G.T. KIRAKOSSIAN, A.K. MAYILYAN

IMPROVING THE BURN CLASSIFICATION SYSTEM BY A NEURAL NETWORK BY DATABASE AUGMENTATION

The method of image recognition and classification of burns by neural network is presented. The method was developed by convolutional neural network, using the Conv2D, Max Pooling, Flatten layers. The accuracy of the training and validation data was used for the model evaluation, and the Confusion Matrix and the Principal Component Analysis methods were used for dataset evaluation.

Keywords: Convolutional Neural Network, Neural layer, pixels, supervised learning.

ՀՏԴ 004.421:371.27

Հ.Ա. ՃԱՆՃԱՊԱՆՅԱՆ

ԱԴԻ ՇԱՄԻՐԻ ՇԵՄԱՅԻՆ ՍԽԵՄԱՅԻ ԱԶԴԵՑՈՒԹՅՈՒՆԸ ՔՈՄՓՅՈՒԹԵՐԱՅԻՆ ՑԱՆՑԵՐԻ ԱՐՏԱԴՐՈՂԱԿԱՆՈՒԹՅԱՆ ՎՐԱ

Քոմփյութերային ցանցերի արագագործության և անվտանգության ապահովումը կարևոր է նրանց շահագործման ընթացքում: Ադի Շամիրի (k,n) շեմային սխեման բանալիների կառավարման արդյունավետ մեթոդներից է: Այն մի կողմից՝ ապահովում է ցանցի անվտանգությունը, սակայն մյուս կողմից՝ հանգեցնում է արագագործության նվազման:

Աշխատանքում կատարված է ցանցային համակարգի արագագործության նվազման գնահատում՝ Ադի Շամիրի բանալիների կառավարման (k,n) շեմային սխեմայի կիրառման դեպքում:

Առանցքային բառեր. քոմփյութերային ցանց, արագագործություն, անվտանգություն, շեմային սխեմա, գաղտնիքի բաշխում, Լագրանժի միջարկում, արտադրողականություն:

Ներածություն: Ադի Շամիրի մեթոդով բանալու բաժանումը գաղտնագրման ալգորիթմ է, որի ժամանակ բանալին (գաղտնիքը) բաժանվում է n մասերի և բաշխվում ցանցում մասնակցող յուրաքանչյուրի մեջ: Բանալին վերականգնելու համար անհրաժեշտ է միավորել բոլոր այդ մասերը կամ դրանցից մի քանիսը: Ցանկացած k կամ ավելի շատ մասերի իմացությունը գաղտնիքը դարձնում է հեշտ հաշվելի: Ցանկացած (k-1) կամ ավելի քիչ մասերի իմացությունը գաղտնիքը թողնում է բոլորովին անորոշ այն առումով, որ դրա բոլոր հնարավոր արժեքները հավասար հավանական են [1]:

Գաղտնիքի ստացման խնդիրը լուծելու համար օգտատերը պետք է ցանցի մասնակիցներից պահանջի և ստանա գաղտնիքի (բանալու) (k-1) հատ մասեր (այդ մասերը ներկայացնում են (k-1) կարգի բազմանդամից հաշվված կետեր՝

(Xi,Yi) կոորդինատներով, դրանք այնքան են, որքան ցանցի մասնակիցները), ավելացնի իր մոտ եղած ևս մի մասը և, օգտագործելով Լագրանժի միջարկման մեթոդը, կառուցի բազմանդամ, որի ազատ անդամը բանալին է: Բանաձևը հետևյալն է [2]՝

$$f(x) = \sum_{j=0}^{k} y_j(x) l_j(x), \quad (1)$$

որտեղ Yj -ն ցանցի մասնակիցներին բաժանված կետերի օրդինատներն են, իսկ lj-երը որոշվում են հետևյալ բանաձևով.

$$l_j(x) = \prod_{j \neq i} \frac{x - xi}{xj - xi}: \quad (2)$$

Ադի Շամիրի մեթոդի մանրամասն նկարագրությունը տրված է [3], [4]-ում:

Աշխատանքի նպատակն է՝ հաշվել քոմփյութերային ցանցում այն հավելյալ ծախսվող ժամանակը, որը պայմանավորված է Ադի Շամիրի (k,n) շեմային սխեմայի կիրառումով:

Այդ ժամանակը բաղկացած է երկու բաղադրիչից, որոնցից առաջինը սխեմայի հաշվողական բարդությունն է՝աշխատատարությունը ($T_{աշխ}$,), իսկ երկրորդը՝ ցանցի մասնակիցներից գաղտնիքի մասերը հավաքելու ժամանակը ($T_{դիմել-ստանալ}$): Առաջին բաղադրիչը որոշվում է Լագրանժի միջարկման մեթոդում (1) և (2) բանաձևերում օգտագործված գործողությունների քանակով և տեսակով: Ուստի այդ բանաձևերը գրվում են բացված տեսքով և հաշվվում են դրանց մեջ պարունակվող գործողությունների քանակն ու տեսակը, ինչի իրականացման արդյունքում ստացվում է՝

$$T_{աշխ} = k\left(2(k-2)t_{բազմ} + \left(2(k-1)t_{հանում} + t_{բաժ}\right) + kt_{բազմ} + (k-1)\,t_{գում}\right), \quad (3)$$

որտեղ $t_{բազմ}$, $t_{բաժ}$, $t_{գում/հան}$ պարամետրերը ցույց են տալիս համակարգչում համապատասխան գործողությունների կատարման վրա ծախսված ժամանակները:

Եթե միջինացնենք այդ ժամանակները, այսինքն՝ բոլոր թվաբանական գործողությունների կատարման համար ընդունենք միջին ժամանակ, ապա $T_{աշխ}$,-ն համար կստանանք՝

$$T_{աշխ} =, k\left(2(k-2)t_{միջին} + \left(2(k-1)t_{միջին} + t_{միջին}\right) + kt_{միջին} + (k-1)\,t_{միջին}\right),$$

կամ պարզեցված տեսքով կլինի՝

$$T_{աշխ}, = (k(4k-3)-1)t_{միջին}: \quad (4)$$

Պետք է հաշվի առնել, որ վերը հաշվարկված ժամանակի վրա ավելանում է նաև ցանցի (k -1) մասնակիցներին դիմելու և նրանցից գաղտնիքի

մասերը ստանալու ժամանակը: Հավելյալ ծախսվող ժամանակի երկրորդ բաղադրիչի մեջ մտնում է հենց այդ ժամանակը: Նկատենք,, որ գաղտնիքի վերականգնման համար անհրաժեշտ k մասերից մեկը գտնվում է տվյալ մասնակցի մոտ, որը ի սկզբանե բաժանված է լինում ցանցի բոլոր մասնակիցներին վարողի կողմից:

Վերը բերված դատողություններից ելնելով՝ ժամանակը, որը ծախսվում է Շամիրի մեթոդի վրա գաղտնիքը վերականգնելու համար, կլինի՝

$$T_{Շամիր}, = T_{աշխ}, + (k - 1)\ t_{դիմել-ստանալ}, \quad (5)$$

որտեղ երկրորդ բաղադրիչի առկայությունը պայմանավորված է (k -1) մասնակիցներից գաղտնիքի մասերի ստացումով:

Տեղադրենք $T_{աշխ}$,-ն արժեքը (4) բանաձևից (5)-ի մեջ, կստանանք՝

$$T_{Շամիր} = ((4k - 3)\ k - 1)t_{միջին} + (k - 1)\ t_{դիմել-ստանալ}: \quad (6)$$

Ստացանք Ադի Շամիրի մեթոդի օգտագործման դեպքում հավելյալ ծախսված ժամանակի գնահատման բանաձևը:

Ինչպես երևում է (6) բանաձևից, աշխատատարության կախվածությունը k-ից ունի քառակուսային բնույթ: Ցանցի անվտանգության ապահովման աստիճանի տրված լինելու դեպքում կարելի է որոշել k-ն, իսկ վերջինիս արժեքը տեղադրելով (6)-ի մեջ՝ ժամանակի մեծացման (արագագործության նվազման) չափը:

Նկատենք, որ եթե բանալին պահվում է օգտագործողի մոտ, ապա երկրորդ բաղադրիչի ազդեցությունը ցանցի արագագործության իջեցման վրա նվազում է:

Եթե հաշվի առնենք որևէ մեթոդով գաղտնագրման {5] [ու փոխանցման ժամանակները, ապա փաթեթի նախապատրաստման և փոխանցման համար ծախսվող ընդհանուր ժամանակը՝ ($T_{Շամիր-փոխ}$), կլինի՝

$$T_{Շամիր-փոխ} = ((4k - 3)\ k - 1)t_{միջին} + (k - 1)\ t_{դիմել-ստանալ} + T_{գաղտն} + T_{փոխանցում}: \quad (7)$$

Ադի Շամիրի սխեմայում գործում են հետևյալ պայմանները՝ k>=2; k<= n;

k=1-ի դեպքում $T_{աշխ}$, և $T_{Շամիր}$, ժամանակները հավասարվում են զրոյի, այսինքն մեթոդը չի կիրառվում, և ունենք միայն գաղտնագրում ու փոխանցում՝ առանց Ադի Շամիրի մեթոդի օգտագործման: Այսինքն՝

$$T_{փոխ-առանց-Շամիր} = T_{գաղտն} + T_{փոխանցում}: \quad (8)$$

Նշանակենք R -ով համակարգի արագագործության իջեցման գործակիցը (դա նույնն է, ինչ ծախսվող ժամանակի մեծացման հակադարձը) և համեմատենք առանց Շամիրի մեթոդի գաղտնագրված տվյալների փոխանցման հետ՝ կազմելով դրանց հարաբերությունը:

$$R= T_{Շամիր-փոխ}/ T_{փոխ-առանց-Շամիր}; \quad (9)$$

Տեղադրենք $T_{Շամիր-փոխ}$ և $T_{փոխ-առանց-Շամիր}$ արժեքները համապատասխանաբար (7) և (8) բանաձևերից (9)-ի մեջ, կստանանք՝

$$R=(((4k-3)\,k-1)t_{միջին}+(k-1)\,t_{դիմել-ստա}+T_{գաղտն}+T_{փոխանցում})/(T_{գաղտն}+T_{փոխանցում}),$$

կամ՝

$$R= 1 +(((4k-3)\,k-1)t_{միջին}+(k-1)\,t_{դիմել-ստանալ})/(T_{գաղտն}+T_{փոխանցում}): \quad (10)$$

Եզրակացություն: Ստացված (10) բանաձևից հետևում է, որ k -ի մեծացման արդյունքում ցանցի աշխատանքի ժամանակը ավելանում է R անգամ /կամ որ նույնն է՝ արտադրողականությունը նվազում է 1/R անգամ: R-ը մեկից մեծ մեծություն է: Շամիրի մեթոդը չկիրառելու դեպգում, այսինքն, երբ k=1, R-ը ևս հավասար է մեկի, և չկա ազդեցություն:

Հարկ է նշել, որ մյուս կողմից՝ k--ի մեծացման արդյունքում բարձրանում է ցանցի աշխատանքի անվտանգության աստիճանը, իսկ դա նշանակում է, որ առաջանում է k -ի օպտիմալ արժեքի որոշման խնդիր, որն այս հոդվածի շրջանակում չի դիտարկվում:

ԳՐԱԿԱՆՈՒԹՅԱՆ ՑԱՆԿ

1. **Shamir Adi** “How to share a secret” // Communications of the ACM22.- 1979.-11-P.612-613.
2. https://en.wikipedia.org/wiki/Lagrange_polynomial
3. https://ru.wikipedia.org/wiki//Схема разделения секрета Шамира.
4. **Ճանճապանյան Հ.Ա., Մաթևոսյան Կ.Ա.** Համակարգչային տեղեկատվության պաշտպանության մեթոդներ և միջոցներ. Լաբորատոր աշխատանքների մեթոդական ցուցումներ.-Երևան, 2011:
5. http://www.garykessler.net/library/crypto.html, Обзор криптографии.- 2016.

А.А. ДЖАНДЖАПАНЯН

ВЛИЯНИЕ ПОРОГОВОЙ СХЕМЫ ADI SHAMIR НА ПРОИЗВОДИТЕЛЬНОСТЬ КОМПЬЮТЕРНОЙ СЕТИ

При эксплуатации компьютерных сетей важное значение имеет обеспечение скорости и безопасности. Пороговая схема Adi Shamir (k, n) входит в число эффективных методов управления ключами. С одной стороны, это обеспечивает безопасность сети, с другой - снижает производительность. В статье произведена оценка снижения производительности компьютерной сети при применении пороговой схемы (k, n) Adi Shamir.

***Ключевые слова*:** компьютерная сеть, скорость, безопасность, пороговая схема, распределение секрета, интерполяция Лагранжа, производительность.

A.A. TSHATSHAPANYAN

THE IMPACT OF ADI SHAMIR THRESHOLD SCHEME ON COMPUTER NETWORK PRODUCTIVITY

Ensuring the speed and security of computer networks is important during their operation. Adi Shamir (k, n) threshold scheme is among the effective key management methods. On the one hand, it ensures network security, on the other hand, it reduces performance. The artikle includes an estimation of the decrease in the performance of the computer network when applying the of Adi Shamir key management (k,n)threshold scheme.

Keywords: computer network, speed, security.threshold scheme, secret distribution, Lagrange Interpolation,performance.

ՀՏԴ 371.214

Գ.Ա. ՀԱՐՈՒԹՅՈՒՆՅԱՆ, Է.Հ. ՀՈՎՀԱՆՆԻՍՅԱՆ

ԳԻՏԵԼԻՔՆԵՐԻ ՍՏՈՒԳՄԱՆ ԱՎՏՈՄԱՏԱՑՎԱԾ ՀԱՄԱԿԱՐԳՈՒՄ ՊԱՏԱՍԽԱՆՆԵՐԻ ՃՇՏՈՒԹՅԱՆ ԱՍՏԻՃԱՆԻ ՈՐՈՇՈՒՄԸ

Ուսումնասիրվել են ավտոմատացված ուսուցման համակարգերում սովորողների պատասխանների դիֆերենցիալ գնահատման խնդիրները, իրականացվել է տեքստային հարցերի ներկայացման տարբեր ձևերի և համապատասխանաբար պատասխանների վերլուծություն: Առաջարկվում են գործնականում իրագործելի մեթոդներ՝ պատասխանների ճշգրտությունը որոշելու համար, որոնք կախված չեն հարցերի սեմանտիկ կառուցվածքից և թույլ են տալիս կատարել դիֆերենցված գնահատում:

Առանցքային բառեր. ուսուցման ավտոմատացված համակարգ, գիտելիքների վերահսկման համակարգ, թեստավորում, բազմություն, ցուցակ, նմանության աստիճան:

Ներածություն: Կրթական գործընթացի հիմքը ուսումնական համակարգերի օգտագործման ժամանակ սովորողի ինքնավերահսկվող ինքնուրույն աշխատանքն է:

Գիտելիքների վերահսկման ավտոմատացված համակարգերում սովորաբար օգտագործվում են գիտելիքների վերահսկման կազմակերպման 2 հիմնական մոտեցումներ.

1.Սովորողի գործողությունների գնահատում [1]: Այս մեթոդը կիրառվում է փորձագիտական համակարգերում, այսինքն՝ այն համակարգերում, որոնք հիմնված են գիտելիքների վրա: Առարկայական ոլորտի վերաբերյալ գիտելիքները և սովորողի գործողությունների գնահատման կանոնները թույլ են տալիս երկխոսության ընթացքում որոշել սովորողի գիտելիքների մակարդակը [2]: