UDC 519.688

# STEGANOGRAFIYA USULLARINING TAHLILI

*Zaynalov N.R.* [1], *Achilov S.S.* [1], *Vafayev M.A.* [1]
[1] Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Samarqand filiali, Samarqand, O‘zbekiston
nodirz@mail.ru

**Annotatsiya**. *Steganografiya usullari bevosita axborotlarni yshirishga yoki raqamli obyektlarga qo‘shimcha ma’lumotlarni kiritishga qaratilgan. Ushbu jarayonda obyektda qisman o‘zgarishlar yuzaga keladi. Bu erda obyekt yoki konteyner sifatida audio, video, tarmoq paketlari kabi raqamli formatlar qo‘llaniladi. Oxirgi yillarda matnli konteynerlarda axborotlarni yashirishga bag‘ishlangan maqolalar ko‘p uchramoqda. Steganografiya usullari bevosita konteynerda mavjud xossalarni o‘zgartirish orqali maxfiy ma’lumotlarni yashirishga harakat qiladi va sodir bo‘ladigan o‘zgarishlarni inson kuzata olmaydi. Tashkilotlarda matnli hujjatlarning keng qo‘llanilishi bevosita ularni konteyner sifatida qabul qilishga asos bo‘lib xizmat qiladi, ammo ularda katta hajmdagi ma’lumotlarni joylashtirish qiyin. Shu bois, matnli hujjatlarda ma’lumotlarni yashirish algoritmlarini ishlab chiqish murakkab masala. Ushbu maqolada matnli steganografiya usullarining tahliliy natijalari keltirilgan. Mualliflarning yondashuvini tushuntirish maqsadida ba’zi-bir usullarning mazmuni izohlab berilgan. Olingan natijalar mavjud usullarning 3 ta sinfga ajratilgan tasnifi sifatida keltirilgan. Shu bilan birga usullarning qabul qilingan nomlanishi saqlab qolingan. Shunday qilib, taklif etilgan xabarlarni yshirish usullarining tasniflash sxemasi amaliy jihatdan sodda va tushunish uchun samarali hisoblanadi.*

**Kalit so‘zlar:** *ma’lumotlarni yashirish, steganografiya, matnli steganografiya, tasnif.*

## I. KIRISH

Ma’lumotlarni yashirish (“information hiding” yoki “data hiding”) qadimdan foydalanilib kelingan va dolzarb bo‘lgan soha sanalgan. Ma’lumotlarni yashirish deganda kontent (rasmlar, qo‘shiqlar, videolar va b.) ichida kerakli ma’lumotlarni yashirish tushuniladi. Bu yerda, yashirish tushunchasi, ma’lumotni sezilmaydigan ko‘rinishda keltirish yoki ma’lumot maxfiyligining mavjudligini saqlash uchun foydalaniladi. Qadimda turli ma’lumotlarni yashirish usullaridan foydalanilgan holda, ma’lum doiradagi odamlar orasida ma’lumotlar almashinilgan.

Axborot xavfsizligini ta’minlsh qadimdan muhim masala hisoblanib kelingan [1], shu o‘rinda kriptografiya va steganografiya usullari ishlab chiqilgan. Hozirgi kungacha bu soha ko‘p olimlarning diqqatini jalb qilib kelmoqda. Ma’lumonlarni yashirish sohasi steganografiya nomi bilan yuritiladi.

Bu so‘z yunoncha Steganos (maxfiy, sir) va Graphy (yozuv) so‘zlaridan kelib chiqqan va «sirli yozuv» degan ma’noni bildiradi. Steganografiya usullari, ehtimol, yozuv paydo bo‘lishidan oldin paydo bo‘lgan (dastlab shartli belgi va belgilashlar qo‘llanilgan) [2,3]. Steganografiyaning kriptografiyadan boshqa yana o‘zgacha masalasi ham bor, ya’ni uning maqsadi - maxfiy xabarni

o‘zining mavjudligini ham yashirish. Bu ikkala usul birlashtirilishi ham mumkin va natijada axborotni himoyalash samaradorligini oshirish uchun ishlatilishi imkoni paydo bo‘ladi (masalan, kriptografik kalitlarni uzatish uchun). Steganografiya usullarida yashiriladigan ma’lumotlar bevosita diqqatni jalb qilmaydigan obyektda joylashtiriladi va u konteyner deb nomlanadi.

Kompyuter texnologiyalarining keskin rivojlanishi ushbu sohaga qo‘shimcha imkoniyatlar yaratib bermoqda. Bularga aydio fayllar, raqamli rasmlar, matnlar va bajariladigan dasturlar misol bo‘la oladi. Steganografiya orqali yashirilgan ma’lumotlarni maxsus algoritmlar orqali xabarlarni qabul qiluvchi aniqlash imkoniga ega bo‘ladi [4]. Agar ma’lumotlar shifrlangan bo‘lsa, unda qandaydir xabar borligi ayon bo‘ladi va yovuz niyatli shaxslar tomonidan hujum uyushtirilishi mumkin [5].

Steganografiyaning klassik usullari asosan quyidagicha tasniflangan:

• Konteyner faylining formatlar oralig‘ida ma’lumotlarni yashirish. Bunda ma’lumotlar fayl-konteynerning o‘qilmaydigan joylarida yoziladi, masalan, faylning oxirida, ya’ni EOF maxsus belgisidan keyin qo‘yiladi.

• Niqoblash orqali yashirish – bunda konteynerning fayl sifatidagi bo‘sh bo‘lgan xizmatvazifacini bajarishga mo‘ljallangan hududlarda joylashtiriladi. Masalan, faylning kelgusidagi imkoniyatlarini kengaytirishga qaratilgan bo‘sh joylari misol bo‘la oladi.

Shu bilan birga fayllarning formatining maxsus xossalaridan foydalanish mumkin, masalan:

• binar bajariladigan fayllarda maxsus ajratilgan va ammo ishlatilmaydigan maydonlar;

• fayldagi matnni maxsus formatlash, masalan, so‘zlar orasini siljitish;

• faylni identifikasiyalovchi sarlavhani o‘chirish.

Matnli steganografiyada belgilarning xossalaridan foydalanib ma’lumotlarni yashirish nazarda tutiladi. Matnli formatdagi fayl katta hajm talab etmagan va unda ishlash uslubi sodda bo‘lganligi sababli ushbu yo‘nalish keng imkoniyatlarga ega bo‘lmoqda. Masalan, kichik hajmdagi matnli faylda katta hajmdagi ma’lumotlarni yashirish.

Ushbu maqolada matnli steganografiyaga mansub usullar tasnifi tushunarli va soddalashgan shaklda ishlab chiqilgan va bunda ba’zi-bir usullarga to‘xtalib o‘tilgan.

## II. MAVJUD YONDASHUVLAR

Matnli steganografiya usullarining xilma-xilligi va ularning keng rivojlanishi bevosita ushbu usullarni tizimli o‘rganishni talab qiladi. Ushbu sohada ilk qadamlar bajarilgan, masala [6,7]. Albatta, tasniflash ma’lum bir alomatlar bo‘yicha obyektlarni tartibga solish tushuniladi. Masalan, yashiriladigan axborotning hajmi bo‘yicha tasniflash [7] keltirilgan. Shundan kelib chiqqan holda steganografiya uchta toifaga bo‘lingan: 1) belgilar bilan kiritish, 2) bitlar bilan kiritish va 3) aralash holda kiritish. Bundan tashqari [8] maqolada tasniflash bevosita usullarning mohiyatidan kelib chiqqan holda bajarilgan va misollar bilan tasdiqlangan.

Ma’lumotlarni yashirin jo‘natishda oddiy gazetalardan foydalanish hollari

tarixda uchrab turgan. Masalan, Angliyadagi gazetalardan birida harflar ostiga sezilar-sezilmas nuqtalar qo‘yilgan. Ushbu harflar birlashtirilganda esa yashirin yozuv hosil bo‘ladi. Ushbu g‘oyadan foydalanib Word muhitida ma’lumotlarni yashirish mumkinligi mualliflar tomonidan ko‘rib chilgan [8]. umumiy holda ushbu usulni “Index” deb nomlash mumkin bo‘ladi. Quyidagi misolda Hofiz Sheroziyning buyuk misralarda axborotni yashirish yo‘lini keltiramiz:

Агар кўнглимни шод этса ўшал Шероз жонони,
Қаро холига бахш этгум Самарқанду Бухорони.

Ushbu matnga “амир жахон” xabarini joylashtirish uchun Word muhitida mavjud “Предметный указатель” texnologiyasidan foydalanilsa, unda quyidagi hosil bo‘ladi:

Ага XE "а" р кўнглим XE "м" ни XE "и" шод этса ўшал Шер XE "р" оз ж XE "ж" онони,
Ка XE "а" ро х XE "х" о XE "о" лига бахш этгум Самарканду Бухорон XE "н" и.

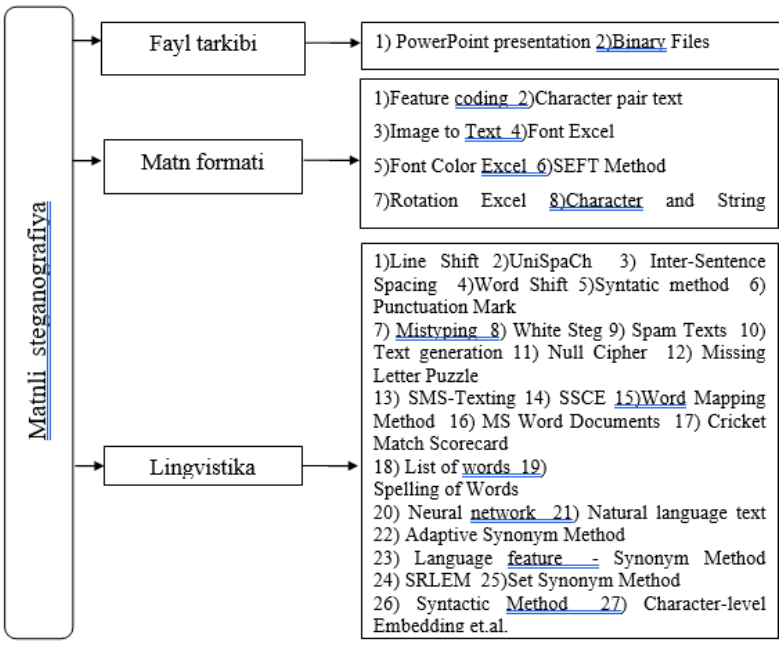
Ushbu belgilarni “Alt+X” tugmalari orqali ham shakllantirish mumkin. Agar ushbu rejim yopilsa, oddiy matn rejimiga o‘tiladi va yozuvdagi yashirin xabar ko‘rinmas holatga o‘tkaziladi.

## III. TAKLIF ETILADIGAN YECHIM

Oldingi bo‘limda ko‘rib chiqilgan tasniflash jarayoni juda kuchli vosita hisoblanib, jarayonni, hodisani va obyektlarni o‘rganishda va tahlil qilishda muhim hisoblanadi. Obyektning xossalarini o‘rganishga ulardagi umumiylikni asos qilib olish mumkin. Masalan, obyekt sifatida fayllarni oladigan bo‘lsak, ularni bevosita matnli yoki binarli fayllarga taqsimlash mumkin. Taklif etiladigan usulda tasniflash obyektlari sifatida quyidagilar qabul qilingan: Fayl tarkibi, Matn formati va Lingvistika. Ushbu yashirin ma’lumotlarni shakllantirishda mavjud usullarni ushbu xossalar bo‘yicha ajratib olamiz (1-rasm). Faylning formati bu ma’lumotlarning tarkibiy tuzilishi bo‘yicha kelishuv bo‘lib, uning identifikatori sifartida fayl kengaytmasi qabul qilingan. Ushbu identifikator orqali amaliy va tizimli dasturlar fayllarni qayta ishlashga asos bo‘lib xizmatqiladi. Ushbu format bevosita faylning o‘zida ham kiritilgan bo‘ladi. Masalan, “doc” formati bevosita Word 97-2003 ning hujjati bo‘lib, umumiy holda binar faylda saqlanadi, shu bilan birga “docx” formatli fayl ham Word dasturining hujjati hisoblanadi, ammo faylning formati XML ga asoslangan. Shu bois Word hujjati umumiy holda murakkab obyektlardan iborat bo‘ladi va tarkiblangan mohiyatiga asoslanib tashkillashtiriladi.

Xuddi shunday Excel 2007 tizimida ham XML formati qo‘llanilgan va barcha obyektlar (kitob, varaq, shablon va b.) ushbu formatda shakllantirilgan. Shu bilan birga ushbu obyektlar ZIP arxivlarda saqlanadi.

Shunday qilib, matnli steganografiyada mavjud usullarni tasniflashda fayllarning yuqoridagi sifatlari ham e’tiborga olinadi. Shu bilan birga ba’zi-bir usullar haqida qisqa ma’lumotlar berilgan. Ushbu tasnif doirasida mavjud usullarning taqqoslash va rivojlanish yo‘nalishlarini belgilab beradi va yaratilgan algoritmlarni ilmiy izlanishlarda va tijorat masalalarida qo‘llash paydo bo‘ladi. Ushbu chizmada keltirilgan matnli steganografiya usullari [7] keltirilgan bo‘lib, ularning ba’zilarida to‘xtalib o‘tamiz.




**1-rasm.** Matnli steganografiya usullarining tasnifi.

### 3.1 PowerPoint Presentation

Ushbu usulda PowerPoint fayli asos qilib olingan bo‘lib, uning keng tarmoqli tarkibiy qismidan foydalaniladi. Ushbu usul mualliflari [9] PowerPoint dasturida yaratilgan faylning tarkibida ko‘p bo‘sh joylar borligini tahlil qilib aniqlashgan. Umumiy holda PowerPoint fayli bevosita sarlavha va tartiblangan konteynerlardan iborat bo‘ladi. Ushbu konteynerlar ma’lumotlarni yashirish uchun juda qulay vosita bo‘lib xizmat qiladi.

### 3.2 Feature coding

Ushbu usulga mansub ko‘p ishlanmalar mavjud bo‘lib, asosiy g‘oya sifatida belgilarning xossalari hisoblanadi. Masalan, [10] keltirilgan usulda shriftlar ustida o‘zgarishlarni amalga oshirish orqali (shrift o‘lchami, yozilish stili va b.) ko‘p hajmda ma’lumotlarni joylashtirish mumkinligi ko rsatilgan. Ba’zi-bir ishlanmalarda faqatgina ASCII kodiga mos kelgan belgilar doirasida emas, balkim maxsus belgilardan foydalanish mumkinligi ko‘rsatilgan, masalan, Space, Enter, LR va b. Ushbu usullar bo‘yicha keltirilgan ma’lumotlar boshqa nom bilan ham uchraydi, masalan, Character Marking [7].

### 3.3 Line Shift

Ushbu usul klassik usullardan biri bo‘lib, so‘zlar orasida Space belgisini kiritish orqali amalga oshiriladi. Bu yerda belgilarni faqatgina gorizontal bo‘yicha siljitish bilan birga, vertikal siljitish algoritmlari ham ishlab chiqilgan [6, 11]. To‘liq qatorlar orasidagi masofani o‘zgartirish orqali ma’lumotlarni yashirish esa [12] keltirilgan.

Umumiy holda, 1-rasmda keltirilgan Lingvistika usulllariga mansub bo‘lgan matnli konteynerda ma’lumotlarni yashirish usullarini shartli ravishda quyidagi ikki sinfga ajratish mumkin.

### 3.4 Sintaksis usullar

Ushbu usulga mansub ishlanmalar, masalan, ko‘rinmas belgilarni matga joylashtirish usuli [13] bo‘lib, bunda qo‘shimcha bo‘sh kataklar joylashtirish

taklif qilingan. Ushbu belgilar matn ma’nosiga hech qanday ta’sir ko‘rsatmaydi. Keyingi usulda [14], matnning maxsus joylarida “izlar” qoldiriladi. Ushbu sinfga mansub usullar juda oddiy yo‘l bilan aniqlanib olinishi mumkinligi sababli hozirgi kunda keng qo‘llanilmaydi.

### 3.5 Semantik usullar

Ushbu usullarda matn ma’nosi o‘zgarmagan holda gaplar boshqa ko‘rinishda yoziladi [15-16]. Shu bilan birga matnni boshqa tillarga tarjima qilish ham mumkin bo‘ladi, bunda to‘g‘ri tarjima yashirin ma’lumotga mos keladi [17-18]. Qiziqarli yo‘nalishlardan biri – bu tushunarsiz matnni genertasiya qilish usuli hisoblanib [19], unda matn til qoidalari bo‘yicha shakllantiriladi, ammo ma’nosiz hisoblanadi, shu bilan birga undagi yashirin matnni aniqlash ham qiyin bo‘ladi. Ushbu sinfga mansub keyingi usulda sinonimlar almashuvi qo‘llaniladi [20], bunda sinonimlar uzatiladigan bitlarni anglatadi. Bu bilan matnning ma’nosi o‘zgarmay qoladi, ammo til qoyidalariga zid ifodalar paydo bo‘lishi mumkin, bu esa ushbu usulning zaif qismi hisoblanadi.

## IV. OLINGAN NATIJALAR

Ishlab chiqlgan matnli steganografiya usullarining tasnifi asosan ma’lumotlar formatining maxsus xossalaridan foydalanishga qaratilganligi aniqlanildi. Umumam olganda ushbu yo‘nalishda kelgusida yanada ko‘p ilmiy izlanishlarni kutish mumkin, chunki amaliy dasturlarning har bir keyingi varianti kengroq imkoniyatlarga ega bo‘ladi. Shu qatorda, matndagi yozuvning lingvistik tamoyillari bevosita har xil tillarni qamrab olishi mumkin, ya’ni keltirilgan usulni boshqa tillarda ham qo‘llash mumkin. Ammo fayllarning tarkibini chuqur o‘rganish va unda ma’lumotlarni yashirishga qaratilgan ilmiy ishlanmalar ozligi bevosita ushbu sohada yaratilishi mumkin bo‘lgan usullarni kutish mumkin.

Tasniflash doirasida olib borilgan izlanishlar natijasida bulutli texnologiyalarga e’tibordan chetda qolmoqda. Ammo [21] keltirilgan izlanishlar bu sohada ham steganografiya usullarini ishlab chiqish mumkinligidan dalolat beradi. Umumam olganda, bulutli texnologiyalarni steganografiyada qo‘llash bo‘yicha alohida ilmiy izlanishlar olib borish zarur.

## IV. XULOSA

Keyingi yillarda mamlakatimizda olib borilayotgan ijtimoiy-iqtisodiy va ijtimoiy-siyosiy islohotlarning samaradorligini oshirishning muhim sharti sifatida davlat va jamiyat boshqaruvi sohasiga zamonaviy axborot-kommunikatsiya tizimlarini joriy etishga muhim e’tibor qaratib kelinmoqda.

Afsuski, bugungi kunda axborot xavfsizligi uchun yuz foizlik natijani ta’minlaydigan profilaktik muhofaza qilish tizimi mavjud emas. Shuning uchun hujumlarni aniqlash va ularga to‘g‘ri baho berish masalasi axborot xavfsizligi muammolarini hal qilishda birinchi o‘ringa chiqadi. Shu bois matnli steganografiya usullarini chuqur o‘rganish va ularni iqtisodiy masalalarda vujudga keladigan axborotlarni himoyalashda kriptografiya usullari bilan birgalikda foydalanish yuqori ahamiyatga egadir.

Shunday qilib, steganografiya usullarining rivojlanishi bevosita kompyuterda fayllarni saqlashdagi yangi texnologiyalarning rivojlanishi bilan chambarchas bog‘liq bo‘lib, kelgusida axborotlarni yashirish va ularni uzatishda keng imkoniyatlar vujudga keladi.

## ADABIYOTLAR

[1] *Zaynalov N.R., Muhamadiev A.N., Kiyamov J.* Kriptografiya usullariga doir oddiy misollar// Fizika, matematika va informatika jurnali, 2019, № 2, 26-34 b.

[2] *Fabien A.P. Petitcolas, Ross J.Anderson, Markus G.Kuhn.* (1999). Information hiding—a survey. In: Proc IEEE 87(7): pp.1062-1078.

[3] *Por LY, Ang TF, Delina B* (2008) WhiteSteg-a new scheme in information hiding using text steganography. WSEAS Trans Comput 7(6): pp.735-745.

[4] *Changder S, Ghosh D, Debnath N.C.* (2010). Linguistic approach for text steganography through Indian text. In: 2010 2nd international conference on computer technology and development, pp. 318-322.

[5] *Ross J. Anderson, Fabien A.P. Petitcolas.* (1998). On the limits of steganography. IEEE J Sel Areas Commun 16(4): pp.474-481.

[6] *Hassan Shirali-Shahreza M., Mohammad Shirali-Shahreza* (2006) A new approach to persian/arabic text steganography. In: 5th IEEE/ACIS international conference on computer and information science and 1st IEEE/ACIS international workshop on component-based software engineering, software architecture and reuse, pp 310-315.

[7] *Bala Krishnan R., Prasanth Kumar Thandra, M. Sai Baba.* An overview of text steganography. 4th International Conference on Signal Processing, Communi-cations and Networking (ICSCN - 2017), March 16 - 18, 2017, Chennai, INDIA.

[8] *Zaynalov N.R., Narzullaev U.Kh., Muhamadiev A.N., Bekmurodov U.B., Mavlonov O.N.* Features of using Invisible Signs in the Word Environment for Hiding Data. 2019. International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8, Issue-9S3, July 2019. pp.1377-1379.

[9] *Tiwari R.K., Sahoo G.* Microsoft power point files: A secure steganographic carrier. 2011. International Journal of Digital Crime and Forensics. 3(4), pp. 16-28.

[10] *Shut'ko N. P.* The algorithms of realization of text steganography methods based on the modification of the geometric and color text parameters. Belarusian State Technological University. BGTU. № 6 2016, pp.160-165.

[11] *Hassan Shirali-Shahreza M., Mohammad Shirali-Shahreza* (2008) A new dynonym text steganography. In: International conference on intelligent information hiding and multimedia signal processing, pp. 1524-1526.

[12] *Blinova E. A.* Steganographic method based on the line-shift coding method on non-displayed symbols of the electronic text document. Belarusian State Technological University. BGTU. № 6 2016, pp.166-169.

[13] *Koluguri A., Gouse S., Reddy P. B.* Text steganography methods and its tools. Int. J. Adv. Sci. Tech. Res. 2014. V. 2. No. 4. P. 888-902.

[14] *Judge J. C.* Steganography: past, present, future. Lawrence Livermore National Lab., CA (US), 2001. – №. UCRL-ID-151879.

[15] *Atallah M. et al.* Natural language watermarking: Design, analysis, and a proof-of-concept implementation. Information

Hiding. – Springer Berlin/ Heidelberg, 2001. P. 185-200.
[16] *Meral H. M. et al.* Natural language watermarking via morphosyntactic alterations. Computer Speech & Language. 2009. V. 23. No. 1. P. 107-125.
[17] *Grothoff C. et al.* Translation-based steganography. International Workshop on Information Hiding. – Springer, Berlin, Heidelberg. 2005. P. 219-233.
[18] *Stutsman R. et al.* Lost in just the translation. Proceedings of the 2006 ACM symposium on Applied computing. – ACM. 2006. P. 338-345.
[19] *Chapman M., Davida G.* Hiding the hidden: A software system for concealing ciphertext as innocuous text. International Conference on Information and Communications Security. – Springer Berlin/Heidelberg, 1997. P. 335-345.
[20] *Winstein K.* Lexical steganography through adaptive modulation of the word choice hash. URL: http://web.mit.edu/keithw/tlex/ (Ochilgan sanasi: 14.01.2019).
[21] *Islomov S.Z., Mavlonov O.N., Muhamadiev A.N., Shodmonov D.A., Djumaev S.N.* New authentication scheme for cloud computing. 2018. Journal of Advanced Research in Dynamical and Control Systems. 10(10), c. 2316-2319.

*Поступила в редакцию 29.03.2022*

**Citation**: *Zaynalov N.R., Achilov S.S., Vafayev M.A.* Steganografiya usullarining tahlili. // Raqamli texnologiyalarning nazariy va amaliy masalalari xalqaro jurnali. – 2022. – № 1(1). – B. 23-30.

# ANALYSES OF STEGANOGRAPHY METHODS

*Zaynalov N.R.* [1], *Achilov S.S.* [1], *Vafaev M.A.* [1]
[1] Samarkand branch of Tashkent University of information technologies named after Muhammad al-Khwarizmi, Samarkand, Uzbekistan
nodirz@mail.ru

**Abstract**. *The current state and development of information systems and technologies requires information security, therefore, in this paper, the methods of steganography are considered and a new classification is given. Steganography is a method that is based on hiding or embedding additional information in digital objects, while causing some distortion of these objects. In this case, an image, audio, video, network packets and other types of data formats can be used as objects or a container. There have been a lot of posts lately in the field of hiding information in a text container. To implement the secret, steganographic techniques rely on redundant information about the covering medium used or properties that the human perceptual system cannot discern. Since text documents are widely used in organizations, using a text document as the storage medium may be the preferred choice in such an environment with little redundant information. Therefore, the choice of using a text document as an information carrier is the most difficult, since it contains less redundant information. In this article, we present the result of the analysis of steganography methods based on text documents. At the same time, comments are given to some methods for understanding the approach of the authors. The result of this work is presented in the form of classifications of existing methods into*

*three classes. In addition, it can be noted that the given methods are accompanied by the generally accepted names of these methods. Thus, the proposed classification scheme is practical and effective for understanding message hiding methods.*

**Keywords**: *information hiding, steganography, text steganography, classification.*

# АНАЛИЗ МЕТОДОВ СТЕГАНОГРАФИЙ

*Зайналов Н.Р.* [1], *Achilov S.S.* [1], *Вафаев М.А.*[1]
[1]Самаркандский филиал Ташкентского университета информационных технологий имени Мухаммада ал-Хорезми, Самарканд, Узбекистан
nodirz@mail.ru

**Аннотация**. *Современное состояние и развитие информационных систем и технологий требует обеспечения информационной безопасности, исходя из этого в данной работе рассмотрены методы стеганографий и даётся новая классификация. Стеганография — это метод, который основан на сокрытии или внедрении дополнительной информации в цифровые объекты, вызывая при этом некоторые искажения этих объектов. При этом в качестве объектов или контейнера могут быть использованы изображение, аудио, видео, сетевые пакеты и другие виды форматов данных. В последнее время наблюдается очень много публикации в области скрытия информации в текстовом контейнере. Для встраивания секрета стеганографические методы опираются на избыточную информацию об использованном покрывающем носителе или свойствах, которые человеческая система восприятия не может различить. Так как текстовые документы широко используются в организациях, использование текстового документа в качестве носителя информации может быть предпочтительным выбором в такой среде, при этом имеют малую избиточную информацию. Поэтому, выбор использования текстового документа в качестве носителя информации является наиболее сложным, так как он содержит менее избыточную информацию. В этой статье мы представляем результат анализа методов стеганографии на базе текстовых документов. При этом даются комментарий некоторым методам для понимания подхода авторов. Результат данной работы оформлен в виде классификаций существующих методов на три класса. Кроме того, можно заметить, что приведенные методы сопровождаются общепринятыми названиями этих методов. Таким образом, предлагаемая схема классификаций является практичной и эффективной для понимания методов скрытия сообщения.*

**Ключевые слова:** *скрытие информации, стеганография, текстовая стеганография, классификация.*