INTERNET TARMOGIDA VIDEOTASVIRLARNI HIMOYA QILISH MODEL VA USULLARI

Normatov Ibroximali Xolmatovich
Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy universiteti professori
E-mail: i_normatov@nuu.uz
tel: +998977210920
Doschanova Aziza Xusainboy qizi
Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy universiteti magistranti
Abduqaxxorova Nigora Doniyor qizi
Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy universiteti magistranti

Annotatsiya. Ushbu maqolada robast Xesh funksiyasidan foydalangan holda videotasvirlarning yaxlitligini ta'minlash masalasi ko'rib chiqilgan. Shuningdek, maqolada har bir komponent bo‘yicha olib borilgan tadqiqotlar asosida videotasvirlarning yaxlitligini himoya qilish uchun mo‘ljallangan model taklif etiladi. Ushbu modelning grafik diagrammasi keltirilgan. Yaxlitlikni himoya qilish tizimlarida autentifikatorlarni uzatishning asosiy yondashuvlari o‘rganilgan. Autentifikatorning himoyalangan video ma’lumotlardan ajralmasligiga erishish, shuningdek, aloqa kanaliga qo‘shimcha yuklanish masalasini hal qilish uchun autentifikatorni raqamli videoregistrator sifatida uzatildi. Eng ishonchli usul sifatida video ma’lumotlarini himoya qilish uchun mo’ljallangan va tashqi va ichki huquqbuzarlardan himoya qilishga imkon beradigan usul, ya’ni Yoxansson sxemasiga asoslangan usul tanlangan. Ko‘rib chiqilgan komponentlar asosida video ma’lumotlarning yaxlitligini himoya qilish model va usullari taklif etilgan.

Kalit so‘zlar: model, algoritm, usul, videotasvir, videoregistrator, autentifikator, Xesh funksiya, diagramma, tarmoq

Аннотация. В данной статье рассматривается вопрос обеспечения целостности видеозаписей с помощью хеш-функции robast. В статье также предлагается модель, предназначенная для защиты целостности видеозаписей на основе исследований каждого компонента. Представлена графическая схема данной модели. Изучены основные подходы к передаче аутентификаторов в системах защиты целостности. Чтобы добиться неотделимости аутентификатора от защищенных видеоданных, а также решить вопрос о дополнительной нагрузке на канал связи, Аутентификатор передается как цифровой видеорегистратор. В качестве наиболее надежного метода был выбран метод, предназначенный для защиты видеоданных и позволяющий защитить их от внешних и внутренних нарушителей, то есть метод, основанный на схеме Йоханссона. На основе рассмотренных

ISSN 3030-3907

компонентов предложены модель и методы защиты целостности видеоданных.

Ключевые слова: модель, алгоритм, метод, видеоизображение, видеорегистратор, аутентификатор, хеш-функция, диаграмма, сеть.

Annotation. This article discusses the issue of ensuring the integrity of video recordings using the robust hash function. The article also proposes a model designed to protect the integrity of video recordings based on research on each component. A graphical diagram of this model is presented. The main approaches to the transfer of authenticators in integrity protection systems have been studied. In order to ensure the inseparability of the authenticator from the protected video data, as well as to resolve the issue of additional load on the communication channel, the Authenticator is transmitted as a digital video recorder. The method designed to protect video data and protect it from external and internal intruders, that is, the method based on the Johansson scheme, was chosen as the most reliable method. Based on the considered components, a model and methods for protecting the integrity of video data are proposed.

Key words: model, algorithm, method, video image, DVR, authenticator, hash function, diagram, network.

Kirish

Bugungi kunda sayyoramizda internet foydalanuvchilari soni 55 foizdan ko‘proq aholisi yoki 5,5 mlrd kishi internetdan foydalanish imkoniga ega va bu ko‘rsatkich oshishda davom etmoqda [1-7]. Foydalanuvchilarning videotasvirlarga bo'lgan ehtiyojning oshishi unga tahdidlar sonining ko'payishiga olib keladi. Videotasvirlarning yaxlitligini ta'minlashga ma'lum bo'lgan barcha asosiy yondashuvlarni ikki guruhga - “passiv” va "faol" yondashuvlarga bo'lish mumkin.

Videotasvirlarning yaxlitligini ta'minlashga ma'lum bo'lgan barcha asosiy yondashuvlarni ikki guruhga bo'lish mumkin:

- birinchi guruh “passiv” yondashuvlarni o‘z ichiga oladi, bunda qasddan buzilishlar uzatuvchi tomonda autentifikatorlar hosil bo‘lmagan holda videotasvirlarni informatsion xususiyatlar bilan aniqlanadi;

- ikkinchi guruh "faol" yondashuvlarni o‘z ichiga olib, bunda ma’lum bir tarzda autentifikatsiya qiluvchilarni shakllantirish jo'natuvchi va qabul qiluvchi tomonidan amalga oshiriladi. “Faol” yondashuvlar “passiv” yondashuvlarga qaraganda qasddan buzilishdan ko'proq himoya qiladi. Elektron raqamli imzoda tasodifiy buzilishlarga qarshilikning ehtimoli bitta autentifikatsiya bitining buzilishi uchun 10^{-9} ga teng [1-4].

Materiallar va tadqiqot usullari

ISSN 3030-3907

Maqolada modelni qurishning umumiy yondashuvlari, shuningdek, har bir komponent bo‘yicha olib borilgan tadqiqotlar asosida videotasvirlarning yaxlitligini himoya qilish uchun mo‘ljallangan model [1-6] taklif etiladi. Ushbu modelning grafik diagrammasi 1-rasmda keltirilgan.

Model quyidagi asosiy komponentlardan iborat:

1. Jo‘natuvchini himoya qilish komponenti quyidagilardan iborat:

1.1 Robast Xash funksiyasi modeli - F

1.2 Autentifikatorni shakllantirish modeli - Q

1.3 RSB shakllantirish va joylashtirish modeli - W_{emd}

2. V_T jo‘natuvchining asosiy ma’lumotlari

3. Uzatish kanali. Ushbu element C kodlovchi modellarini va dekoder D video ma’lumotlarini o‘z ichiga oladi.

4. V_R qabul qiluvchining asosiy ma’lumotlari

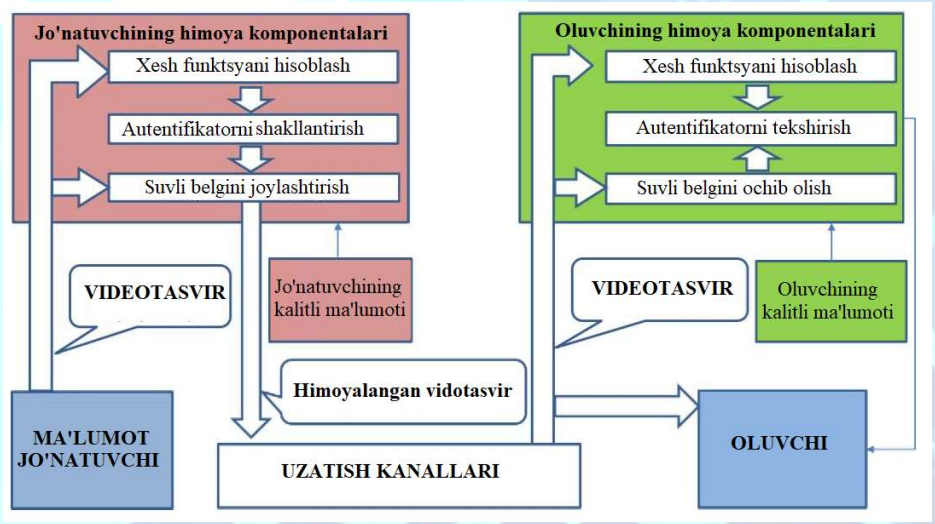
5. Qabul qiluvchini himoya qilish komponenti quyidagilardan iborat:

5.1 Robast Xesh funksiyasi modeli - F

5.2 Autentifikatorni tekshirish modeli - A

5.3 RSB chiqarish modeli - W_{ext}.

Maqolada videotasvirlarning yaxlitligini ta'minlash va himoyalash modeli taklif etiladi [7-10]. Ushbu modelning grafik diagrammasi 1-rasmda keltirilgan.



1-rasm. Video ma’lumotlarining yaxlitligini himoya qilish modeli.

Yuqorida tavsiflangan model quyidagi $I'_w = W_{emd}(I, Q(F(I,q),h,V_T),w)$, ko‘rinishda keltirish munkin, bu yerda I'_w - RSB bilan qoplangan video ma’lumotlarning bir qismi, W_{emd} - RSB shakllantirish modeli, Q - har bir bitta autentifikator uchun:

$$\alpha = V_{T1} \oplus X \cdot V_{T2} \quad (1)$$

$$\beta = V_{T3} \oplus X \cdot V_{T4} \quad (2)$$

ISSN 3030-3907

(1) va (2) formulalar bo‘yicha autentifikatorni shakllantirish modeli, F - xesh funksiyasining modeli, h - autentifikatorning uzunligi, q - xesh funksiyasi parametrlarining vektori. Ushbu parametr vektoriga h ham kiradi. w - RSB modeli parametrlarining vektori, ushbu parametr vektoriga h kiradi. V_T – jo‘natuvchining asosiy ma’lumotlari. Autentifikatorlarni RSB sifatida joylashtirish amalga oshirilgandan so‘ng, fragment siqiladi:

$$I'_{cw} = C(I'_w) \qquad (3)$$

bu yerda I'_{cw} - siqilgan va C kodlash modelidan foydalangan holda qo‘llaniladigan RSB bilan oqimga joylashtirilgan video segment, keyin himoyalangan video segment uzatish kanaliga kiradi. Qabul qiluvchi quyidagi teskari dekompressiya jarayonini amalga oshiriladi: $I'_{pw} = D(I'_{cw})$, bu yerda I'_{pw} - video ma’lumot dekoderining modeli D himoyalangan video segmenti. Shundan so‘ng, qabul qiluvchining himoya komponentida olingan videoni tekshirish tartibi boshlanadi. Buning uchun RSB mustaqil ravishda olinadi, shuningdek olingan parcha uchun xesh kodi hisoblanadi. Shundan so‘ng, olingan autentifikator qabul qiluvchining asosiy ma’lumotlari va hisoblangan xesh kodi yordamida tekshiriladi. Tekshirishning matematik formulasi quyidagi tengsizlik ko‘rinishida $U(A(W_{ext}(I'_{pw}, w, h), F(q, I'_{pw}), V_R), h) \leq P_{max}$ ifodalanishi mumkin, bu yerda U - qasddan buzilishlarni aniqlamaslik ehtimolini baholashning kombinatorial formulasi. Qasddan buzilishlarni aniqlamaslik ehtimolini baholashning kombinatsion formulasi bo‘lsa, A har bir autentifikator uchun W_{ext} chiqarish modelini, shuningdek V_R ma’lumotlarni qabul qiluvchining asosiy ma’lumotlarini qo‘llash orqali raqamli qiymat sifatida chiqarilgan autentifikatordan foydalangan holda autentifikatorni tekshirish modeli. Agar aniqlanmaslik ehtimoli belgilangan P_{max} chegarasidan past bo‘lsa, fragment tekshiruvdan o‘tgan deb hisoblanadi.

Video ma’lumotlarning yaxlitligini himoya qilish modellaridan oqilona foydalanish uchun video ma’lumotlarning himoya qilishning usullari taklif etiladi:

- ikki sinfli klassifikator rejimida video ma’lumotlarning yaxlitligini himoya qilish modelidan foydalanish;
- komponentlarni tanlash va ishlatilgan yaxlitlikni himoya qilish modelining xavfsizlik parametrlarini sozlash;
- qasddan buzilishlardan xavfsizlikni baholash.

Tadqiqot natijalarini muhokama qilish

Ushbu usullarda video ma’lumotlarning yaxlitligini himoya qilish modeli himoyalangan video ma’lumotlarning ikki sinfli klassifikatori rejimida qo‘llaniladi. Model elementlarini tanlash mezonining matematik formulasi quyidagicha ifodalaniladi:

ISSN 3030-3907

$$S = \frac{1}{m}\sum_{i=1}^{m} \gamma(W_e, F, X_i, w, q, h, y_i) \to min$$

bu yerda S - bu butunlikni himoya qilish modeli uchun sifat funksiyasi. γ funksiya, X_m – o‘quv namunasi, W_e - elektron raqamli imzo modeli, F - mustahkam xesh funksiyasi modeli, w – raqamli suv belgisi modeli parametrlari vektori, q - mustahkam xesh funksiyasi parametrlari vektori, h - “yarim mo‘rt” ning ishlatilgan uzunligi, y_i - ta’lim namunasi X_i obyektining i obyektiga javob va $y_i \in \{-1, +1\}$ “o‘qituvchi” javoblaridir. Qasddan va tasodifiy buzilishlar uchun $y_i = +1$ ga, tasodifiy buzilishlar uchun esa $y_i = -1$ ga mos keladigan qiymatni ko‘rib chiqamiz. Vizual buzilish darajasi V funksiyasi bilan baholanadi:

$$V(I, I'_p) \gg V(I, I'_w), V(I, I'_p) \approx V(I, I'_{pw}), \;\; V(I, I'_{pw}) \ll V(I, I'_f),$$

bu yerda I – videotasvirlarning asl qismi, o‘rnatilgan raqamli video yozuvlar tomonidan kiritilgan buzilishlar bilan video ma’lumotlarning bir qismi, I'_p, I'_{pw} - qabul qilinadigan ishlov berish va maqbul qayta ishlash natijasida tasodifiy buzilishlar kiritilgan va bir-biriga qo‘yilgan video ma’lumotlarining bo‘laklari. I'_f qoidabuzar tomonidan ataylab buzilgan video ma’lumotlarning bir qismidir. Aniqlanmaslik ehtimoli kombinatorial tarzda quyidagi formula yordamida baholanadi:

$$P \geq \frac{\sum_{v=0}^{k} C_n^v}{\sum_{v=0}^{k} C_n^v + \sum_{v=k+1}^{n} C_n^v} \qquad (4)$$

bu yerda P - bitta “mo‘rt” autentifikatorlarning umumiy soni, k – tekshirilmagan bitta “mo‘rt” autentifikatorlarning soni. Autentifikatorni uzunligi bo‘yicha tekshirish va video ma’lumot parchasini sinflardan biriga tayinlash quyidagicha ifodalanishi mumkin:

$$\gamma_i = sign\left(U\left(\sum_{j=1}^{h} a\left(u_j\left(x_j \oplus x'_j, P_e(h)\right)\right)\right) - P_{max}\right), \quad i = \overline{1, m},$$

bu yerda a - j-chi mustaqil autentifikatorni tekshirish va agar u to‘g‘ri bo‘lsa, funksiya 0 ni qaytaradi, aks holda 1. Foydalanish qulayligi uchun ularning ehtimolliklarini o‘nlik logarifmlar bilan almashtiramiz. Qaror qabul qilishning ehtimollik chegarasidan [2,3] chekinishni quyidagicha belgilaymiz:

$$M_i(h, q) = y_i \frac{2}{h \log_{10} 2} \log_{10} \frac{1}{P_{max}} U\left(\sum_{j=1}^{h} a\left(x_j(F(q)) \oplus x'_j(F(q)), P_e(h)\right), h\right).$$

ISSN 3030-3907

Matematik formulalar, komponentlarni tanlash va parametrlarni sozlash uchun optimallashtirish muammosi sifatida, mos yozuvlar vektorlari usulini belgilashga o‘xshaydi [1-10] va aniqlanmaslik ehtimoli makonidagi buzilish sinflari orasidagi bo‘shliqni maksimal darajada oshirishdan iborat va quyidagicha ifodalanishi mumkin:

$$\begin{cases} \frac{1}{m}\sum_{i=1}^{m0}\left(1 - M_i\left(h, F(q), P_e(h)\right)\right) + G\sum_{i=1}^{m}\tau_i + R\sum_{i=1}^{m}\mu_i \to min \\ \log_{10} U(k(P_e(h), I_i), h) \le \log_{10} P_{max} + \tau_i \\ V\left(I_i, I'_{w_i}\left(P_{e_i}(h)\right)\right) \le b - \mu_i \\ \tau_i \ge 0, i = 1 \dots m \\ \mu_i \ge 0, i = 1 \dots m \end{cases}.$$

Ratsional yechimni topish uchun quyidagi ikkita alohida vazifaga bo‘lish mumkin [1-4]:

1. RSB modelini tanlash va parametrlarni sozlash - tasodifiy buzilishlar bilan obyektlar sinfida tizim yechimlarini ratsionalizatsiya qilish uchun mo‘ljallangan:

$$\begin{cases} \frac{2}{hm\log_{10} 2}\sum_{i=1}^{m/2}\log_{10} U(k(P_e(h), I_i), h) + G\sum_{i=1}^{m/2}\tau_i + R\sum_{i=1}^{m/2}\mu_i \to min \\ V\left(I, I'_w, P_{e_i}(h)\right) \le b - \mu_i \\ \log_{10} U(k(P_e(h), I_i), h) \le \log_{10} P_{max} + \tau_i \\ h \ge \log_2(P_{max}) \end{cases}.$$

2. Robast Xesh funksiyasi modelini tanlash va parametrlarni sozlash - qasddan buzilishlarni o‘z ichiga olgan obyektlar uchun video ma’lumotlarning yaxlitligini himoya qilish modelining ishlashi ratsionalizatsiya qilinadi:

$$\sum_{j=1}^{h} x_j \oplus x'_j \le \sum_{j=1}^{h} a\left(u_j((x_j \oplus x'_j), P_e(h)\right), \vartheta_{R_j}),$$

$$\sum_{j=1}^{h} a(u_j\left(x_j \oplus x'_j, P_e(h)\right), \vartheta_{R_j}) \le \sum_{j=1}^{h} a\left(u_j\left(x_j \oplus x'_j, P_e(h) + P_f(h)\right), \vartheta_{R_j}\right),$$

bu yerda, $P_f(h)$ - qasddan buzilish sodir bo‘lganda, j -chi bitta autentifikator yo‘q qilinishi ehtimoli. Qasddan buzilgan sinf uchun parametrlar va komponentlarni tanlash vazifasi xesh funksiyalarining ishlashini o‘rganishga qisqartirilishi mumkin.

Xulosa

Maqolada videotasvirlarining yaxlitligini himoya qilishni ta’minlashning asosiy yondashuvlari ko‘rib chiqilgan bo‘lib, yaxlitlikni himoya qilishning asosiy

ISSN 3030-3907

komponenti sifatida xesh funksiyasidan foydalangan holda ushbu yondashuvlar birlashtirildi, yaxlitlikni himoya qilish tizimlarida autentifikatorlarni uzatishning asosiy yondashuvlari o‘rganildi. Autentifikatorning himoyalangan video ma’lumotlardan ajralmasligiga erishish, shuningdek, adabiyotda tasvirlangan aloqa kanaliga qo‘shimcha yuklanish muammosini hal qilish uchun autentifikatorni raqamli videoregistrator sifatida uzatishga qaror qilindi. Autentifikatorni shakllantirishning asosiy yondashuvlari ko‘rib chiqildi. Eng istiqbolli usul sifatida Yoxansson sxemasiga asoslangan usul tanlandi, u video ma’lumotlarini himoya qilish uchun moslashtirildi, bu tashqi va ichki huquqbuzarlardan himoya qilishga imkon berdi. Ko‘rib chiqilgan komponentlar asosida video ma’lumotlarning yaxlitligini himoya qilish modeli va usuli taklif etildi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. Мартимов Р.Ю. Электронная стенографическая подпись видеоданных//Автоматизация процессов управления. №2 (36). ФНПЦ АО «НПО МАРС». 2014 г. - 20 - 27 с.
2. Мартимов Р.Ю. Способ численной оценки защищенности от преднамеренных искажений с использованием робастной хэш функции. И66 Инновации в науке// Сб. сб. по материалам XLVI международной научно-практической конф. №6 (43). Новосибирск: Изд. «СибАК», 2015. - 26 -33 с
3. Оков И.Н. Аутентификация речевых сообщений и изображений в каналах связи. Военная академия связи. СПб, Издательство Политехнического университета, - 2006, - 300 с.
4. Портал, посвященный машинному обучению URL:http://MachineLearning.ru (Дата обращения 2.10.2015)
5. А.В.Аграновский, А.В.Балакин, Р.А.Хади, Классические шифры и методы их криптоанализа, М: Машиностроение, Информационные технологии, №10, - 2001 г.
6. Кабулов В.К., Кабулов А.В., Норматов И.Х. Алгоритмизация в теории управляющих систем//Монография: Ташкент-2017, Изд. “Навруз” С.176.
7. Кабулов В.К., Кабулов А.В., Норматов И.Х. Логические методы алгоритмизации в теории управляющих систем. Монография: Германия.2018, Изд. “Ламберт” С.191.
8. Скляров В.А., Кабулов А.В. Микропроцессорная система с распределенным управлением// ДАН УзССР, 1988, № 7, С.12-14.
9. Кабулов А.В., Норматов И.Х. и др, Инвариантное продолжение дискретных многозначных функций и их реализация// 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), 2021. – С. 1 -6, doi: 10.1109/IEMTRONICS52119.2021.9422486.

ISSN 3030-3907

10. Норматов И.Х., Бабаджанов О.Ф., Кудайбергенов А. Исследование методов поиска максимальных совместных подсистем систем нелинейных булевых уравнений// Научный вестник НамГУ, № 2024-11, С. 81-85.

ISSN 3030-3907