

APRIL 27-28, 2023

KONTENT AUTENTIFIKATSIYASI

<sup>1</sup>Fozilov Shavkatjon Ibrohimjon o'g'li, <sup>2</sup>Yo'ldosheva Maftuna Zokirjon qizi

<sup>1</sup>NamDU. O'qituvchi E-mail: shavkatmanager@gmail.com

<sup>2</sup> NamDU. Magistrant

<https://doi.org/10.5281/zenodo.7859352>

**Abstract.** *This article examines the use of watermarked content to verify its integrity.*

**Keywords:** *authentication, detections, reversal, thin watermarking, signature attachment, removable watermarking symbols.*

Aksariyat autentifikatsiyalash tizimining vazifasi bu kontentning yuboruvchi va qabul qiluvchi tomonlar orasida almashinuvida o'zgarishlarga uchramaganligini aniqlashdir. Hattoki kontentning bir-birining almashinishi kontentni autentifikatsiya jarayonidan o'tmaganligini anglatadi.

Aniq autentifikatsiyalash watermarkingdan foydalanishning ikkita yondoshuvi mavjud. Birinchisi holda watermarking belgisi shunday hosil qilinadiki, belgi qo'yilgan kontentning o'zgarishi belgini aniqlanmasligini ta'minlaydi. Ikkinchi yondoshuvda kriptografik raqamli imzolaridan foydalanish orqali, kontent o'zgargan holda imzoni tegishli emasligi aniqlanadi.

Nozik watermarking belgilar. Nozik watermarking belgilari shunday belgilarki, kontentning kichik o'zgarishi bu belgilarni aniqlanmasligini ta'minlaydi. Shu vaqtgacha o'tilgan mavzularga teskari bo'lgan, bu xususiyatlar kontentga bo'lgan ta'sirlarni muhim ekanligini anglatadi. Nozik o'rnatilgan belgilar aniqlansa, demak kontentga o'zgarish amalga oshirilmagan. Aks holda esa, kontentga qandaydir o'zgarish amalga oshirilgan.

Eng keng tarqalgan nozik watermarking belgilariga LSB usulida qo'yilgan belgilarni olish mumkin. Sababi, bu usulda kontentning eng kichik biti o'rniga ma'lumotning muhimligi katta bo'lgan biti yashiriniladi. Eng kichik bit esa tashqi ta'sirlarga juda ham sezgir bo'ladi.

Imzolarni biriktirish. Imzolaridan qanday tarzda foydalanish kriptografik ilovalar uchun tushunarli. Imzolaridan watermarking tizimlarida kontent autentifikatsiyasi uchun foydalalanish mumkin. Kriptografiyada qo'yilgan imzo ma'lumotga sarlavha kabi biriktirilsa, watermarking tizimlarida esa bu kontent bo'ylab tekis taqsimlanadi. Sarlavha kabi qo'yilganda uni osonlik bilan olib tashlash imkoniyati mavjud bo'ladi.

Qo'yiluvchi imzolar nozik watermarking belgilari shaklida èki bardoshli belgilar shaklida ifodalanadi. Bardoshli belgilar shaklida ifodalanganda kontent ustida o'zgarishlarni amalga oshirgan taqdirdaham qo'yilgan belgi o'zgarmaydi. Buning natijasida kontent xususiyatidan hisoblangan imzo va aniqlangan imzo bir-biriga tengligi kontentning o'zgarmaganligini, bir-biriga teng bo'lmagan holda esa uni o'zgarganligini bildiradi. Nozik belgilardan foydalanilgan taqdirda esa bardoshli belgilardan foydalanilganga qaraganda soddaroq bo'ladi. Kontentga qo'yilgan nozik belgi kichkina o'zgarishga ta'sirli sanalib, detektorlanganda bu belgi aniqlanmasa kontentga o'zgarishlar amalga oshirilgan. Aks holda kontentga o'zgarishlar amalga oshirilmagan.

Olib tashlanuvchan watermarking belgilar. Ba'zida kontentga biriktirilgan eng kichik hajmdagi imzo ham, kontentga ta'sir qilishi mumkin. Masalan, tibbiètga aloqador ilovalarda kontentga biriktirilgan imzo kam bo'lsa ham, kontent o'zgarishiga ta'sir qiladi. Bu esa shifokorni

**APRIL 27-28, 2023**

qaror qabul qilishiga aks ta'sir qilishi mumkin. Shu sababli olib tashlanuvchan watermarking belgilarni ishlab chiqishni ta'lab etadi (belgi qo'yilgan kontentdan belgini olib tashlash va haqiqiy kontentdan nusxaolish uchun).

Quyida olib tashlanuvchan watermarking belgilarini yaratishning asosiy qadamlari keltirib o'tilgan:

-Haqiqiy kontentning butun yuzasi bo'ylab imzo hisoblanadi. Hisoblangan imzo kontentga olib tashlanuvchanlik xususiyati bilan birlashtiriladi;

-Qabul qiluvchi kontentdan imzoni ajratib oladi va uni qayd etib qo'yadi;

-Qabul qiluvchi kontentdan imzoni olib tashlaydi. Bu holatda olingan kontent haqiqiy kontent bilan bir xil bo'lishi kerak;

-Buni tekshirish uchun qabul qiluvchi belgi olib tashlangan kontentning xesh qiymatini hisoblaydi. Qayd qilingan imzoni dekodlab olingan xesh qiymat bilan kontentning xesh qiymati bir-biriga mos kelgan taqdirda kontent o'zgirishga uchramagan. Aks holda kontent o'zgarishga uchragan;

Amalda olib tashlanuvchan belgilarni birlashtirish juda muammoli sanalib, buni amalga oshirishda quyidagi uchta shart bajarilishi kerak:

-Belgini birlashtirishni 100 % samaradorlik bilan amalga oshirish;

-Kontentni qayta tiklaganda (kontentdan belgini ajratganda) haqiqiy holatdagisi bilan bir xil bo'lishi;

-Juda kam miqdorda e'lg'ondan tasdiqlash ko'rsatkichini mavjud bo'lishi talab etiladi.

**Maxsus autentifikatsiyalash.** Aniq autentifikatsiyalash usuli juda ko'p ilovalarda foydalaniladi. Masalan, bu usulda foydalanilganda kontentdagi bir-ikkita bitlarni o'zgarishi natijani tamomila boshqa ko'rinishga olib keladi. Boshqa so'z bilan aytilganda bu usul o'zgarishlarga juda ham tasirchan. Shunga qaramasdan, kontent ustida ba'zi o'zgarishlarni amalga oshirganda kontentning ko'rinishiga jiddiy ta'sir etmaydi(1-rasm).

Olingan rasmlar bir-biriga juda o'xshasada, ular aniq autentifikatsiyadan o'ta olmaydi. Bu esa maxsus autentifikatsiyalash usulini yaratishga sabab bo'ladi. Bu usulda kontent ustida muhim o'zgarish sodir bo'lgan taqdirdagina autentifikatsiyadan o'ta olmaslik mumkin bo'ladi.

Noqonuniy va qonuniy o'zgarishlar. Maxsus autentifikatsiyalash usullari kontentga quyidagi, yo'qotilishli chiqish, filterlash, tahrirlash, o'zgarishlar amalga oshirilganda talab etiladi. Bu o'zgarishlar o'z navbatida ikki turga: qonuniy va noqonuniy o'zgarishlarga ajratiladi. Kontent qonuniy o'zgarishga uchraganda tizim kontentni autentifikatsiyalashdan muvofiqiyatli o'tadi yoki noqonuniy o'zgarishlarga uchragan kontent autentifikatsiyalashdan o'ta olmaydi.

APRIL 27-28, 2023



Haqiqiy kontent

1-rasm. Maxsus autentifikatsiyalash

Odatda kontentga qonuniy va noqonuniy o'zgarishlar amalga oshirilganda yaqqol ko'rinishidan farqlanadi. Masalan yuqoridagi 1-rasmda amalga oshirilgan o'zgarishni qonunuy deb olish mumkin. Quyida keltirilgan o'zgarishni esa noqonuniy o'zgarishga kiritish mumkin(2-rasm).



JPEG formatda (95 % aniqlik bilan siqilishdagi)



Haqiqiy kontent

2-rasm. Noqonuniy o'zgarishlar

Yuqoridagi ikki rasmdan qonuniy va noqonuniy o'zgarishlarni yaqqol ajratish mumkin. Quyida qonuniy o'zgarishlar keltirilgan(3-rasm).



Tahrirlangan kontent



Haqiqiy kontent

3-rasm. Qonuniy o'zgarishlar

Javob esa kontentga bog'liq holda aniqlanadi. O'zgarishlarni qonuniy va qonuniy bo'lmagan turlarga ajratish yetarlicha katta muammo sanaladi.

Yarim-nozik watermarking belgilari. Bu turdagi belgilarga qonuniy o'zgarishlar ta'sir etmaydi, noqonuniy o'zgarishlar esa tasir etadi. Bu turdagi belgilarni yaratish maxsus autentifikatsiyalash usullarini ishlab chiqishda erdam beradi. Yarim-nozik watermarking belgilarini ishlab chiqishda, belgini qonuniy o'zgarishlarga bardoshliligi ta'minlansa, shuning o'zi yetarli sanaladi.



JPEG formatda (20 % aniqlik bilan siqilishdagi)

APRIL 27-28, 2023

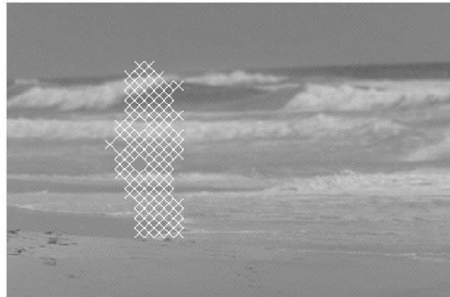
Nazoratchi yoki chaqimchi watermarking belgilari. Yuqori yarim-nozik belgilardan foydalanishdan maqsad, qonuniy va noqonuniy orasidagi farqni aniqlashdan iboratligi aytib o‘tiladi. Shunga qaramasdan, ba’zi watermarking tizimlarida qonuniy va noqonuniy o‘zgarishlar orasidagi farq vaqt o‘tishi bilan, joy o‘zgarishi bilan o‘zgarib turadi. Bu holda ko‘proq kontent o‘zgarishga uchradi degan savoldan ko‘ra, kontent qayday o‘zgarishga uchradi degan savol muhimroq sanaladi. Bu savolni javobini aniqlashda Nazoratchi yoki chaqimchi watermarking belgilaridan foydalaniladi.

**Aniqlanishlar.** Ko‘plab autentifikatsiyalash metodlari birlashtirilgan belgini qachon va qayerga qo‘yilganini aniqlashga asoslanadi. Kontentning qolgan qismi esa o‘zgarmasdan qoladi. Bu qobiliyat – aniqlanish deb aytiladi.

Belgilarni qayerda va qachon yashiringanligini bilish orqali belgini o‘zgargan e‘ki o‘zgarmaganligini aniqlash, autentifikatsiyalashni amalga oshirish mumkin.

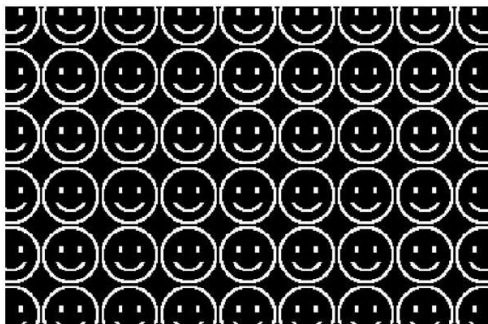
Aniqlashda quyidagi ikki endoshuv keng foydalaniladi:

Bloshlashga asoslangan kontent autentifikatsiyasi. Bu usulda asoslangan autentifikatsiyalashda kontent bir nechta vaqt yoki maydon xususiyati bo‘yicha bloklarga bo‘lanadi. Belgi ham har bir blok uchun alohida- alohida qo‘yiladi. Autentifikatsiyalash har bir blok ustida amalga oshiriladi. Agar o‘zgarish amalga oshirilgan taqdirda faqat o‘zgargan blok autentifikatsiyalashdan o‘ta olmaydi(4-rasm).

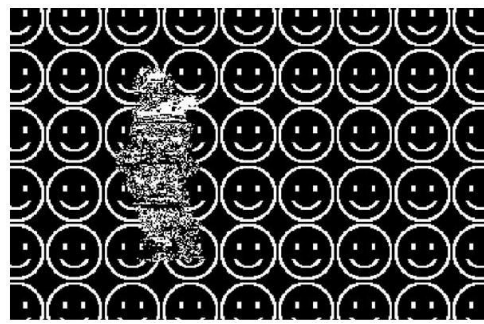


4-rasm. Bloklashga asoslangan autentifikatsiyalash.

Na‘munaga asoslangan autentifikatsiyalash usuli. Bu usul bloklashga asoslangan usulning bir xususiy holi bo‘lib, bunga ko‘ra kontent ko‘plab kichkina bloklarga emas, balki yagona bloklarga ajratiladi.



Na‘munalarga ajratish



Na‘munaga asoslangan  
autentifikatsiyalash

5-rasm. Na‘munaga asoslangan autentifikatsiya.

**Qaytarish.** O‘tilgan barcha ma‘ruzalardan kelib chiqib, kontent o‘zgargan taqdirda ham belgini aniqlash imkonini mavjudligini aytish mumkin. Bu esa o‘z navbatida o‘zgargan kontentni qaytarish imkonini mavjudligini anglatadi. Ikki xil usulda qaytarish imkonini mavjud bo‘lib, ular:

**APRIL 27-28, 2023**

aniq qaytarish va taqribiy qaytarish. Nomiga bog‘liq holda, aniq qaytarishda o‘zgargan kontent o‘zining holatida to‘liq qaytariladi va bu ancha katta muammodir.

Taqribiy qaytarishda esa xatolik bilan qaytariladi. Bu usul amalda keng foydalaniladi. Quyida bularning har biri bilan alohida tanishib chiqiladi.

Biriktirilgan qoldiq ma’lumot. Bu usul aniq qaytarish usuliga kiradi. Bu usuldagi qaytarishda xatoliklarni aniqlash va tuzatish kodlari keng foydalaniladi. Kontentni o‘zgarishi xatoliklarni tuzatish imkoniyati darajasida bo‘lsa, u holda o‘zgangan kontent to‘liq qaytariladi.

Xatoliklarni tuzatish kodlari ERI algoritmlariga o‘xshasada, ulardan vazifasi jixatidan kengroqdir. ERI algoritmlari faqat o‘zgarishni aniqlasa, xatoliklarni tuzatish kodlari esa ularni tuzatadi ham.

O‘zini o‘ziga biriktirish. Bu usul taqriban qaytarish usuliga kiradi. Ko‘plab manbalarda, kontent siqilgan ko‘rinishini kontentning o‘ziga biriktirish amalga oshiriladi. Bu usul o‘zini o‘ziga biriktirish usuli deb yuritiladi. Bunga misol sifatida quyidagini olish mumkin. Haqiqiy kontent rasm olinib, undan 50 % siqilgan JPEG formatdagi ko‘rinishi olinadi. Bu holda o‘rtacha bir pikseldan bir bitiga teng bo‘ladi. Olingan bir bit mos haqiqiy kontentga LSB usulida biriktiriladi.

Ko‘rko‘rona qaytarish. Bu usul ham taqriban qaytarish usuliga kiradi. Bu usulga asosan dastlab kontentning o‘zgargan qismlari aniqlanadi va ular invertlash orqali dastlabki holatga qaytariladi. Bu usul faqat o‘zgaishlar invertlash xususiyatiga ega bo‘lgan taqdirdagina katta yutuq beradi.

## **REFERENCES**

1. Fozilov, Sh.I., Ovozni tanish algoritmlari. *Oriental renaissance: Innovative, educational, natural and social sciences 2.5-2* (2022): 553-562.
2. N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems, " *IBM systems Journal*, vol. 40, p. 614-634.
3. Fozilov Sh.I., Yo‘ldosheva M.Z.,. Yuz shakli bo'yicha autentifikatsiyalash usullari. *Ta'lim va rivojlanish tahlili onlayn ilmiy jurnali 2.8* (2022): 148-154.
4. Fozilov Sh.I., Yo‘ldosheva M.Z., Biometrik autentifikatsiyalash tizimlari. *Barqarorlik va yetakchi tadqiqotlar onlayn ilmiy jurnali 2.8* (2022): 55-59.
5. Fozilov Sh.I., Yo‘ldosheva M.Z., Autentifikatsiya muammolari, usullari va vositalari. *Oriental renaissance: Innovative, educational, natural and social sciences 2.6* (2022): 1197-1206.
6. M. A. Dabbah, W. L. Woo, and S. S. Dlay, "Secure Authentication for Face Recognition, " presented at *Computational Intelligence in Image and Signal Processing, 2007. CIISP 2007. IEEE Symposium on*, 2007.
7. Fozilov Sh.I., Yo‘ldosheva M.Z. Yuz rasmi xarakteristikalarini xususiyatlari va elementlarini aniqlash. *Barqarorlik va yetakchi tadqiqotlar onlayn ilmiy jurnali 2.8* (2022): 86-88.