KRIPTOLOGIK MA’LUMOTLARNI TASNIFLASH UCHUN SUN’IY NEYRON TARMOG‘I PARAMETRLARINI OPTIMALLASHTIRISH USULLARI

Davlatov Mirzo-Ulug‘bek Bobir o‘g‘li
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti tayanch doktoranti
e-mail: mirzoulugbekdavlatov@gmail.com
Allanov Orif Menglimuratovich
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti, Kiberxavfsizlik va kriminalistika kafedrasi mudiri
E-mail: orif_allanov@mail.ru

Annotatsiya. *Ushbu maqolada kriptologik ma’lumotlarni, xususan ochiq matn–shifrmatn juftliklari asosida shakllantirilgan belgilarni sun’iy neyron tarmog‘i yordamida tasniflash masalasi ko‘rib chiqiladi. Tasniflash samaradorligiga ta’sir qiluvchi asosiy giperparametrlar — yashirin qatlamlar soni, neyronlar soni, aktivatsiya funksiyasi, o‘rganish tezligi, batch size, epoch va regularizatsiya parametrlarini tanlash masalasi tahlil qilinadi. Giperparametrlarni qo‘lda tanlashdagi subyektivlikni kamaytirish maqsadida genetik algoritmga asoslangan optimallashtirish sxemasi taklif etiladi. Taklif etilgan yondashuv kriptologik ma’lumotlarning nolinear bog‘lanishlarini hisobga olgan holda klassifikatsiya modelining barqarorligi va umumlashtirish qobiliyatini oshirishga yo‘naltirilgan.*

Kalit so‘zlar: *kriptologiya, kriptotahlil, sun’iy neyron tarmog‘i, tasniflash, giperparametr, genetik algoritm, AES, S-AES, optimallashtirish, mashinaviy o‘qitish.*

Аннотация. *В статье рассматривается задача классификации криптологических данных с использованием искусственной нейронной сети, в частности признаков, формируемых на основе пар открытый текст–шифртекст. Анализируются основные гиперпараметры, влияющие на эффективность классификации: число скрытых слоёв и нейронов, функция активации, скорость обучения, размер пакета, число эпох и параметры регуляризации. Для уменьшения субъективности ручного подбора гиперпараметров предлагается схема оптимизации на основе генетического алгоритма. Подход ориентирован на повышение устойчивости и*

обобщающей способности модели при выявлении нелинейных зависимостей в криптологических данных.

Ключевые слова: *криптология, криптоанализ, искусственная нейронная сеть, классификация, гиперпараметры, генетический алгоритм, AES, S-AES, оптимизация, машинное обучение.*

Abstract. *This article considers the classification of cryptological data using an artificial neural network, with particular attention to features formed from plaintext–ciphertext pairs. The principal hyperparameters affecting classification performance are examined, including the number of hidden layers and neurons, activation function, learning rate, batch size, number of epochs, and regularization parameters. To reduce the subjectivity of manual hyperparameter selection, a genetic-algorithm-based optimization scheme is proposed. The approach is intended to improve model stability and generalization while capturing nonlinear relationships in cryptological data.*

Keywords: *cryptology, cryptanalysis, artificial neural network, classification, hyperparameters, genetic algorithm, AES, S-AES, optimization, machine learning.*

Kirish

Raqamli axborot almashinuvi hajmining ortishi kriptografik tizimlarning ishonchliligini baholash, kriptotahlil usullarini takomillashtirish hamda katta hajmdagi kriptologik ma’lumotlardan yashirin qonuniyatlarni aniqlash masalalarini dolzarb qilib bormoqda. An’anaviy kriptotahlilda statistik, algebraik, differensial va chiziqli yondashuvlardan foydalaniladi. Biroq murakkab nolinear o‘zgartirishlarga ega blokli shifrlarda belgilar orasidagi munosabatlarni oldindan qat’iy matematik shaklda ifodalash har doim ham oson emas. Shu sababli so‘nggi yillarda mashinaviy o‘qitish va chuqur o‘qitish vositalaridan kriptografik tuzilmalarni tahlil qilishda foydalanishga qiziqish ortmoqda.

Sun’iy neyron tarmoqlari kirish ma’lumotlaridagi murakkab va nolinear bog‘lanishlarni o‘rganish xususiyati sababli kriptologik ma’lumotlarni tasniflashda istiqbolli vosita hisoblanadi. Masalan, ochiq matn va unga mos shifrmatn bitlaridan tuzilgan xususiyatlar vektori tarmoq kirishiga uzatilishi, chiqishda esa shifr kalitining muayyan biti yoki sinf belgisi bashorat qilinishi mumkin. 2026-yilda e’lon qilingan S-AES bo‘yicha tadqiqotda 32 kirishli MLP modeli va sozlangan learning rate hamda batch size yordamida bit bo‘yicha aniqlikning taxminan 84 foizdan 92 foizgacha yaxshilangani qayd etilgan [1]. Bu natija kriptologik masalalarda nafaqat tarmoq arxitekturasi, balki giperparametrlarni to‘g‘ri tanlash ham muhim ekanini ko‘rsatadi.

Neyron tarmoq giperparametrlari model o‘qitilishidan oldin belgilanadigan boshqaruv qiymatlaridir. Ularga yashirin qatlamlar va ulardagi neyronlar soni, aktivatsiya funksiyasi, learning rate, batch size, epoch soni, dropout darajasi, optimizator turi va regularizatsiya koeffitsiyentlari kiradi. Ushbu qiymatlarning noo‘rin tanlanishi modelning sekin yaqinlashishi, lokal minimumda qolishi, overfitting yoki underfitting holatlariga olib kelishi mumkin. Genetik algoritm kabi evolyutsion usullar esa katta va diskret-uzluksiz aralash qidiruv fazosida istiqbolli kombinatsiyalarni avtomatik izlash imkonini beradi [2, 3].

Mazkur maqolaning maqsadi kriptologik ma’lumotlarni tasniflash uchun sun’iy neyron tarmog‘i parametrlarini optimallashtirish usullarini tizimlashtirish hamda genetik algoritm asosida samarali arxitektura va giperparametrlarni tanlashning konseptual modelini ishlab chiqishdan iborat.

Asosiy qism

Kriptologik ma’lumotlarni neyron tarmoq uchun tayyorlash. Tasniflash jarayonining birinchi bosqichi ma’lumotlar to‘plamini shakllantirishdan iborat. Soddalashtirilgan AES kabi tajriba modelida tasodifiy ochiq matn P va kalit K generatsiya qilinadi, so‘ng shifrlash algoritmi orqali C = E_K(P) shifrmatn olinadi. Agar P va C ning har biri 16 bitdan iborat bo‘lsa, ularni birlashtirish orqali 32 o‘lchamli kirish vektori hosil qilish mumkin:

$$X = [P_1, P_2, \ldots, P_{16}, C_1, C_2, \ldots, C_{16}].$$

Tasniflash nishoni Y sifatida kalitning alohida biti $K_j \in \{0,1\}$ olinishi mumkin. Shunda har bir kalit biti uchun masala ikkilik klassifikatsiya ko‘rinishiga keladi. Tarmoq $f_\theta(X)$ kirish vektorini qayta ishlab, 0 va 1 sinflari uchun ehtimollik bahosini beradi. Model parametrlari θ o‘qitish ma’lumotlari bo‘yicha yo‘qotish funksiyasini minimallashtirish orqali aniqlanadi:

$$\theta^* = \arg\min_\theta (1/N) \Sigma_i L(f_\theta(X_i), Y_i).$$

Ikkilik tasniflashda Binary Cross-Entropy funksiyasidan foydalanish maqsadga muvofiq. U modelning bashorat ehtimoli bilan haqiqiy sinf orasidagi tafovutni baholaydi. Kriptologik ma’lumotlarda sinflarning balanslanganligi ham alohida nazorat qilinishi kerak, chunki bir sinfning ustunligi aniqlik ko‘rsatkichini sun’iy ravishda oshirishi mumkin.

Sun’iy neyron tarmog‘i arxitekturasi. Kriptologik ma’lumotlar uchun bazaviy model sifatida to‘liq bog‘langan ko‘p qatlamli perseptron (MLP) tanlanishi mumkin. Kirish qatlami xususiyatlar soniga mos keladi, undan keyingi yashirin qatlamlar ma’lumotdagi nolinear munosabatlarni ajratib oladi. Chiqish qatlamida bitta neyron va sigmoid aktivatsiyasi ikkilik kalit biti klassifikatsiyasi uchun qulay. Yashirin qatlamlarda ReLU, PReLU yoki GELU kabi aktivatsiya funksiyalarini qiyosiy

sinash mumkin. PReLU manfiy sohada ham o‘rganiladigan kichik gradientni saqlashi bilan, GELU esa silliq nolinearligi bilan farqlanadi.

Sun’iy neyron tarmog‘ining asosiy giperparametrlari

Giperparametr	Qidiruv oralig‘i (misol)	Modelga ta’siri	Kodlash turi
Yashirin qatlamlar soni	1–5	Model murakkabligi va abstraksiya darajasi	Butun son
Neyronlar soni	32–512	Model sig‘imi	Butun son
Aktivatsiya	ReLU/PReLU/GELU	Nolinearlik va gradient oqimi	Kategorik
Learning rate	10^{-5}–10^{-2}	Yaqinlashish tezligi va barqarorligi	Haqiqiy son
Batch size	16/32/64/128	Gradient bahosi va hisoblash tezligi	Diskret
Dropout	0.0–0.5	Overfittingni cheklash	Haqiqiy son
Epoch	30–300	O‘qitish davomiyligi	Butun son
L2 koeffitsiyenti	10^{-6}–10^{-2}	Vaznlarni regularizatsiyalash	Haqiqiy son

Giperparametrlarni optimallashtirish usullari

Genetik algoritm tabiiy tanlanish tamoyillariga asoslangan populyatsion optimallashtirish usulidir. Neyron tarmoqning bitta giperparametrlar to‘plami xromosoma sifatida ifodalanadi. Dastlabki populyatsiya tasodifiy shakllantiriladi. Har bir individ bo‘yicha model qisqa yoki to‘liq o‘qitilib, validatsiya to‘plamidagi natijaga ko‘ra fitness qiymati hisoblanadi. Keyin eng istiqbolli individlar selection bosqichida tanlanadi, crossover orqali yangi avlod hosil qilinadi va mutation qidiruv fazosining yangi nuqtalarini tekshirishga yordam beradi. Nikbakht va hammualliflar GA yordamida neyron tarmoq giperparametrlarini optimallashtirishni tizimli ravishda ko‘rsatgan [2]. HyperBRKGA kabi populyatsion yondashuvlar esa qidiruv va lokal yaxshilash mexanizmlarini birlashtiradi [4].

Kriptologik masalalarda fitness funksiyasi faqat accuracy bilan cheklanmasligi maqsadga muvofiq. Masalan, F1-score, validation loss, bit bo‘yicha aniqlik va model murakkabligi birgalikda hisobga olinishi mumkin:

$$\text{Fitness} = \alpha \cdot \text{Acc} + \beta \cdot \text{F1} - \gamma \cdot \text{Loss} - \lambda \cdot \text{Complexity},$$

bu yerda α, β, γ va λ — mezonlarning nisbiy ahamiyatini belgilovchi koeffitsiyentlar. Bunday ko‘p mezonli baholash katta modelni shunchaki yuqori

accuracy sababli tanlash o‘rniga aniqlik va hisoblash xarajatlari o‘rtasida muvozanat yaratadi.

Genetik algoritm asosidagi optimallashtirish jarayoni

Taklif etilayotgan jarayon quyidagi mantiqiy bosqichlardan tashkil topadi: 1) kriptologik ma’lumotlarni generatsiya qilish va normal ko‘rinishga keltirish; 2) o‘quv, validatsiya va nazorat tanlanmalariga ajratish; 3) giperparametrlarning qidiruv fazosini belgilash; 4) boshlang‘ich populyatsiyani generatsiya qilish; 5) har bir xromosoma bo‘yicha SNT modelini qurish va o‘qitish; 6) fitnessni hisoblash; 7) selection, crossover va mutation operatorlarini bajarish; 8) yangi avlodni shakllantirish; 9) to‘xtash sharti bajarilguncha jarayonni takrorlash; 10) eng yaxshi konfiguratsiyani to‘liq o‘quv to‘plamida qayta o‘qitish va mustaqil nazorat to‘plamida baholash.

Kriptologik ma’lumotlarni shakllantirish va xususiyatlar fazosi

Kriptologik tasniflash masalasida neyron tarmoqning o‘rganish qobiliyati, avvalo, kirish ma’lumotlarining qanday shakllantirilganiga bog‘liq. Ochiq matn P, shifr kaliti K va shifrmatn C o‘rtasidagi C = E_K(P) munosabatda shifrlash algoritmi ko‘p bosqichli nolinear o‘zgartirishlarni amalga oshiradi. Shu sababli tasniflash uchun xususiyatlar vektorini faqat bitta qiymatdan emas, balki ochiq matn va shifrmatnning bitli yoki baytli ifodalarini birlashtirish orqali tuzish maqsadga muvofiq. S-AES singari soddalashtirilgan modelda bunday yondashuv nazorat qilinadigan tajriba muhitini yaratib, tarmoqning kalitga bog‘liq qonuniyatlarni qay darajada ajrata olishini tekshirish imkonini beradi.

Ma’lumotlar to‘plamini shakllantirishda har bir kuzatuv uchun yangi ochiq matn va kalit generatsiya qilinishi, shifrlash natijasi esa aynan shu kalit bilan bog‘lanishi kerak. Agar bir xil namunalar o‘quv va nazorat to‘plamlarida takrorlansa, model real kriptologik bog‘lanishni emas, ma’lumotlarning takrorlanishini o‘rganishi mumkin. Shu bois ma’lumotlarni generatsiya qilish, aralashtirish va ajratish bosqichlari neyron tarmoq arxitekturasini tanlash kabi muhim metodologik ahamiyatga ega. Zamonaviy neural cryptanalysis tadqiqotlarida katta hajmdagi maxsus generatsiya qilingan plaintext–ciphertext juftliklari va differensial juftliklardan foydalanish keng uchraydi [25, 26].

SNT arxitekturasining kriptologik tasniflashdagi xususiyatlari

Ko‘p qatlamli perseptronda har bir qatlam oldingi qatlamdan kelgan signallarni vaznlar orqali o‘zgartiradi, bias qiymatini qo‘shadi va aktivatsiya funksiyasi orqali keyingi qatlamga uzatadi. Matematik jihatdan l-qatlam chiqishi h^(l) = φ(W^(l)h^(l−1)+b^(l)) ko‘rinishida ifodalanadi. Kriptologik ma’lumotlar uchun ushbu jarayonning ahamiyati shundaki, ketma-ket qatlamlar bitlar yoki baytlar

orasidagi sodda statistik aloqalardan boshlab murakkab nolinear kombinatsiyalargacha bo‘lgan xususiyatlarni bosqichma-bosqich shakllantirishi mumkin.

Yashirin qatlamlar sonini haddan tashqari oshirish har doim ham natijani yaxshilamaydi. Kichik ma’lumotlar to‘plamida juda chuqur model ortiqcha moslashishga moyil bo‘ladi, juda sodda model esa shifrlash jarayonidagi murakkab bog‘lanishlarni ifodalash uchun yetarli sig‘imga ega bo‘lmasligi mumkin. Shu sababli qatlamlar soni va har bir qatlamdagi neyronlar soni birgalikda optimallashtirilishi kerak. AES bo‘yicha differential-neural cryptanalysis ishlarida konvolyutsion bloklar, batch normalization, ReLU va skip connectionlardan tashkil topgan chuqur arxitekturalar ham qo‘llanib, tarmoq arxitekturasining kriptografik ma’lumot formatiga moslashtirilishi muhimligi ko‘rsatilgan [26].

Giperparametrlarning o‘qitish jarayoniga ta’siri

Learning rate gradient bo‘yicha vaznlarning har bir yangilanish qadamida qanchalik o‘zgarishini belgilaydi. Juda katta qiymat minimum atrofidan sakrab o‘tishga va o‘qitishning beqarorlashishiga, juda kichik qiymat esa konvergentsiyaning keskin sekinlashishiga olib kelishi mumkin. Kriptologik ma’lumotlarda sinflar orasidagi farqlar nozik bo‘lishi mumkinligi sababli learning rate modelning foydali signallarni ajratish qobiliyatiga sezilarli ta’sir ko‘rsatadi. Ayrim AES neural-cryptanalysis tadqiqotlarida siklik yoki dinamik learning-rate jadvalidan foydalanilishi ham shu sabab bilan izohlanadi [26].

Batch size bir iteratsiyada gradientni hisoblash uchun nechta namuna ishlatilishini belgilaydi. Kichik batch gradientga ko‘proq tasodifiylik kiritadi va ba’zan modelning umumlashtirish qobiliyatini yaxshilaydi, biroq o‘qitish vaqtini oshirishi mumkin. Katta batch hisoblash resurslaridan samarali foydalanadi, ammo xotira talabini oshiradi. Epoch soni esa modelning butun o‘quv to‘plamini necha marta ko‘rishini bildiradi. Ushbu ikki parametr learning rate bilan o‘zaro bog‘liq bo‘lganligi sababli ularni mustaqil emas, umumiy konfiguratsiyaning tarkibiy qismlari sifatida optimallashtirish maqsadga muvofiq.

Dropout va L2 regularizatsiya modelning o‘quv ma’lumotlarini yodlab olish ehtimolini kamaytirishga xizmat qiladi. Dropout o‘qitish vaqtida ayrim neyronlarni vaqtincha faoliyatdan chiqaradi; L2 esa juda katta vazn qiymatlariga jarima qo‘shadi. Kriptologik tasniflashda bu mexanizmlar ayniqsa muhim, chunki model tasodifiy shovqin yoki konkret kalitlar to‘plamiga xos belgilarni asosiy qonuniyat sifatida qabul qilmasligi kerak.

Genetik algoritm yordamida qidiruv fazosini tashkil etish

Genetik algoritmda yechimlarning boshlang‘ich populyatsiyasi tasodifiy yoki oldindan belgilangan chegaralar asosida yaratiladi. Har bir individ neyron tarmoqning muayyan konfiguratsiyasini ifodalaydi. Masalan, [3, 256, GELU, 0.001, 64, 0.20] xromosomasi uchta yashirin qatlam, ma’lum neyronlar konfiguratsiyasi, GELU aktivatsiyasi, 0.001 learning rate, 64 batch size va 0.20 dropoutni ifodalashi mumkin. Shu tariqa diskret, kategorik va uzluksiz parametrlar yagona qidiruv mexanizmida birlashtiriladi.

Selection bosqichida yuqori fitnessga ega konfiguratsiyalarning keyingi avlodga o‘tish ehtimoli oshiriladi. Crossover ikki yoki undan ortiq ota-ona xromosomalarining genlarini kombinatsiyalab yangi konfiguratsiya yaratadi. Mutation esa ayrim parametrlarni tasodifiy o‘zgartirib, populyatsiyaning xilma-xilligini saqlaydi va algoritmning bitta lokal sohada qolib ketish xavfini kamaytiradi. AES(t) blok shifrlari bo‘yicha olib borilgan tadqiqotlarda ham GA populyatsiya hajmi, avlodlar soni va fitness funksiyasining tanlanishi kriptotahlil jarayoniga sezilarli ta’sir qilishi ko‘rsatilgan [27].

GAning muhim afzalligi — maqsad funksiyasidan analitik gradient talab qilmasligidir. Neyronlar soni, qatlamlar soni, aktivatsiya turi va batch size kabi turli tabiatli parametrlar birgalikda optimallashtirilishi mumkin. Biroq hisoblash xarajati populyatsiya hajmi P, avlodlar soni G va har bir modelni o‘qitish xarajati bilan ortadi. Shuning uchun amaliy tizimda qidiruv fazosini asossiz kengaytirmaslik, dastlabki avlodlarda qisqaroq o‘qitish va istiqbolli individlarni keyinchalik to‘liq o‘qitish samarali strategiya hisoblanadi.

Optimallashtirish usullarining qiyosiy xususiyatlari

Grid Search parametrlarning belgilangan qiymatlaridan hosil bo‘ladigan barcha kombinatsiyalarni tekshiradi. Ikki yoki uch parametrli kichik fazoda bu usul tushunarli va takrorlanuvchan, biroq parametrlar soni ortishi bilan hisoblashlar soni keskin ko‘payadi. Random Search esa tasodifiy nuqtalarni tekshiradi va ayrim hollarda bir xil hisoblash budjeti doirasida Grid Searchdan samaraliroq qidiruvni ta’minlaydi. Bayesian Optimization oldingi sinovlardan olingan ma’lumotlar asosida keyingi istiqbolli konfiguratsiyani tanlashga harakat qiladi. Genetik algoritm esa populyatsiya bilan ishlashi va crossover hamda mutation orqali yangi kombinatsiyalarni hosil qilishi bilan ushbu usullardan farqlanadi.

Kriptologik ma’lumotlarni tasniflashda qidiruv fazosi ko‘pincha aralash xarakterga ega: learning rate uzluksiz, batch size diskret, aktivatsiya funksiyasi kategorik, qatlamlar va neyronlar soni esa butun sonli parametrdir. Shu sababli GA kabi evolyutsion algoritm bunday fazoni tabiiy tarzda kodlash imkonini beradi. 2026-yilgi sharhda deep-learning side-channel attack modellarida batch size, epoch,

filtrlar va to‘liq bog‘langan qatlamlar kabi giperparametrlarni tizimli sozlash model ishonchliligiga bevosita ta’sir qilishi qayd etilgan [28].

Kriptologik tasniflash uchun taklif etilayotgan optimallashtirish modeli

Taklif etilayotgan modelda dastlab plaintext–ciphertext juftliklari asosida xususiyatlar vektori hosil qilinadi. Keyingi bosqichda tasniflash nishoni sifatida kalitning tegishli biti belgilanadi. Har bir bit uchun alohida ikkilik klassifikator qurish yondashuvi chiqish fazosini soddalashtiradi va qaysi kalit bitlari ma’lumotlardan yaxshiroq o‘rganilayotganini alohida tahlil qilish imkonini beradi. Modelning arxitektura va o‘qitish giperparametrlari GA xromosomasiga kodlanadi.

Optimallashtirish siklida xromosoma dekodlanib SNT modeli avtomatik yaratiladi, belgilangan o‘quv tanlanmasida o‘qitiladi va validatsiya natijasi fitness sifatida qaytariladi. Eng yaxshi individlar elitizm mexanizmi orqali saqlanib, qolgan populyatsiya selection, crossover va mutation orqali yangilanadi. To‘xtash sharti sifatida maksimal avlodlar soni, ma’lum avlodlar davomida yaxshilanish kuzatilmasligi yoki belgilangan hisoblash budjetiga erishish qo‘llanishi mumkin.

Mazkur yondashuvning metodologik ustunligi shundaki, neyron tarmoq konfiguratsiyasi tadqiqotchining subyektiv tanloviga to‘liq bog‘lanib qolmaydi. Shu bilan birga GA topgan konfiguratsiya universal optimal model deb talqin qilinmasligi kerak: uning optimal holati ma’lumotlar to‘plami, shifr varianti, kalit fazosi, random seed va qidiruv chegaralariga bog‘liq. Shuning uchun optimallashtirish natijasi aniq eksperimental sharoit doirasida talqin qilinishi zarur.

Kriptotahlilda neyron tarmoqlar va evolyutsion optimallashtirishning rivojlanish yo‘nalishlari

So‘nggi tadqiqotlar neyron tarmoqlardan faqat klassifikator sifatida emas, balki differensial distinguisher, side-channel leakage xususiyatlarini ajratuvchi model va kriptografik komponentlarni optimallashtiruvchi vosita sifatida ham foydalanilayotganini ko‘rsatmoqda. Differential-neural cryptanalysis bo‘yicha AES tadqiqotlarida neyron tarmoq shifrning differensial tarqalish xususiyatlarini o‘rganishga moslashtirilgan [26]. Boshqa ishlarda esa genetik algoritmlar AES oilasidagi blok shifrlarni tahlil qilish [27], dinamik S-boxlarni shakllantirish [29] hamda kriptografik protokollarni optimallashtirishda qo‘llanmoqda [30].

Bu tendensiya kelajakda kriptologik tahlil tizimlarini ikki darajali optimallashtirishga olib kelishi mumkin: birinchi darajada kriptografik ma’lumotlardan informativ belgilar tanlanadi, ikkinchi darajada esa ushbu belgilar bilan ishlovchi neyron tarmoq arxitekturasi va giperparametrlari evolyutsion algoritm orqali moslashtiriladi. Natijada inson tomonidan oldindan qat’iy belgilangan bitta arxitekturaga bog‘liqlik kamayib, muayyan shifr va ma’lumotlar

to‘plamiga moslashuvchi avtomatlashtirilgan kriptologik tasniflash modeli shakllanadi.

Muhokama

Xulosa

Kriptologik ma’lumotlarni sun’iy neyron tarmog‘i yordamida tasniflashda modelning yakuniy samaradorligi nafaqat o‘quv ma’lumotlari sifatiga, balki arxitektura va giperparametrlarning to‘g‘ri tanlanishiga ham bevosita bog‘liq. Yashirin qatlamlar va neyronlar soni, aktivatsiya funksiyasi, learning rate, batch size, dropout va regularizatsiya kabi parametrlar o‘zaro bog‘liq bo‘lib, ularni qo‘lda ketma-ket tanlash katta qidiruv fazosida samarasiz bo‘lishi mumkin.

Genetik algoritm turli tipdagi giperparametrlarni yagona xromosomada kodlash, istiqbolli konfiguratsiyalarni tanlash va crossover hamda mutation operatorlari orqali yangi yechimlarni izlash imkonini beradi. Shu sababli u kriptologik ma’lumotlarni tasniflash uchun SNT arxitekturasini avtomatlashtirilgan tarzda sozlashda maqsadga muvofiq usullardan biri hisoblanadi. Taklif etilgan yondashuvni S-AES yoki boshqa nazorat qilinadigan kriptografik modellar asosida tajribadan o‘tkazishda mustaqil test to‘plami, bir nechta baholash mezoni va takroriy tajribalar qo‘llanishi ilmiy ishonchlilikni oshiradi.

Foydalanilgan adabiyotlar

1. A Data Driven Cryptanalysis of S-AES using Machine Learning Technique // Procedia Computer Science. – 2026. – Vol. 283. – P. 2260–2269. – DOI: 10.1016/j.procs.2026.06.298.

2. Nikbakht S., Anitescu C., Rabczuk T. Optimizing the neural network hyperparameters utilizing genetic algorithm // Journal of Zhejiang University-SCIENCE A. – 2021. – Vol. 22, No. 6. – P. 407–426. – DOI: 10.1631/jzus.A2000384.

3. El-Hassani F.Z., Amri M., Joudar N.-E. et al. A New Optimization Model for MLP Hyperparameter Tuning: Modeling and Resolution by Real-Coded Genetic Algorithm // Neural Processing Letters. – 2024. – Vol. 56. – Article 105. – DOI: 10.1007/s11063-024-11578-0.

4. A Population-Based Hybrid Approach for Hyperparameter Optimization of Neural Networks // IEEE Access. – 2023. – Vol. 11. – P. 50752–50768. – DOI: 10.1109/ACCESS.2023.3277310.

5. Hameed F., Alkhzaimi H. Hybrid genetic algorithm and deep learning techniques for advanced side-channel attacks // Scientific Reports. – 2025. – Vol. 15. – Article 25728.

6. Leung F.F., Lam H.K., Ling S.H., Tam P.S. Tuning of the structure and parameters of a neural network using an improved genetic algorithm // IEEE Transactions on Neural Networks. – 2003. – Vol. 14, No. 1. – P. 79–88. – DOI: 10.1109/TNN.2002.804317.

7. Bashiri M., Farshbaf Geranmayeh A. Tuning the parameters of an artificial neural network using central composite design and genetic algorithm // Scientia Iranica. – 2011. – Vol. 18, No. 6. – P. 1600–1608. – DOI: 10.1016/j.scient.2011.08.031.

8. Sexton R.S., Dorsey R.E., Johnson J.D. Optimization of neural networks: A comparative analysis of the genetic algorithm and simulated annealing // European Journal of Operational Research. – 1999. – Vol. 114, No. 3. – P. 589–601. – DOI: 10.1016/S0377-2217(98)00114-3.

9. Maghrebi H., Portigliatti T., Prouff E. Breaking Cryptographic Implementations Using Deep Learning Techniques // Security, Privacy, and Applied Cryptography Engineering (SPACE 2016). – Cham: Springer, 2016. – P. 3–26.

10. Gohr A. Improving Attacks on Round-Reduced Speck32/64 Using Deep Learning // Advances in Cryptology – CRYPTO 2019. – Cham: Springer, 2019. – P. 150–179.

11. Benadjila R., Prouff E., Strullu R., Cagli E., Dumas C. Deep Learning for Side-Channel Analysis and Introduction to ASCAD Database // Journal of Cryptographic Engineering. – 2020. – Vol. 10. – P. 163–188.

12. Zhang L., Wang Z., Wang B. Improving Differential-Neural Cryptanalysis // Cryptology ePrint Archive. – 2022. – Report 2022/183.

13. Ankele R., Kölbl S. Mind the Gap – A Closer Look at the Security of Block Ciphers against Differential Cryptanalysis // Selected Areas in Cryptography – SAC 2018. – Cham: Springer, 2019. – P. 163–190.

14. Abadi M., Andersen D.G. Learning to Protect Communications with Adversarial Neural Cryptography // arXiv preprint arXiv:1610.06918. – 2016.

15. Danziger M.M., de Lima M.A., de Oliveira G.M.B. et al. Neural Networks-Based Cryptography: A Survey // IEEE Access. – 2021. – Vol. 9. – P. 124727–124740. – DOI: 10.1109/ACCESS.2021.3109635.

16. Gulli A., Pal S. Deep Learning with Keras. – Birmingham: Packt Publishing, 2017. – 318 p.

17. Goodfellow I., Bengio Y., Courville A. Deep Learning. – Cambridge, MA: MIT Press, 2016. – 800 p.

18. Bergstra J., Bengio Y. Random Search for Hyper-Parameter Optimization // Journal of Machine Learning Research. – 2012. – Vol. 13. – P. 281–305.

19. Snoek J., Larochelle H., Adams R.P. Practical Bayesian Optimization of Machine Learning Algorithms // Advances in Neural Information Processing Systems. – 2012. – Vol. 25. – P. 2951–2959.

20. Holland J.H. Adaptation in Natural and Artificial Systems. – Ann Arbor: University of Michigan Press, 1975. – 183 p.

21. Goldberg D.E. Genetic Algorithms in Search, Optimization, and Machine Learning. – Reading, MA: Addison-Wesley, 1989. – 432 p.

22. Cagli E., Dumas C., Prouff E. Convolutional Neural Networks with Data Augmentation Against Jitter-Based Countermeasures // Cryptographic Hardware and Embedded Systems – CHES 2017. – Cham: Springer, 2017. – P. 45–68.

23. Picek S., Heuser A., Jovic A., Bhasin S., Regazzoni F. The Curse of Class Imbalance and Conflicting Metrics with Machine Learning for Side-Channel Evaluations // IACR Transactions on Cryptographic Hardware and Embedded Systems. – 2019. – No. 1. – P. 209–237.

24. Perin G., Chmielewski Ł., Picek S. Strength in Numbers: Improving Generalization with Ensembles in Machine Learning-Based Profiled Side-Channel Analysis // IACR Transactions on Cryptographic Hardware and Embedded Systems. – 2020. – No. 4. – P. 337–364.

25. Gohr A. Improving Attacks on Round-Reduced Speck32/64 Using Deep Learning // Advances in Cryptology – CRYPTO 2019. – Cham: Springer, 2019. – P. 150–179.

26. Differential-Neural Cryptanalysis on AES // IEICE Transactions on Information and Systems. – 2024. – DOI: 10.1587/transinf.2024EDL8044.

27. Albarracín-Sánchez R., et al. Study of Parameters in the Genetic Algorithm for the Attack on Block Ciphers // Symmetry. – 2021. – Vol. 13, No. 5. – Article 806. – DOI: 10.3390/sym13050806.

28. Recent Advances in Deep-Learning Side-Channel Attacks on AES Implementations // Journal of Information Security and Applications. – 2026.

29. Dynamic S-boxes generation for IoT security enhancement: A genetic algorithm approach // Alexandria Engineering Journal. – 2024.

30. Singh P., Pranav P., Dutta S. Optimizing cryptographic protocols against side channel attacks using WGAN-GP and genetic algorithms // Scientific Reports. – 2025. – Vol. 15. – Article 2130. – DOI: 10.1038/s41598-025-86118-4.