ՀՀ ԳԱԱ ԻՆՖՈՐՄԱՏԻԿԱՅԻ ԵՎ ԱՎՏՈՄԱՏԱՑՄԱՆ ՊՐՈԲԼԵՄՆԵՐԻ ԻՆՍՏԻՏՈՒՏ

Չիդեմյան Սերգեյ Սերգեյի

ՁԵՌՔԻ ԱՓԻ ԵՐԱԿՆԵՐԻ ՑԱՆՑԻ ՎՐԱ ՀԻՄՆՎԱԾ ԿԵՆՍԱՉԱՓԱԿԱՆ ԳԱՂՏՆԱԳՐՄԱՆ ՀԱՄԱԿԱՐԳԻ ՄՇԱԿՈՒՄ

Ե.13.05 «Մաթեմատիկական մոդելավորում, թվային մեթոդներ և ծրագրերի համալիրներ» մասնագիտությամբ տեխնիկական գիտությունների թեկնածուի գիտական աստիճանի հայցման ատենախոսության

ՍԵՂՄԱԳԻՐ

Երևան – 2015

ИНСТИТУТ ПРОБЛЕМ ИНФОРМАТИКИ И АВТОМАТИЗАЦИИ НАН РА

Чидемян Сергей Сергеевич

РАЗРАБОТКА БИОМЕТРИЧЕСКОЙ КРИПТОСИСТЕМЫ, ОСНОВАННОЙ НА ВЕНАХ ЛАДОНИ

АВТОРЕФЕРАТ

диссертации на соискание ученой степени кандидата технических наук по специальности 05.13.05 - “Математическое моделирование, численные методы и комплексы программ”

Ереван – 2015

Ատենախոսության թեման հաստատվել է ՀՀ ԳԱԱ Ինֆորմատիկայի և ավտոմատացման պրոբլեմների ինստիտուտում

Գիտական ղեկավար՝	տեխ.գիտ. դոկտոր	Գ.Հ. Խաչատրյան
Պաշտոնական ընդդիմախոսներ՝	ֆիզ.մաթ.գիտ.դոկտոր	Լ.Հ.Ասլանյան
	ֆիզ.մաթ.գիտ.թեկնածու	Ս.Ե.Աբրահամյան

Առաջատար կազմակերպություն՝ Հայաստանի պետական ճարտարագիտական համալսարան

Պաշտպանությունը կայանալու է 2015թ. հունիսի 18-ին, ժ. 16.00-ին ՀՀ ԳԱԱ Ինֆորմատիկայի և ավտոմատացման պրոբլեմների ինստիտուտում գործող 037 «Ինֆորմատիկա և հաշվողական համակարգեր» մասնագիտական խորհրդի նիստում հետևյալ հասցեով՝ Երևան, 0014, Պ. Սևակի 1:

Ատենախոսությանը կարելի է ծանոթանալ ՀՀ ԳԱԱ ԻԱՊԻ գրադարանում:

Սեղմագիրը առաքված է 2015թ. Մայիսի 18-ին:

Մասնագիտական խորհրդի գիտական քարտուղար, ֆիզ.մաթ.գիտ.դոկտոր Հ. Գ. Սարուխանյան

Тема диссертации утверждена в Институте проблем информатики и автоматизации НАН РА

Научный руководитель:	доктор тех. наук	Г.Г. Хачатрян
Официальные оппоненты:	доктор физ.-мат. наук	Л.А. Асланян
	кандидат физ.-мат. наук	С.Е. Абраамян

Ведущая организация: Государственный инженерный университет Армении

Защита состоится 18-го июня 2015г. в 16.00 на заседании специализированного совета 037 «Информатика и вычислительные системы» Института проблем информатики и автоматизации НАН РА по адресу: 0014, г. Ереван, ул. П. Севака 1.

С диссертацией можно ознакомиться в библиотеке ИПИА НАН РА.
Автореферат разослан 18-го мая 2015г.

Ученый секретарь специализированного совета, д.ф.м.н. А. Г. Саруханян

ԱՇԽԱՏԱՆՔԻ ԸՆԴՀԱՆՈՒՐ ԲՆՈՒԹԱԳԻՐԸ

Թեմայի արդիականությունը

Մեր օրերում անձը նույնականացնելու խնդիրը դառնում է ավելի ու ավելի կարևոր, բայց միևնույն ժամանակ ավելի բարդ մեր անընդհատ շարժման մեջ գտնվող և չափազանց փոխկապակցված հասարակության պարագայում: Սովորաբար անձի նույնականացման խնդիրը լուծելու համար օգտագործվում են նրան բնութագրող մի շարք հատկություններ, որոնցից մեկը կենսաչափական տվյալներն են:

Կենսաչափական տվյալների օգտագործումը դիտարկվում է որպես առանցքային լուծում անվտանգության և նույնականացման բազմաթիվ խնդիրների համար: Նույնականացման խնդիրը լուծելու համար օգտագործվող յուրաքանչյուր կենսաչափական բնութագիր ունի իր դրական և բացասական կողմերը: Մասնավորապես, ամենատարածված կենսաչափական բնութագիրը՝ մատնահետքն ունի մի ակնհայտ թերություն. այն հնարավոր է պատճենել: Բացի այդ, գոյություն ունեն արհեստական մատնահետքեր ստանալու բազմաթիվ եղանակներ[1]: Նմանատիպ վտանգներից խուսափելու համար ճապոնական «Fujitsu»-ի կողմից առաջարկվել է ձեռքի ափի երակների վրա հիմնված նույնականացման տեխնոլոգիան[2]: Այս բնութագիրը համարվում է ամենախոստումնալիցներից և ամենաանվտանգներից մեկը:

Կենսաչափական բնութագրերի վրա հիմնված նույնականացումը համընդհանուր տարածված մեխանիզմ է, սակայն այս տեխնոլոգիան պահանջում է կենսաչափական տվյալների պահպանում, որը բավականին մեծ թերություն է: Կենսաչափական տվյալների պահպանումը կարող է բերել ինֆորմացիայի արտահոսքի կամ անձնական տվյալների գողությանը: Դա կարող է առաջացնել խնդիրներ, քանի որ կենսաչափական բնութագրերը հատուկ են տվյալ անձին, և դրանց կորստի դեպքում այն հնարավոր չէ փոխարինել: Կենսաչափական շաբլոնների պաշտպանության սխեմաներն, որոնցում գաղտնագրության մեխանիզմները համատեղած են կենսաչափական բնութագրերի հետ, դիտարկվում են որպես խոստումնալից լուծում վերոհիշյալ խնդիրների համար:

Արդյունքում պարզ է դառնում այնպիսի մի կենսաչափական գաղտնագրման համակարգի մշակման անհրաժեշտություն, որն ապահովում է բարձր անվտանգությունը, հնարավորինս ճշգրիտ է, կիրառելի է օգտագործողի կողմից և, ինչը շատ կարևոր է, նման համակարգի կիրառմամբ լուծվում է պատճենելով գողանալու հետ կապված խնդիրները:

---

[1] Sandstrom M. “Liveness Detection in Fingerprint Recognition Systems”, Department of Electrical Engineering, Linkoping Institute of Technology,Institutionen for systemteknik, Linkoping, 2004.

[2] Fujitsu Develops Technology for World's First Contactless Palm Vein Pattern Biometric Authentication System. Tokyo, URL: http://pr.fujitsu.com/en/news/2003/03/31.html, 2003.

Աշխատանքի նպատակը

Աշխատանքի նպատակն է մշակել գաղտնագրման այնպիսի մի համակարգ, որը հիմնված կլինի ձեռքի ափի երակների ցանցից առանձնացված բնութագրերի վրա և կապահովի բարձր անվտանգություն: Այդ համակարգը պետք է լինի հնարավորինս ճշգրիտ և հնարավորություն ընձեռնի լուծել նաև կենսաչափական բնութագրերի պատճենելու խնդիրը, որն առկա է, մասնավորապես, մատնահետքի վրա հիմնված համակարգերում: Միևնույն ժամանակ ցանկալի է, որ այդ համակարգը հարմար լինի օգտագործողի տեսակետից և մրցունակ նմանատիպ այլ համակարգերի հետ:

Հետազոտման մեթոդները

Աշխատանքում օգտագործված են պատկերների մշակման թվային մեթոդները, կենսաչափական նույնականացման, կենսաչափական շաբլոնի պաշտպանության, բանալու կցմամբ գաղտնագրման համակարգերի անվտանգության վերլուծության մեթոդները:

Գիտական նորույթը

- Առաջարկվել է ձեռքի ափի երակների պատկերներից բնութագրերի առանձնացման տարբեր մեխանիզմների համադրմամբ նոր մեխանիզմը:
- Ձեռքի ափի երակների ցանցից առանձնացված բնութագրերի հիման վրա մշակվել է գաղտնագրման համակարգ և վերլուծվել են նրա անվտանգության և ճշգրտության հատկությունները:
- Ձեռքի ափի երակների ցանցից և մատնահետքերից առանձնացված բնութագրերի հիման վրա մշակվել է բազմակենսաչափական գաղտնագրման համակարգ և ուսումնասիրվել են նրա անվտանգության և ճշգրտության հատկությունները:

Ստացված արդյունքների կիրառական նշանակությունը

Ստացված արդյունքների հիման վրա մշակվել է ձեռքի ափի երակների վրա հիմնված նույնականացման և կենսաչափական շաբլոնը պաշտպանելու հնարավորություն ընձեռնող համակարգ, որն ունի բարձր կիրառական ճշգրտություն: Հաշվի առնելով, որ նրա հիմքում ընկած է օգտագործողների նույնականացման ոչ կոնտակտային տեխնոլոգիան, այն կարող է լայն տարածում ստանալ այնպիսի տեղերում, որտեղ հիգիենայի հետ կապված հարցերը կանգնած են բավականին սուր, օրինակ՝ բուժհաստատություններում՝ հիվանդների անձնական տվյալներին հասանելիություն ստանալու համար: Բացի այդ, այն հնարավոր է օգտագործել. ա) բանկային ոլորտում՝ ֆինանսական գործարքները կատարելիս, բ) ուսումնական հաստատություններում՝ ուսումնական համակարգ մուտք գործելու իրավասությունները ստուգելիս, գ) օդանավակայաններում՝ ուղևորների ինքնությունը պարզելու համար, և այլն:

Աշխատանքի արդյունքների հավաստիությունը հիմնավորվում է մշակված ծրագրային համակարգի կիրառմամբ ստացված մի շարք փորձնական արդյունքներով:

Աշխատանքի արդյունքների ներդրումը

Մշակված ձեռքի ափի երակների ցանցի վրա հիմնված համակարգը փորձարկվել է «Հայկական Ծրագրեր» Ընկերության ուսումնական կենտրոնում: Համապատասխան համակարգով կատարվել է ուսանողների կողմից ուսումնական համակարգ մուտք գործելու իրավասությունների ստուգում:

Պաշտպանությանը ներկայացվող դրույթները.

1. Ձեռքի ափի երակների պատկերներից բնութագրերի առանձնացման տարբեր մեխանիզմների համադրմամբ նոր մոտեցում
2. Ձեռքի ափի երակների ցանցից առանձնացված բնութագրերի հիման վրա գաղտնագրման համակարգի մշակում
3. Ձեռքի ափի երակների ցանցից և մատնահետքերից առանձնացված բնութագրերի հիման վրա բազմակենսաչափական գաղտնագրման համակարգի մշակում
4. Ձեռքի ափի երակների ցանցից առանձնացված բնութագրերի հիման վրա գաղտնագրման համակարգի ծրագրային իրականացում

Աշխատանքի արդյունքները զեկուցվել են. Հայ-Ռուսական (Սլավոնական) Համալսարանի տարեկան գիտական ժողովների ընթացքում (2013-2014 թթ., ք. Երևան), Հայկական մաթեմատիկական միության նստաշրջանի ժամանակ (2014 թ., ք.Երևան), ՀՀ ԳԱԱ ինֆորմատիկայի և ավտոմատացման պրոբլեմների ինստիտուտի ընդհանուր սեմինարում:

Հրատարակումներ: Ատենախոսության հիմնական արդյունքները տպագրված են 4 գիտական աշխատություններում, որոնք թվարկված են սեղմագրի վերջում:

Աշխատանքի կառուցվածքը և ծավալը: Ատենախոսությունը բաղկացած է ներածությունից, 4 գլուխներից, եզրակացությունից և օգտագործված գրականության ցանկից: Աշխատանքի ընդհանուր ծավալն է 140 էջ՝ ներառյալ 60 նկար, 122 անուն՝ օգտագործված գրականության ցանկում:

ԱՇԽԱՏԱՆՔԻ ԲՈՎԱՆԴԱԿՈՒԹՅՈՒՆԸ

Ներածության մեջ հիմնավորված են թեմայի արդիականությունը, ձևակերպված են աշխատանքի նպատակները, գիտական նորույթները և հիմնական դրույթները, որոնք ներկայացված են պաշտպանությանը:

Ատենախոսության **առաջին գլխում** նկարագրվել են կենսաչափական համակարգերում օգտագործվող բնութագրերը՝ այդ թվում ձեռքի ափի երակների ցանցից առանձնացված բնութագրերը: Բերվել են նրանց գնահատականները հետևյալ կարևոր հատկությունների տեսակետից՝

1. **Համընդհանրություն (Universality)**՝ արդյո՞ք բոլոր մարդիկ ունեն այդ բնութագիրը:

2. **Տարբերականություն (Distinctiveness)**՝ հնարավո՞ր է տարբերակել մարդկանց այդ բնութագրի հիման վրա:
3. **Մշտականություն (Permanence)**՝ որքա՞ն անփոփոխ է ժամանակի ընթացքում տվյալ բնութագիրը:
4. **Հավաքելիություն (Collectability)**՝ ի՞նչ հեշտությամբ և որքա՞ն հատկանիշներ է հնարավոր առանձնացնել այդ բնութագրերից:
5. **Արտադրողականություն (Performance)**՝ տվյալ կենսաչափական բնութագրի վրա հիմնված համակարգի արագությունն ու ճշգրտությունը:
6. **Ընդունելիություն (Acceptability)**՝ մարդկանց պատրաստակամությունը տվյալ կենսաչափական բնութագրի վրա հիմնված համակարգն օգտագործելու:
7. **Հուսալիություն (Foolproof)**՝ տվյալ կենսաչափական բնութագրի վրա հիմնված համակարգի հուսալիությունը:

Ցույց է տրվել, որ ձեռքի ափի երակները իրենցից ներկայացնում են լավ կենսաչափական բնութագիր այդ 7 հատկությունների տեսակետից, և, ինչը շատ կարևոր է համակարգի կառուցման տեսակետից, այդ բնութագիրը ունի բարձր արտադրողականության և հուսալիության գնահատականներ:

Դիտարկվել են կենսաչափական համակարգերի խոցելիության հարցերը, բերվել են խոցելիության հիմնական պատճառները: Ամենամեծ վնաս հասցնող շաբլոնների հենքի վրա հարձակմանը դիմադրելու համար դիտարկվել են կենսաչափական շաբլոնի պաշտպանության սխեմաները: Նկարագրվել են կենսաչափական գաղտնագրման համակարգերի անվտանգության և ճշգրտության հիմնական հատկանիշները: Բացի այդ դիտարկվել են մեկից ավելի կենսաչափական բնութագրերի վրա հիմնված համակարգերի նախագծման հարցերը, ուսումնասիրվել բազմակենսաչափական շաբլոնի պաշտպանության խնդիրները:

Գլխի վերջում, կատարված հետազոտությունների հիման վրա, ձևավորվել են կենսաչափական գաղտնագրման համակարգերում առկա խնդիրները և աշխատանքի նպատակը:

Երկրորդ գլխում ներկայացված է ձեռքի ափի երակների հիման վրա նույնականացում իրականացնելու մոտեցումը: Մոտեցումը փորձարկելու համար անհրաժեշտ է անցնել հետևյալ չորս փուլերը՝

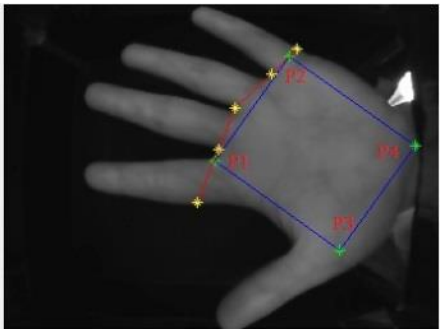
- Ձեռքի ափի երակների պատկերների հավաքում
- Պատկերների որակի բարելավում
- Ձեռքի ափի պատկերներից երակների ցանցի առանձնացում
- Բնութագրերի առաձնացում (մինուցիաներ և այլն)

Ձեռքի ափի երակների պատկերների հավաքման փուլում օգտագործվել է բաց հասանելիության մեջ գտնվող CASIA հենքը[3]:

[3] http://biometrics.idealtest.org/dbDetailForUser.do?id=5.

Ձեռքի պատկերների բարելավման փուլը բաղկացած է երկու մասերից՝ ձեռքից մեզ հետաքրքրող ուղղանկյունաձև մասի առանձնացումից (Region of Interest segmentation) և ինֆրակարմիրին մոտ լույսով արված պատկերների որակի բարելավումից:

Երակների գտնվելու մասի առանձնացման քայլի հիմնական նպատակն է ձեռքի պատկերից առանձնացնել ուղղանկյունաձև կտոր, որտեղ գտնվում է երակների կառուցվածքի մեծ մասը:



Նկար 1: Ձեռքի ափից առանձնացված ուղղանկյունաձև կտոր:

Այս մասի առանձնացման ժամանակ ծագող խնդիրներից կարևորագույնն է, թե ինչպես փոփոխության ենթարկել նկարը այնպես, որ օգտագործողի և սարքի միջև փոխազդեցության ժամանակ առաջացած աղավաղումները, մասնավորապես, ձեռքը սարքի նկատմամբ պտտելու հետ կապված խնդիրները, նվազեցվեն: Այս խնդիրները լուծելու համար օգտագործվել է մոտեցում, ըստ որի անհրաժեշտ է առանձնացնել երկու կետեր՝ ցուցամատի և միջամատի միջև կետը մատանեմատի և ճկույթի միջև կետի հետ միասին (Նկ.1): Այս կերպ առանձնացված ուղղանկյունաձև կտորը ապահովում է, որ տարբեր փորձերի ժամանակ առանձնացված կտորները կհամապատասխանեն ձեռքի նույն մասին և կապված չեն լինի ձեռքի չափերի հետ:

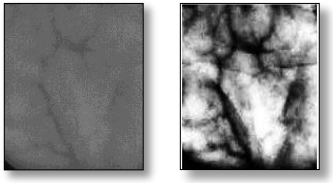
Ձեռքի նկարները արված են ինֆրակարմիրին մոտ լուսավորության ներքո, ինչը ազդում է նրանց որակի վրա: Մասնավորապես, այդ նկարները մութ են, ցածր ցայտագունությամբ և ունեն որակի լավացման կարիք: Նկարի որակի լավացման նպատակով օգտագործվել է նկարների մշակման 5×5 միջինացման ֆիլտրը (median filter), որի միջոցով նկարը մաքրվում է բծիկավոր աղմուկից: Բարձր հաճախականության աղմուկի խնդիրը լուծելու համար օգտագործվել է 10×10 Վիների ֆիլտրը: Բարձր հաճախականության աղմուկը հեռացնելուց հետո՝ օգտագործվել է աղմուկ հեռացնող վերջին ֆիլտրը՝ անիզոտրոպիկ ցրման ֆիլտրը (anisotropic diffusion):

Դիցուք՝ $\Omega \subset \mathbb{R}^2$ հարթությունների ենթաբազմություն է և $I(.,t): \Omega \to \mathbb{R}$ իրական պատկերի մոխրագույն ներկայացումների (grayscale) ընտանիք է: Անիզոտրոպիկ ցրումը այդ դեպքում կարելի է ներկայացնել հետևյալ կերպ.

$$\frac{\partial I}{\partial t} = div(c(x,y,t)\nabla I) = \nabla c \nabla I + c(x,y,t)\Delta I \qquad (1)$$

որտեղ Δ-ով նշված է Լապլասի օպերատորը, ∇-ով նշված է գրադիենտը, իսկ *div(…)*-ով՝ դիվերգենցիայի օպերատորը: *c(x,y,t)*՝ ցրման գործակից է և հաճախակի ընտրվում է

որպես պատկերի գրադիենտի ֆունկցիա: Որպես ցրման գործակից օգտագործվել է հետևյալ ֆունկցիան՝ $c(\|\nabla I\|) = e^{-(\frac{\|\nabla I\|}{K})^2}$, որտեղ K հաստատունը որոշում է պատկերի սահմանի նկատմամբ զգայունությունը: Փորձերի արդյունքում ընտրվեց $K = 20$ արժեքը: Նկարի ցայտագունությունը լավացնելու համար կատարվել է նկարի հիստոգրամի հավասարեցումը: Առաջարկված մոտեցումների կիրառման արդյունքում պատկերների որակը էականորեն բարելավվել է (Նկ. 2):



Նկար 2: Առանձնացված ուղղանկյունաձև մասը որակի բարելավումից առաջ և հետո:

Ձեռքի ափի պատկերներից երակների առանձնացման փուլը բաղկացած է երկու մասից՝ երակների որակի բազմաչափ բարելավումից[4] (multiscale vessel enhancement) և գլոբալ նվազմամբ լոկալ բինարիզացիայից (local thresholding with global reduction):

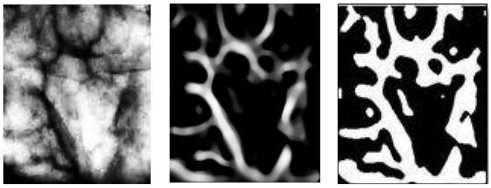
Հավաքման փուլում ընտրված հենքի ուսումնասիրման արդյունքում պարզ է դարձել, որ երակների կառուցվածքը բարելավված պատկերներից առանձնացնելու համար կարելի է օգտագործել երակների *բազմաչափ բարելավման սխեման*: Մասնավորապես, ըստ այդ մեթոդի՝ երակների առանձնացումը դիտարկվում է որպես ֆիլտրման ընթացքում գլանային երկրաչափական կառուցվածքների փնտրում:

Երակների կառուցվածքի ավելի հստակ ներկայացում ստանալու համար, անհրաժեշտ է առանձնացնել այն պատկերի ֆոնից: Ստացված պատկերների վերլուծության արդյունքում պարզ դարձավ, որ հայտնի բինարիզացիայի ալգորիթմները ցանկալի արդյունք չեն տալիս: Ի նկատի ունենալով վերոհիշյալը որոշեցինք օգտագործել գլոբալ նվազմամբ լոկալ բինարիզացիայի ալգորիթմը (local thresholding with global reduction): Այս ալգորիթմը պատկանում է հարմարեցվող (adaptive) ալգորիթմների շարքին, որն իրենից ներկայացնում է լոկալ և գլոբալ բինարիզացիայի համադրումը: Ալգորիթմը որոշում է պատկերի յուրաքանչյուր պիքսելի համար տարբեր արժեքներ՝ կախված այդ պիքսելի հարևան պիքսելների արժեքներից՝

$$BinarizedImage(i,j) = \begin{cases} 1, & \text{եթե } Image(i,j) \geq \mu_{i,j} - T \\ 0, & \text{հակառակ դեպքում} \end{cases} \quad (2)$$

որտեղ $\mu_{i,j}$-ն (i,j) պիքսելի $N \times N$ շրջակայքում գտնվող պիքսելների արժեքների միջինն է, իսկ T-ն՝ ընդհանուր շեղումն է: Պատկերների հենքի վերլուծության արդյունքում որոշվել է N-ի և T-ի արժեքները ընդունել համապատասխանաբար 10 և 6:

[4] A. F. Frangi, W. J. Niessen, K. L. Vincken, and M. A. Viergever, *"Multiscale vessel enhancement filtering"*, MICCAI, Springer, LNCS 1496, pp. 130-137, 1998.



(ա) (բ) (գ)

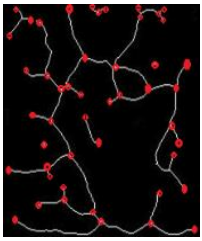
Նկար 3: (ա) բարելավված որակով պատկեր, **(բ)** պատկերը երակների բազմաչափ բարելավման սխեման կիրառելուց հետո, **(գ)** պատկերը գլոբալ նվազմամբ լոկալ բինարիզացիայի ալգորիթմը կիրառելուց հետո:

Նկար 3-ում պատկերված է երակների բազմաչափ բարելավման սխեմայի կիրառման արդյունքում ստացված պատկերն ու գլոբալ նվազմամբ լոկալ բինարիզացիայի ալգորիթմի կիրառման արդյունքը:

Ձեռքի ափի երակներից բնութագրերի առաձնացման փուլը բաղկացած է երկու մասից՝ կմախքացումից (skeletonization) և մինուցիաների առաձնացումից:

Երակների բինարիզացված պատկերներից բնութագրերի առաձնացման համար, նախ անհրաժեշտ է կատարել երակների կմախքացումը: Կմախքացումն իրենից ներկայացնում է երակների կառուցվածքի լայնքի նեղացումը մինչ մեկ պիքսել:

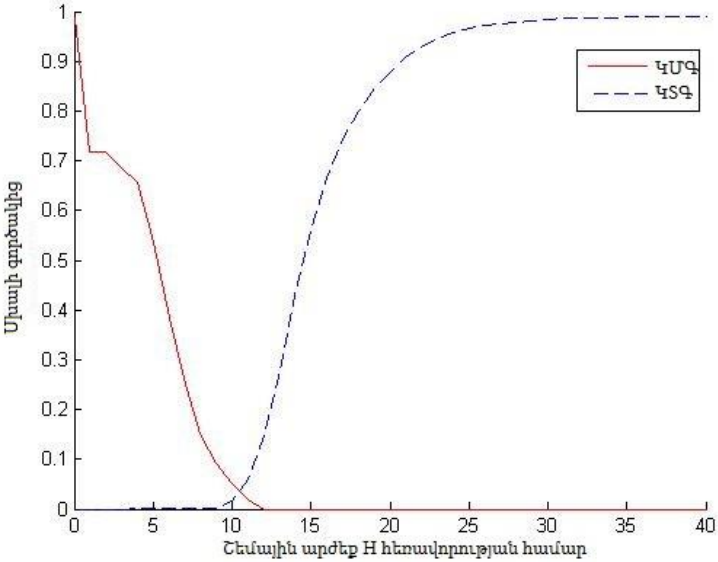
Ձեռքի ափի երակները կարող են ներկայացվել որոշ կետերի միջոցով, որոնց անվանում են մինուցիաներ: Այդպիսի կետերից են ձեռքի ափի երակների կառուցվածքի կմախքային ներկայացման մեջ ճյուղավորման և եզրային կետերն են: Որպես եզրային կետեր այստեղ դիտարկվում են երակների այն եզրային կետերն, որոնք հայտնվել են ձեռքի ափի հետաքրքրող մասի (region of interest) առանձնացման արդյունքում ստացված պատկերի մեջ: Չնայած, որ դրանք ձեռքի ափի երակների իրական եզրային կետերը չեն, նրանց անտեսել չի կարելի, քանի որ նրանք պարունակում են երակների կառուցվածքի մասին երկրաչափական որոշ ինֆորմացիա: Որպես ճյուղավորման կետեր դիտարկվում են երեք կորերի միացման կետերը (Նկ.4):



Նկար 4: Ձեռքի ափի երակներից առանձնացվող մինուցիաների կետեր:

CASIA հենքի վրա մեր փորձերի արդյունքում ստացվել է, որ մարդու ձեռքի ափի երակներից կարելի է առաձնացնել միջինը 25 մինուցիաներ, այդ թվում՝ 10 ճյուղավորման կետ և 15 եզրային կետ: Այս կետերի քանակը բավական է անձի նույնականացումն իրականացնելու համար, սակայն պետք է նաև համեմատել այդ մինուցիաների

բազմությունները (նույն անձին պատկանող մինուցիաների բազմությունները տարբեր փորձերի ժամանակ պետք է իրար մոտ լինեն, իսկ տարբեր անձանց համար՝հեռու): Որպես համեմատման չափանիշ ընտրվել է Հաուսդորֆի փոփոխված ալգորիթմը: Տրված T շեմային արժեքի համար կասենք, որ A և B բազմությունները իրար մոտ են, եթե Հաուսդորֆի փոփոխված հեռավորությունը՝ H(A,B)≤T: Տալով T-ին տարբեր արժեքներ՝ հաշվարկվել է ձեռքի ափի երակների վրա հիմնված նույնականացման համակարգի ճշգրտության գնահատականները՝ համակագին հասանելիության կեղծ տրամադրման գործակիցը (ԿՏԳ) և համակարգի հասանելիության կեղծ մերժման գործակիցը (ԿՄԳ):



Նկար 5: ԿՏԳ-ի և ԿՄԳ-ի գրաֆիկները՝ կախված շեմային T արժեքից:

Նկար 5-ում պատկերված է ԿՏԳ-ի և ԿՄԳ-ի գրաֆիկները՝ կախված շեմային T արժեքից: Այդ գրաֆիկը կառուցելու համար գրանցման փուլում օգտագործվել է անձի ձեռքի ափի մեկ պատկերից առանձնացված մինուցիաների բազմությունը (այս գլխում նշված ալգորիթմով): ԿՄԳ-ը հաշվելու համար նույնականացման ժամանակ օգտագործվել է նույն անձի ձեռքի ափի մնացած հինգ պատկերները, իսկ ԿՏԳ-ը հաշվելու համար՝ մյուս 99 անձանց ձեռքի ափի վեցական պատկերներ: Ինչպես երևում է Նկար 5-ից, այս համակարգն ունի մոտավորապես 1% սխալների հավասարեցման գործակից (ՍՀԳ), երբ շեմային արժեքը ընտրված է 11-ին հավասար, որը բավականին լավ արդյունք է նմանատիպ համակարգերի համար:

Հաշվի առնելով առանձնացվող մինուցիաների քանակը, այն հենքի մեծությունը, որի վրա կիրառվել է առաջարկվող մոտեցումը և ճշգրտության հատկանիշները՝ կարելի

է ասել, որ մինուցիաներն իրենցից ներկայացնում են ձեռքի ափի երակների տարբերիչ բնութագրեր:

Երրորդ գլխում ներկայացված է ձեռքի ափի երակներից ստացված բնութագրերի հիման վրա «ոչ հստակ» պահոցների[5] սխեմայի կառուցման եղանակը: Օգտագործողի տվյալների տատանման էֆեկտի նկատմամբ (intra-class variations) կայունությունն ու ոչ կարգավորված տվյալների հետ աշխատանքը «ոչ հստակ» պահոցների սխեման կենսաչափական շաբլոնի պաշտպանության համար դարձնում են ամենախոստումնալից մոտեցումներից մեկը:

«Ոչ հստակ» պահոցների սխեմայի անվտանգությունը հիմնված է բազմանդամի վերականգնման մոտեցման վրա: Այն աշխատում է հետևյալ կերպ. դիցուք պետք է պաշտպանել օգտագործողի կենսաչափական շաբլոնը, որը ներկայացվում է բնութագրերի X ոչ կարգավորված բազմությամբ, K գաղտնագրման բանալու միջոցով: Ոչ կարգավորվածության տակ այստեղ պետք է հասկանալ, որ բազմության բոլոր տարրերը ունիկալ են, և այդ տարրերի հերթականությունը բազմության մեջ էական չէ: Այդպիսի օրինակներից են մատնահետքի կամ ձեռքի ափի երակների մինուցիաները: Այնուհետև, ընտրվում է P բազմանդամը, որը ծածկագրում է K բանալին ինչ-որ ձևով և հաշվվում են բազմանդամի արժեքները X բազմության բոլոր տարրերի համար: Այնուհետև ընտրվում են մեծ քանակությամբ պատահական սկզբունքով գեներացված «աղմուկ» կետերը (chaff points), որոնք չեն պատկանում տվյալ բազմանդամին: Այդ երկու բազմությունների միավորումը ձևավորում է «ոչ հստակ» V պահոցը:

«Ոչ հստակ» պահոցի վրա հիմնված օգտագործողի նույնականացումը իրականացվում է հետևյալ կերպ. դիցուք՝ հարցման ժամանակ կենսաչափական շաբլոնից առանձնացվել է բնութագրերի X' բազմությունը: Եթե X-ն ու X'-ը էականորեն հատվում են, ապա օգտագործողը կարող է գտնել V պահոցից P բազմանդամին պատկանող շատ կետեր: Եթե գտնվել են բազմանդամին պատկանող բավականաչափ քանակի կետեր, ապա բազմանդամի վերականգնումն ու, հետևաբար, բանալու վերծանումը կարող է իրականացվել սխալներ ուղղելու սխեմաների միջոցով: Եթե վերծանման արդյունքում գտնվել է ճիշտ բանալին, ապա նույնականացումը համարվում է հաջողված: Եթե X-ն ու X'-ը շատ քիչ են հատվում, ապա P բազմանդամի վերականգնումը դառնում է անհնարին, և նույնականացումը համարվում է անհաջող: Կենսաչափական շաբլոնից և գաղտնագրման K բանալուց պահոց կառուցելու քայլերը ներկայացված են ստորև՝

Ալգորիթմ 1 (Ծածկագրման ալգորիթմ)՝

- **Բաց պարամետրեր՝** F դաշտ:
- **Մուտքի պարամետրեր՝** n-ը բազմանդամի աստիճանն է, s-ը աղմուկ կետերի քանակ, r-ը շաբլոնից առանձնացվող բնութագիր կետերի քանակ ($0 < n < r \ll s$), բանալի K, $X = \{x_i\}_{i=1}^{r}$ բազմությունն, որը ներկայացնում է կենսաչափական

[5] A. Juels and M. Sudan, "A fuzzy vault scheme" in Proceedings of the IEEE International-Symposium on Information Theory, p.408, 2002.

շաբլոնը և բավարարում հետևյալ պայմաններին՝ $x_i \in F$ ու $x_i \neq x_j \; \forall i \neq j, \quad i,j = 1 \dots r$

- **Ելք՝** $\boldsymbol{V = \{(a_i, b_i)\}_{i=1}^{t}}$ պահոցը, որտեղ $t = r + s$:

Քայլեր՝

1. $P \leftarrow$ *Ծածկագրել*(K);
2. $L, C, Y \leftarrow \emptyset$;
3. $\forall j = 1 \dots r: (a_j, b_j) \leftarrow \big(x_j, P(x_j)\big); L \leftarrow L \cup (a_j, b_j)$;
4. $\forall j = r+1 \dots t: y_j \in F - (X \cup Y); Y \leftarrow Y \cup y_j; z_j \in F - \{P(y_j)\}; (a_j, b_j) \leftarrow (y_j, z_j); C \leftarrow C \cup (a_j, b_j)$;
5. $V' \leftarrow L \cup C; V \leftarrow$ *Վերադասավորել*(V');
6. *Վերադարձնել* V;

Ալգորիթմ 1-ում օգտագործված բոլոր գործողությունները կատարվում են F դաշտում: Ալգորիթմի մուտքին տրվում են երեք պարամետրեր՝ n, r, s, որտեղ r-ը կախված է կենսաչափական շաբլոնից առանձնացվող բնութագրերի քանակից, s-ով տրվում է պահոցին ավելացվող աղմուկ կետերի քանակը, որն ազդում է «ոչ հստակ» պահոցների սխեմայի անվտանգության հատկանիշների վրա, իսկ n-ով տրվում է բազմանդամի աստիճանը, որով որոշվում է վերծանման ժամանակ սխալվելու նկատմամբ համակարգի հանդուրժողականությունը (error tolerance):

Ծածկագրել(K) ֆունկցիան կառուցում է n աստիճան ունեցող P բազմանդամն այնպես, որ P-ն ծածկագրում է K բանալին (տրված P-ի համար պետք է հնարավոր լինի միանշանակ վերականգնել K բանալին): Այդպիսի բազմանդամ կառուցելու պարզ մոտեցումներից է K բանալու ներդրումն է P-ի գործակիցների մեջ: Ֆունկցիան *Վերադասավորել*(V')՝ պատահական կերպով վերադասավորում է V'-ի տարրերը՝ վերջնական V պահոցը ստանալու համար:

Օգտագործողի կենսաչափական տվյալների հիման վրա պահոցից բանալու ստացման եղանակն ունի Ալգորիթմ 2-ում նկարագրված տեսքը՝

Ալգորիթմ 2 (Վերծանման ալգորիթմ)

- **Բաց պարամետրեր՝** F դաշտ:
- **Մուտքի պարամետրեր՝** n-ը բազմանդամի աստիճանն է, s-ը աղմուկ կետերի քանակ, r-ը շաբլոնից առանձնացվող բնութագիր կետերի քանակ ($0 < n < r \ll s$), $X' = \{x_i'\}_{i=1}^{r}$ բազմությունն, որը ներկայացնում է կենսաչափական շաբլոնը և բավարարում հետևյալ պայմաններին՝ $x'_i \in F$ ու $x'_i \neq x'_j \; \forall i \neq j, \; i,j = 1 \dots r$, պահոց՝ $\boldsymbol{V = \{(a_i, b_i)\}_{i=1}^{t}}$
- **Ելք՝** *K բանալի կամ null, որտեղ null − ը դատարկ արժեք է*

Քայլեր՝

1. $L' \leftarrow \emptyset$;
2. $\forall i = 1 \dots r: \{(a'_i, b'_i) \leftarrow null; \forall j = 1 \dots t \{$ *եթե* $x'_i = a_j$, *ապա* $(a'_i, b'_i) \leftarrow (a_j, b_j)$; *դուրս գալ ցիկլից*; $\} L' \leftarrow L' \cup (a'_i, b'_i); \}$
3. P ← Վերծանում(L');
4. *Եթե* P *null է, ապա վերադարձնել null, հակառակ դեպքում* $\{K \leftarrow$ *ՎերծանելԲանալի*(P); *Վերադարձնել* K; $\}$

Ալգորիթմ 2-ում օգտագործված բոլոր գործողությունները կատարվում են F դաշտում: Ալգորիթմը իր ելքին վերադարձնում է K բանալին, կամ null արժեքն, որը նշանակում է, որ նույնականացումն անցավ անհաջող: Վերծանում(L′) ֆունկցիան Ռիդ-Սոլոմոնի (r, n) վերծանման ալգորիթմն է, որը փնտրում է n աստիճան ունեցող այնպիսի P բազմանդամ, որ $P(a'_i) = b'_i$ ավելի քան $\frac{r+n}{2}$ հատ $(a'_i, b'_i) \in L'$ արժեքների համար: Վերծանում(L′) ֆունկցիան վերադարձնում է բազմանդամ, որը բավարարում է վերևում նշված պայմաններին, կամ null, եթե այդպիսի բազմանդամ չի գտնվել: *ՎերծանելԲանալի*(P) ֆունկցիան Ալգորիթմ 1-ում նշված *Ծածկագրել*(K) ֆունկցիայի հակադարձն է, և այն վերականգնում է K բանալին P բազմանդամից: Պահոցի վերծանման ալգորիթմը գտնում է ճիշտ K բանալին, եթե սխալների քանակը կենսաչափական տվյալներում $|X - X'|$ (օրինակ՝ չհամընկնող մինուցիաների քանակը) փոքր է $\frac{r-n}{2}$ –ից:

Ձեռքի ափի երակների համար իրականացվել է ստանդարտ «ոչ հստակ» պահոցների սխեմայի փոփոխված տարբերակը[6]: Մասնավորապես, այդ սխեմայում չի պահանջվում սխալներ ուղղող կոդեր: Վերջիններիս փոխարեն, դիտարկվում են $n + 1$ տարր ունեցող տարբեր բազմություններ (n-ը բազմանդամի աստիճանն է), որոնք գեներացվում են վերծանման L բազմությունից, և բազմանդամները վերականգնվում են Լագրանժի միջարկման միջոցով: Այս սխեմայի գլխավոր առավելություններից է համակարգի հանդուրժողականության աճը (error tolerance) սխալների նկատմամբ: Քանի որ անհրաժեշտ են միայն $n + 1$ կետեր՝ n աստիճան ունեցող բազմանդամը միանշանակ որոշելու համար, այս սխեմայով հնարավոր է ստանալ K բանալին, երբ սխալների քանակը $(|X - X'|)$ փոքր է $r - n$ –ից, որը ստանդարտ սխեմայի համար վերևում բերված թվից երկու անգամ մեծ է: Այս մոտեցումը մեծ հաշվարկելիության արժեքի պատճառով ունի նաև թերություն, քանի որ այն պահանջում է կատարել մեծ քանակով բազմանդամների մոտարկումներ:

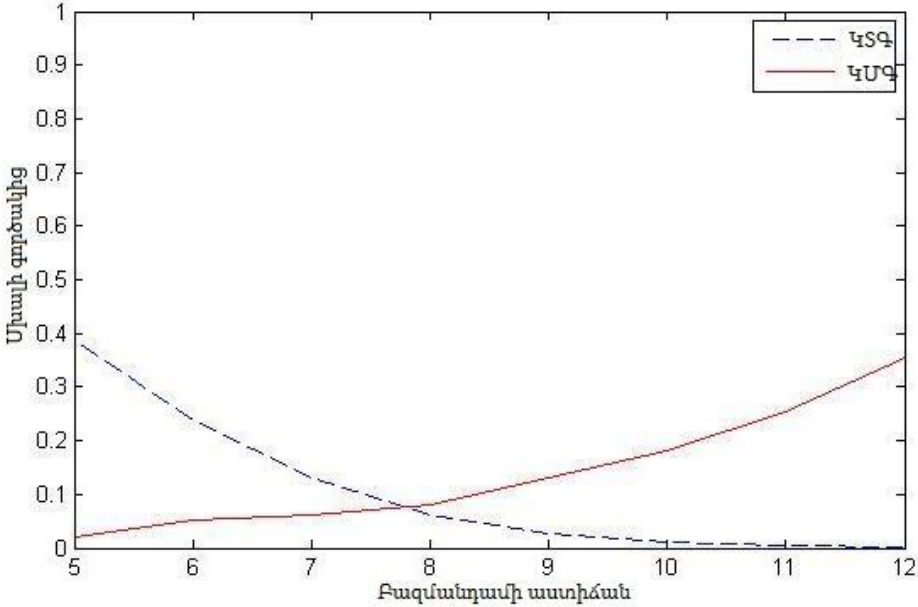
Համակարգի էֆեկտիվությունը չափելու համար օգտագործվել են հասանելիության կեղծ տրամադրման և հասանելիության կեղծ մերժման գնահատականները: Կեղծ մերժման գործակիցը ստանալու նպատակով կատարվել է համակարգին 100 դիմում՝ յուրաքանչյուր 100 օգտագործողի համար մեկական անգամ: Հասանելիության կեղծ տրամադրման գործակիցը ստանալու նպատակով կատարվել է 9900 դիմում՝ փորձելով վերծանել ընտրված մեկ օգտագործողի երակների հիման վրա գաղտնագրված պահոցը՝ մյուս 99 օգտագործողների ձեռքի ափի երակներն օգտագործելով:

Քանի որ վերծանումը համարվում է հաջողված, երբ հարցման մինուցիաների բազմության մեջ (որն ունի r կետ) n+1 կետերը համընկնում են գրանցման շաբլոնի մինուցիաների հետ, կեղծ մերժման և կեղծ տրամադրման գործակիցները փոխվում են n-ի արժեքից կախված (ֆիքսված r-ի դեպքում): Փոքրացնելով n-ը՝ կեղծ մերժման գործակիցը նվազում է, բայց աճում է կեղծ տրամադրման գործակիցը, և, հակառակը, մեծացնելով n-ը՝ կեղծ մերժման գործակիցն աճում է, իսկ կեղծ տրամադրման

[6] U. Uludag, S. Pankanti, and A. K. Jain, *"Fuzzy Vault for Fingerprints",* in Proceedings of Fifth International Conference on Audio- and Video-based Biometric Person Authentication, p. 310–319, USA, 2005.

գործակիցը՝ նվազում: Կեղծ մերժման և կեղծ տրամադրման գործակիցների n-ից կախման գրաֆիկը պատկերված է Նկար 6 –ում:

Առաջարկված սխեմայի թերություններից է կեղծ մերժման գործակցի համեմատաբար բարձր արժեքը:



Նկար 6: Ձեռքի ափի երակների վրա հիմնված «ոչ հստակ» պահոցների սխեմայի ԿՏԳ-ի և ԿՄԳ-ի բազմանդամի աստիճանից կախման գրաֆիկ:

Այսպիսով, փորձերի արդյունքում ստացանք, որ օգտագործողների ձեռքի ափի երակներից առանձնացված մինուցիաների քանակը (25 հատ) բավական է 130 բիթ բանալի գաղտնագրելու համար, երբ համակարգի ԿՏԳ-ը փոքր է 0.01%-ից, ինչը լավ արդյունք է կիրառական օգտագործման տեսակետից:

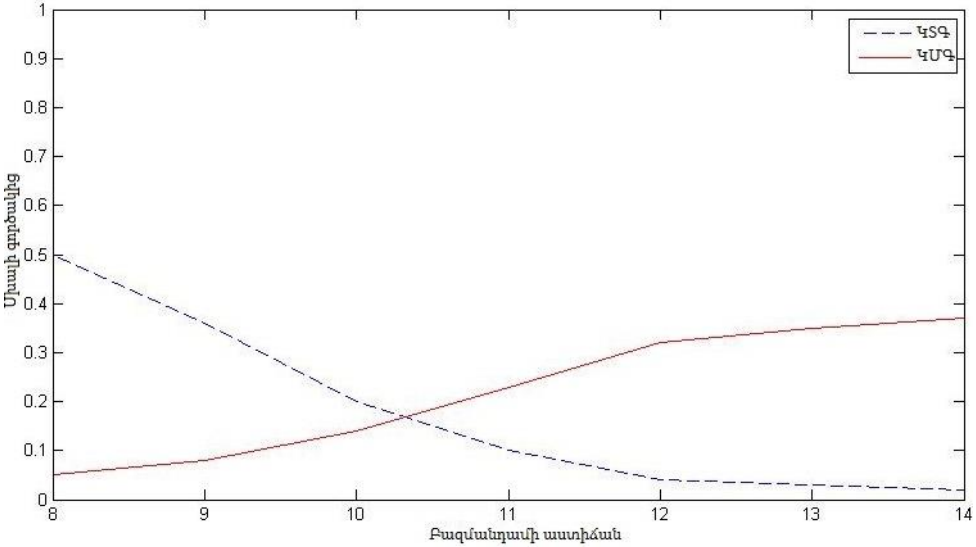
Դիտարկելով ձեռքի ափի երակների վրա հիմնված կենսաչափական գաղտնագրման համակարգի անվտանգությունը օժանդակ տվյալների նվազագույն էնտրոպիայի տեսանկյունից՝ միատեսակ բաշխվածության դեպքում ստացվել է **46** բիթ:

Այս գլխում մշակվել է նաև ձեռքի ափի երակների և մատնահետքի վրա հիմնված բազմակենսաչափական «ոչ հստակ» պահոցների սխեման: Այս սխեման իր մեջ ներառում է բազմակենսաչափական համակարգերին բնորոշ բոլոր առավելությունները, այդ թվում ճշգրտությունն ու բարձր անվտանգությունը:

Համակարգի էֆեկտիվությունը չափելու համար այստեղ ևս օգտագործվել են հասանելիության կեղծ տրամադրման և հասանելիության կեղծ մերժման գնահատականները:

Կեղծ մերժման և կեղծ տրամադրման գործակիցների n-ից (n-ը բազմանդամի աստիճանն է) կախման գրաֆիկը (ֆիքսված ընդհանուր մինուցիաների կետերի քանակի դեպքում) պատկերված է Նկար 7–ում:

Այսպիսով, փորձերի արդյունքում ստացանք, որ օգտագործողների ձեռքի ափի երակներից և մատնահետքերից առանձնացված մինուցիաների ընդհանուր քանակը (55 հատ) բավական է 224 բիթ բանալի գաղտնագրելու համար, երբ համակարգի ԿՏԳ-ը փոքր է 0.01%-ից, ինչը լավ արդյունք է կիրառական օգտագործման տեսակետից:



Նկար 7: Ձեռքի ափի երակների և մատնահետքերի վրա հիմնված բազմակենսաչափական «ոչ հստակ» պահոցների սխեմայի ԿՏԳ-ի և ԿՄԳ-ի բազմանդամի աստիճանից կախման գրաֆիկ:

Բազմակենսաչափական սխեմայի օժանդակ տվյալների նվազագույն էնտրոպիայի տեսանկյունից անվտանգության վերլուծության արդյունքում ցույց տրվեց, որ այն ունի **55** բիթ արժեք: Բացի այդ, բազմակենսաչափական սխեմայի անվտանգության վերլուծության արդյունքում ստացվեց, որ այն ունի էականորեն ավելի բարձր արժեք, քան սխեմաներից յուրաքանչյուրը՝ առանձին վերցրած:

Չորրորդ գլխում բերվում է ձեռքի ափի երակների ցանցի վրա հիմնված PalmVGram համակարգի նկարագրությունը, որն իրականացնում է նախորդ գլխում բերված՝ ձեռքի ափի երակներից առանձնացված բնութագրերի վրա հիմնված գաղտնագրման համակարգի կառուցման ընթացակարգը: PalmVGram համակարգն իրենից ներկայացնում է ծրագրային փաթեթ, որը բաղկացած է երկու հիմնական մասերից. առաջինը գրված է Matlab միջավայրում, իսկ երկրորդը՝ Java:

ԱՇԽԱՏԱՆՔԻ ՀԻՄՆԱԿԱՆ ԱՐԴՅՈՒՆՔՆԵՐԸ

Ատենախոսության շրջանակներում կատարված հետազոտությունները բերել են հետևյալ արդյունքների՝

1. Առաջարկվել է ձեռքի ափի երակների ցանցից բնութագրերի առանձնացման համար պատկերների մշակման եղանակների համադրմամբ նոր մոտեցում [1]:
2. Ձեռքի ափի երակների ցանցից առանձնացված բնութագրերի հիման վրա մշակվել է գաղտնագրման համակարգ և վերլուծվել են նրա անվտանգության և ճշգրտության հատկությունները [2]:
3. Մշակվել է ձեռքի ափի երակների ցանցից և մատնահետքերից առանձնացված բնութագրերի հիման վրա բազմակենսաչափական գաղտնագրման համակարգ և վերլուծվել են նրա անվտանգության և ճշգրտության հատկությունները [3,4]:
4. Մշակվել է ձեռքի ափի երակների ցանցից առանձնացված բնութագրերի հիման վրա գաղտնագրման համակարգի կառուցման ընթացակարգն իրականացնող ծրագրային ապահովություն [1,2]:

ԱՏԵՆԱԽՈՍՈՒԹՅԱՆ ԹԵՄԱՅՈՎ ՏՊԱԳՐՎԱԾ ՀՈԴՎԱԾՆԵՐԸ

[1] S. Chidemyan, A. Jivanyan, G. Khachatryan "Palm Vein Minutiae Feature Extraction for Human Identification", Mathematical Problems of Computer Science 42, pp. 85-96, Yerevan, Armenia, 2014.

[2] S. Chidemyan, A. Jivanyan, G. Khachatryan, H. Khasikyan "Palm-Vein Based Fuzzy Vault Scheme", in Reports of NAS RA, v. 115, № 1, pp. 27-32, Yerevan, Armenia, 2015.

[3] S. Chidemyan, "Palm-Vein and Fingerprint Based Multimodal Fuzzy Vault Scheme", in Proceedings of the YSU, Series phys. and math, № 1, pp. 41-46, Yerevan, Armenia, 2015.

[4] S. Chidemyan, "Palm-vein and fingerprint based improved multimodal fuzzy vault scheme", ITHEA Journal, Information Theories and applications, № 1, pp. 1-5, Bulgaria, 2015.

РЕЗЮМЕ

Чидемян Сергей Сергеевич

“Разработка биометрической криптосистемы, основанной на венах ладони”

В данной работе исследуются проблемы построения биометрических криптосистем. Предметом исследования являются характеристики эффективности и безопасности криптосистем, основанных на венах ладони.

Использование биометрических данных рассматривается как ключевое решение для многих проблем безопасности и аутентификации. Несмотря на многочисленные преимущества использования биометрических данных, существуют работы, в которых указываются их некоторые недостатки. Каждая биометрическая характеристика, используемая при аутентификации, имеет свои положительные и отрицательные стороны. В частности, самой распространенной биометрической характеристике: отпечаткам пальцев, присущ очевидный недостаток – их возможно копировать. Кроме того, существуют многочисленные методы изготовления искусственных отпечатков. Во избежание такого рода угроз японская фирма “Fujitsu” предложила технологию аутентификации, основанную на венах ладони. Эта сравнительно новая технология считается одной из самых безопасных и многообещающих.

Аутентификация, основанная на биометрических данных, является хорошим механизмом, однако для ее реализации требуется хранения большого количества биометрических шаблонов, что является большим недостатком. Хранение большого количества биометрических данных может привести к утечке информации или их краже. Использование схем защиты шаблонов, в которых методы криптографии сочетаются вместе с биометрическими характеристиками, рассматривается как перспективное решение указанных проблем.

Основной целью диссертационной работы является разработка криптосистемы, основанной на сетке вен ладони, которая обеспечила бы высокую безопасность. Эта система должна быть по возможности эффективной и, самое главное, с помощью этой системы решалась бы проблема копирования биометрических характеристик, присущая, в частности, отпечаткам пальцев. В то же время, эта система должна быть удобна в использовании и конкурентоспособна по отношению к подобным системам.

Научная новизна

- Был предложен новый, комбинированный подход, основанный на различных методах извлечения характеристик из изображений вен ладони.
- Была разработана криптосистема, основанная на характеристиках, извлеченных из изображений вен ладони и произведен анализ ее свойств безопасности и эффективности.
- Была разработана мульти-биометрическая криптосистема, основанная на характеристиках, извлеченных из изображений вен ладони и отпечатков пальцев и произведен анализ ее свойств безопасности и эффективности.

Применяемость результатов

На основе полученных результатов была разработана основанная на венах ладони система, предоставляющая возможность производить аутентификацию пользователей и защищать биометрический шаблон, которая обладает хорошими оценками производительности. Учитывая тот факт, что в ее основе лежит технология бесконтактной аутентификации, она может быть широко использована в местах, где вопросы гигиены стоят остро, например, в медицинских учреждениях для предоставления больным доступа к личным данным. Кроме того, эту систему можно использовать: а) в банковской сфере при проведении финансовых операций; б) в учебных заведения для предоставления доступа к обучающим системам; в) в аэропортах для выяснения личности пассажиров и т.д.

На защиту представлены следующие положения:

1. Новый комбинированный подход по извлечению вен ладони.
2. Криптосистема, основанная на характеристиках, извлеченных из изображений вен ладони.
3. Мульти-биометрическая криптосистема, основанная на характеристиках, извлеченных из изображений вен ладони и отпечатков пальцев.
4. Программный пакет, основанный на предложенном подходе построения биометрической криптосистемы, основанной на характеристиках, извлеченных из изображений вен ладони.

В результате исследований, проведенных в данной работе, были получены следующие **основные результаты**:

- Был предложен новый, комбинированный подход по извлечению характеристик из изображений вен ладони [1].
- Была разработана криптосистема, основанная на характеристиках, извлеченных из изображений вен ладони, и был произведен анализ её свойств безопасности и эффективности [2].
- Была разработана мульти-биометрическая криптосистема, основанная на характеристиках, извлеченных из изображений вен ладони и отпечатков пальцев, и был произведен анализ её свойств безопасности и эффективности [3,4].
- Было разработано программное обеспечение, реализующее процесс построения биометрической криптосистемы, основанной на характеристиках, извлеченных из вен ладони [1,2].

Внедрение: Разработанная система, основанная на сетке вен ладоней, была апробирована в учебном центре ООО “Армянские программы”. С помощью данной системы производится проверка доступа студентов к обучающей системе.

ABSTRACT

Sergey S. Chidemyan

"Development of palm-vein based biometric cryptosystem"

The thesis is devoted to studying some problems of building of biometric cryptosystems. The main subject of the study is performance and security characteristics of palm-vein based cryptosystems.

Using biometrics is considered to be a key solution for many problems of security and authentication. Though using biometrics has many advantages, there are many works in which some limitations of them are mentioned. Every biometric used for authentication has its pros and cons. In particular, the most common biometrics as fingerprint has the obvious disadvantage – the possibility to be copied. Moreover, there are many methods of making the artificial fingerprints (gummy fingers). To overcome such kind of problems the palm-vein based authentication technology is reviewed. This relatively new technology is considered to be one of the most secure and promising.

Authentication based on biometrics is a good technique; however it requires the storage of a big amount of the biometric templates, which appears to be a big drawback. The storage of a big amount of users' information can lead to its leakage or steal. Using schemes of biometric templates' protection, in which some cryptographic methods are combined with biometrics, is considered to be a promising solution of the problems mentioned above.

The main objective of the research is to develop palm-vein based cryptosystem, which would provide high security. This system should have as good performance as possible and what is the most important it should solve the problem of copying the biometric features (inherent to fingerprints). At the same time, this system should be user-friendly and competitive with such kind of systems.

Scientific novelty

- The new combined method, based on different techniques of palm veins features' extraction is introduced.
- The cryptosystem based on the features extracted from palm veins is developed and its security and performance analysis is introduced.
- The multi-biometric cryptosystem based on the features extracted from palm veins and fingerprints is developed and its security and performance analysis is introduced.

Applicability of the results

On the basis of the obtained results the palm-vein based system is developed, which allows to authenticate users and protect their biometric templates and at the same time shows good performance. Considering that it is based on contactless authentication technology, it can be widely used in areas where hygiene issues are acute, for example, in hospitals to provide patients access to personal data. In addition, this system can be used: a) in the banking sector during

financial operations; b) in educational institutions to provide access to training systems; c) in the airports to verify the identity of passengers, etc.

The following statements are presented for defense:

1. New combined method of palm veins features' extraction
2. The cryptosystem based on the features extracted from palm veins.
3. The multi-biometric cryptosystem based on the features extracted from palm veins and fingerprints.
4. The application that implements the proposed algorithm of palm-vein based cryptosystems' construction.

The research conducted within the framework of the thesis has produced the following **main results**:

- The new combined method, based on different techniques of palm veins features' extraction is introduced [1].
- The cryptosystem based on the features extracted from palm veins is developed and its security and performance analysis is introduced [2].
- The multi-biometric cryptosystem based on the features extracted from palm veins and fingerprints is developed and its security and performance analysis is introduced [3, 4].
- The application that implements the proposed algorithm of palm-vein based cryptosystems' construction is developed. [1, 2].

System implementation

Developed palm-vein based cryptosystem was implemented at training center of "Armsoft" LLC. With the help of this system the access of students to the training system is checked.