева, магистр, научный сотрудник, Институт информационных и вычислительных технологий КН МОН РК, Академия логистики и транспорта, Алматы, Казахстан, nurbekkyzy_e@mail.ru

Айгерим Еримбетова, старший научный сотрудник, ассоциированный профессор, Институт информационных и вычислительных технологий КН МОН РК, Satbayev University, Алматы, Казахстан, aigerian@mail.ru

Айнур Тойгожинова, PhD, ассоциированный профессор, Академия логистики и транспорта, Алматы, Казахстан, aynur_t@mail.ru

Алмас Турганбаев, инженер-программист, Институт информационных и вычислительных технологий КН МОН РК, Алматы, Казахстан, m1challenge@inbox.ru

Айгерим Нурланбек, магистр, сениор-лектор, Академия логистики и транспорта, Алматы, Казахстан, aika9008@mail.ru

АНАЛИЗ СПОСОБОВ СОКРЫТИЯ ИНФОРМАЦИИ НА ИЗОБРАЖЕНИЯХ С ПОМОЩЬЮ ИНТЕРПОЛЯЦИИ

Аннотация. В данной статье мы проанализировали известные стеганографические агоритмы, изучили их эффективность и способы применения при решении актуальных проблем, таких как защита современной информации, защита авторских прав. При этом в стеганографии рассматривались используемые в качестве контейнеров: текст, изображение, аудио/видофайлы и протоколы. При отправке скрытой информации в

качестве контейнера использовались изображения. Поскольку изображения известны как объект, который имеет наибольшее применение в области стеганографии, в этой статье мы еще раз определили, что он эффективен.

Целью работы являлось: выполнение способов передачи скрытой информации по каналам с помощью бикубической интерполяции и анализ способов ее стеготализации. Для достижения цели в статье были рассмотрены три стеганографических метода. С использованием так называемой бикубической интерполяции была написана программа на языке Phyton, в свою очередь было протестировано 300 экземпляров изображений. Было исследовано, насколько анонимными могут быть контейнеры с пустой и скрытой информацией с помощью стегоанализа RS, и было проведено экспериментальное исследование и получены соответствующие результаты.

Кроме того, объем использованных в работе контейнеров двух типов, т.е. контейнеров с пустой и скрытой информацией, сравнивался с помощью программ архивирования, выбранных случайным образом, и полученные результаты доказывали правильность поставленного эксперимента. Полученные результаты были сопоставлены с результатами работ, использованными в ходе исследования. В дальнейшем планируется проведение других исследований в направлении стеганографии с использованием других видов интерполяции.

Ключевые слова. Стеганография, интерполяция, метод LSB, RS анализ, изображения, стегоконтейнер.

****