ՀՀ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԶԳԱՅԻՆ ԱԿԱԴԵՄԻԱՅԻ ԻՆՖՈՐՄԱՏԻԿԱՅԻ ԵՎ ԱՎՏՈՄԱՏԱՑՄԱՆ ՊՐՈԲԼԵՄՆԵՐԻ ԻՆՍՏԻՏՈՒՏ

ՄԱԼԽԱՍՅԱՆ ՆԱՐԵԿ ԱՐԱՐԱՏԻ

ՄԱՏՆԱՀԵՏՔԱՅԻՆ ՏՎՅԱԼՆԵՐԻ ՄՇԱԿՄԱՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ՈՐՈՇ ԴՐՈՒՅԹՆԵՐ

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

Ս Ե Ղ Մ Ա Գ Ի Ր

ԵՐԵՎԱՆ 2013

ИНСТИТУТ ПРОБЛЕМ ИНФОРМАТИКИ И АВТОМАТИЗАЦИИ НАЦИОНАЛЬНОЙ АКАДЕМИИ НАУК РА

МАЛХАСЯН НАРЕК АРАРАТОВИЧ

НЕКОТОРЫЕ АСПЕКТЫ БЕЗОПАСНОСТИ ОБРАБОТКИ ДАННЫХ ОТПЕЧАТКОВ ПАЛЬЦЕВ

АВТОРЕФЕРАТ

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

ЕРЕВАН 2013

Ատենախոսության թեման հաստատվել է ՀՀ ԳԱԱ Ինֆորմատիկայի և ավտոմատացման պրոբլեմների ինստիտուտում:

Գիտական ղեկավար՝	տ.գ.դ.	Գ. Հ. Խաչատրյան
Պաշտոնական ընդդիմախոսներ՝	տ.գ.դ.	Դ. Գ. Ասատրյան
	տ.գ.թ.	Վ. Ս. Սողոմոնյան

Առաջատար կազմակերպություն՝ Հայաստանի պետական ճարտարագիտական համալսարան

Ատենախոսության պաշտպանությունը կայանալու է 2013թ. մայիսի 14-ին, ժ. 16:00-ին, ՀՀ ԳԱԱ Ինֆորմատիկայի և ավտոմատացման պրոբլեմների ինստիտուտի 037 «Ինֆորմատիկա և հաշվողական համակարգեր» մասնագիտական խորհրդի նիստում, հետևյալ հասցեով՝ 0014, Երևան, Պ. Սևակ փ. 1:

Ատենախոսությանը կարելի է ծանոթանալ ՀՀ ԳԱԱ ԻԱՊԻ-ի գրադարանում:
Սեղմագիրն առաքված է 2013թ. ապրիլի 13-ին:

037 մասնագիտական խորհրդի գիտական քարտուղար, ֆ.մ.գ. դ. Հ. Գ. Սարուխանյան

Тема диссертации утрверждена в Институте проблем информатики и автоматизации НАН РА.

Научный руководитель:	д.т.н.	Г. Г. Хачатрян
Официальные оппоненты:	д.т.н.	Д. Г. Асатрян
	к.т.н.	В. С. Согомонян

Ведущая организация: Государственный инженерный университет Армении

Защита диссертации состоится 14-ого мая 2013г., в 16:00 часов, на заседании специализированного совета 037 “Информатика и вычислительные системы” Института проблем информатики и автоматизации НАН РА, по адресу: 0014, Ереван, ул. П. Севака 1.

С диссертацией можно ознакомиться в библиотеке ИПИА НАН РА.
Автореферат разослан 13-ого апреля 2013г.

Ученый секретарь специализированного совета 037, д.ф.м.н. А. Г. Саруханян

ԱՇԽԱՏԱՆՔԻ ԸՆԴՀԱՆՈՒՐ ԲՆՈՒԹԱԳԻՐԸ

Աշխատանքի արդիականությունը

Տնտեսության տարբեր ոլորտներում համակարգիչների զանգվածային գործածության աճը և տեխնոլոգիական առաջընթացը հանգեցնում են այն փաստին, որ կազմակերպություններն ու անհատներն ավելի և ավելի շատ են վստահում ժամանակակից տեղեկատվական գործիքներին: Կազմակերպությունների և ձեռնարկությունների տեղեկատվական ենթակառուցվածքների աճող բարդությունը, ինչպես նաև սպառնալիքների և ռիսկերի փոփոխվող բնույթը տեղեկատվական անվտանգությունը դարձնում են կենսականորեն անհրաժեշտ խնդիր: Այնուամենայնիվ, տեղեկատվական անվտանգության բազմազան և արդյունավետ միջոցները կարող են գործնականորեն անօգուտ լինել, եթե դրանք չեն ուղեկցվում օգտատերերի նույնականացման հարմարավետ և հուսալի մեթոդներով:

Վերջին տարիները բնութագրվում են կենսաչափական նույնականացման մեթոդների նկատմամբ հետաքրքրության կայուն աճով: Նշված մեթոդները հիմնված են օգտատիրոջ կենսաբանական և վարքագծային առանձնահատկությունների վրա և տալիս են նկատելիորեն ավելի լավ արդյունքներ, քան նույնականացման ավանդական միջոցները, ինչպիսիք են ծածկագրերը, ID քարտերը և այլն: Այս հետաքրքրության հիմնական պատճառը կենսաչափական տեխնոլոգիաների ունակությունն է համեմատաբար պարզորեն տարբերակելու իրական օգտատերերին ոչ իրավասու անձանցից, ովքեր փորձում են խաբեությամբ ձեռք բերել հասանելիության իրավունքներ պաշտպանված տեղեկատվական ռեսուրսների նկատմամբ: Ներկայումս ամենատարածվածը այն կենսաչափական նույնականացման համակարգերն են, որոնք հիմնված են մատնահետքերի ճանաչման վրա, քանի որ դրանք առավել հարմար են օգտագործման տեսանկյունից և ֆինանսապես ավելի արդյունավետ են:

Միևնույն ժամանակ, մատնահետքերի վրա հիմնված նույնականացման համակարգերի դեմ ուղղված հնարավոր հարձակումների վերլուծությունը ցույց է տալիս, որ կենսաչափական տվյալների անվտանգությունն ու ամբողջականությունն ապահովելը կարևոր խնդիր է: Ակնհայտ է, որ կենսաչափական տվյալները, բարձր յուրահատկությամբ օժտված լինելով հանդերձ, գործնականում վատ են պաշտպանված պատճենահանումից, տարատեսակ չարաշահումներից և կողմնակի ազդեցություններից: Ըստ էության, կենսաչափական նույնականացման համակարգը կարող է ճիշտ աշխատել միայն այն դեպքում, երբ այն ի վիճակի է երաշխավորել, որ օգտատերերի գրանցման և նույնականացման փուլերում տվյալները ստացվել են համապատասխան օգտատիրոջից և չեն ենթարկվել կողմնակի ազդեցությունների: Հետևաբար՝ կենսաչափական նույնականացման մեթոդների համատարած օգտագործումը խթանելու տեսանկյունից կենսաչափական, մասնավորապես՝ մատնահետքային տվյալների պաշտպանության խնդիրը դառնում է խիստ արդիական:

Կենսաչափական տվյալների պաշտպանության իրականացումը ստեգանոգրաֆիկ մեթոդների միջոցով բավական խոստումնալից է թվում: Մինչդեռ գաղտնագրային մեթոդները հիմնականում կենտրոնանում են գաղտնի տեղեկությունը կողմնակի անձանց համար անհիմաստ դարձնելու սկզբունքների վրա, ստեգանոգրաֆիան հիմնվում է գաղտնի տեղեկության առկայության փաստի քողարկման վրա: Ստեգանոգրաֆիկ

միջոցները կարող են օգտագործվել մատնահետքերի պաշտպանության համար՝ ապահովելով տվյալների անվտանգությունը և ամբողջականությունը ինչպես անապահով կապուղիներով փոխանցվելիս, այնպես էլ կրիչների վրա պահպանվելիս: Սա կարող է էապես նվազեցնել կենսաչափական տվյալների չարտոնված ձեռքբերման հնարավորությունը, դրանով իսկ կրճատելով այդ տվյալների՝ չարաշահումների և կողմնակի ազդեցությունների ենթարկելու հավանականությունը:

Հետազոտության հիմնական նպատակը

Աշխատանքի հիմնական նպատակը և խնդիրն է մշակել մեթոդներ, որոնք ունակ են ապահովելու մատնահետքերի վրա հիմնված հեռահար նույնականացման համակարգերի անվտանգությունը աշխատանքի բոլոր փուլերում՝ օգտագործելով տեղեկության քողարկման ստեգանոգրաֆիկ միջոցներ:

Նշված նպատակին հասնելու համար աշխատանքում լուծվել են ստորև թվարկված խնդիրները.

- Նախագծել մատնահետքերի վրա հիմնված հեռահար նույնականացման մեթոդ, որը օգտագործում է ստեգանոգրաֆիկ միջոցներ աշխատանքի բոլոր փուլերում, և որը ապահովում է անապահով կապուղով փոխանցվող մատնահետքային տվյալների անվտանգությունը և ամբողջականությունը:
- Մշակել մատնահետքի նկարից առավելագույն տեղեկություն պարունակող տրված չափի հատվածի անջատման մեթոդ:
- Նախագծել նշված հատվածում պարունակվող տեղեկության քանակության բարելավման մեթոդ:

Գիտական նորույթը

- Առաջարկվել է մատնահետքերի վրա հիմնված նույնականացման նոր սխեմա, որն օգտագործում է օգտատիրոջ երկու մատնահետքերը՝ անապահով կապուղով փոխանցված տվյալների նույնականությունը և ամբողջականությունը ստուգելու նպատակով:
- Մշակվել է մատնահետքի նկարից առավելագույն տեղեկություն պարունակող հատվածի անջատման մեթոդ, որը թույլ է տալիս նվազեցնել տվյալների այն քանակությունը, որն անհրաժեշտ է փոխանցել կապուղով՝ նույնականացումը իրագործելու համար:
- Մշակվել է ընտրված հատվածում պարունակվող տեղեկության քանակության բարելավման մեթոդ, որը հնարավորություն է տալիս փոխհատուցել հատվածի անջատման փուլում տեղի ունեցած տեղեկության կորուստը և իրագործել ընդունելի ճշգրտության նույնականացում:

Գործնական ներդրումը

Ստացված արդյունքների հիման վրա մշակվել է կլիենտային և սերվերային մոդուլներից բաղկացած նույնականացման ծրագրային գործիք, որն օգտագործվում է «Երևանի կապի միջոցների գիտահետազոտական ինստիտուտ» ՓԲԸ-ում, ընկերության կողմից մշակված անվտանգության համակարգում օգտատերերի հարմարավետ և

վստահելի հեռահար նույնականացում իրագործելու նպատակով: Աշխատանքի արդյունքների ներդրման ակտը բերված է ատենախոսության հավելվածում:

Պաշտպանությանը ներկայացվող դրույթները

- Մատնահետքերի վրա հիմնված նույնականացման սխեմա, որը նույնականության և ամբողջականության ստուգումներ իրականացնելու նպատակով օգտագործում է օգտատիրոջ երկու տարբեր մատնահետքերի նկարներ:
- Մատնահետքի նկարից առավելագույն տեղեկություն պարունակող հատվածի անջատման մեթոդ:
- Ընտրված հատվածում պարունակվող տեղեկության քանակության բարելավման մեթոդ, մատնահետքի հատուկ կետերը (minutiae points) նկարագրող պարամետրերի ցուցակին հավելյալ պարամետրեր ավելացնելու եղանակով:

Աշխատանքի արդյունքների զեկուցումները

Աշխատանքի հիմնական արդյունքներն ու դրույթները զեկուցվել և քննարկվել են.

- «IT Security for the Next Generation» միջազգային ուսանողական գիտաժողովի Հանրապետական փուլում (Երևան, 2011),
- «CyberSecurity for the Next Generation» միջազգային ուսանողական գիտաժողովի «Ռուսաստան և ԱՊՀ» փուլում (Երևան, 2013),
- Հայաստանի ամերիկյան համալսարանում և ՀՀ ԳԱԱ Ինֆորմատիկայի և ավտոմատացման պրոբլեմների ինստիտուտում կազմակերպված գիտական սեմինարների ընթացքում (Երևան, 2010-2013):

Հրապարակումները

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

Աշխատանքի կառուցվածքը և ծավալը

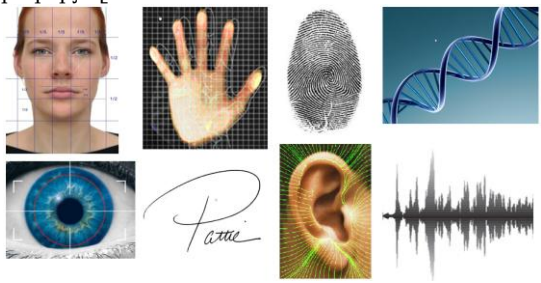
Ատենախոսությունը բաղկացած է ներածությունից, երեք գլուխներից, եզրակացությունից և 94 անուն ընդգրկող գրականության ցանկից: Աշխատանքի ընդհանուր ծավալն է 139 էջ՝ ներառյալ 63 նկար և մեկ աղյուսակ: Ատենախոսությունը գրված է անգլերեն լեզվով:

ԱՇԽԱՏԱՆՔԻ ԲՈՎԱՆԴԱԿՈՒԹՅՈՒՆԸ

Ներածություն: Ներածությունում հիմնավորված է թեմայի արդիականությունը, ձևակերպված են աշխատանքի նպատակները, գիտական նորույթները և պաշտպանությանը ներկայացված հիմնական դրույթները:

Գլուխ առաջին: Ատենախոսության առաջին գլխում բերվում են ամփոփ ներածական տեղեկություններ կենսաչափական տեխնոլոգիաների և նույնականացման համակարգերում դրանց կիրառությունների մասին: Գլուխը բաղկացած է հինգ բաժիններից:

Բաժին 1.1: Այս բաժինը ներկայացնում է համառոտ ակնարկ տարբեր տեսակի կենսաչափական տեխնոլոգիաների, կենսաչափական բնութագրիչների նկատմամբ առկա պահանջների, կենսաչափական համակարգերի արագագործության և դրանց կիրառությունների վերաբերյալ:



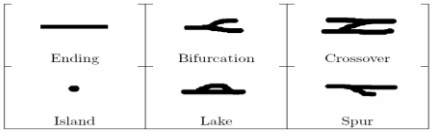
Նկ. 1. Կենսաչափական բնութագրիչների օրինակներ

Բաժին 1.2: Այս բաժնում բերվում են ներածական տեղեկություններ մատնահետքերի ներկայացման տիրույթի, ձևի, մատնահետքերի ճանաչման համակարգերի հիմնական մոդուլների և տարբեր մատնահետքային սկաներների վերաբերյալ: Մատնահետքերի ճանաչման վրա հիմնված համակարգերը ամենահինն են նույնականացման համակարգերի շարքում և դրանք հաճախ գործնական կիրառություն են ունեցել: Հայտնի է, որ յուրաքանչյուր ոք ունի յուրահատուկ մատնահետք, և այն չի փոխվում ողջ կյանքի ընթացքում: Մատնահետքը անհատի մատի մակերևույթի վրա գտնվող այսպես կոչված ակոսների և ծալքերի յուրահատուկ համախմբությունն է: Գոյություն ունեն մատնահետքի ներկայացման երկու մոտեցումներ՝ գլոբալ և լոկալ: Մատնահետքի գլոբալ ներկայացումը հիմնված է այսպես կոչված միջուկների և դելտաների վրա, մինչդեռ լոկալ ներկայացման հիմքում ընկած են ծալքերի վերջավորությունները և ճյուղավորումները (bifurcations), որոնց հաճախ անվանում են նաև հատուկ կետեր (minutiae points): Մատնահետքի նկարի հատուկ կետերի օրինակները պատկերված են նկ. 2-ում: Նույնականացման համակարգերը, որոնց աշխատանքի հիմքում ընկած են հատուկ կետերը, ներկայումս ամենատարածվածներն են, ինչը հիմնականում պայմանավորված է հետևյալ պատճառներով.

- հատուկ կետերի միջոցով հնարավոր է պահպանել մատնահետքը բնութագրող մեծ ծավալի տեղեկություն,
- մատնահետքերի՝ հատուկ կետերի վրա հիմնված ներկայացումները արդյունավետ են տվյալների պահպանման տեսանկյունից,

- հատուկ կետերի հայտնաբերումը մատնահետքի նկարի վրա համեմատաբար կայուն է մատնահետքերի տարատեսակ աղավաղումների նկատմամբ, որոնք կարող են ի հայտ գալ, օրինակ, կտրվածքների սպիացման արդյունքում:

Սովորաբար մատնահետքերի՝ հատուկ կետերի վրա հիմնված ներկայացումները հաշվի են առնում այդ կետերի տեղաբաշխումը մատնահետքի նկարի վրա և մատնահետքի ծալքերի ուղղություններն այդ կետերում:



Նկ. 2. Հատուկ կետերի տարածված տեսակներ

Բաժին 1.3: Այս բաժնում բերվում են ներածական տեղեկություններ տվյալների քողարկման ստեգանոգրաֆիկ մեթոդների և թվային ջրանիշերի (digital watermarks) մասին: Սա անհրաժեշտ է, քանի որ մատնահետքերի վրա հիմնված հեռահար նույնականացման առաջարկվող սխեման էապես հիմնվում է գոյություն ունեցող ստեգանոգրաֆիկ և թվային ջրանշման միջոցների վրա:

Ստեգանոգրաֆիան գիտություն է, որի հիմնական նպատակն է քողարկել հաղորդագրություններն այնպես, որ ոչ ոք, բացի հաղորդագրությունն ուղարկողից և հասցեատիրոջից, չկասկածի հաղորդագրության գոյությունը: Ստեգանոգրաֆիան կարող է օգտագործվել տվյալները տարբեր կոնտեյներների մեջ թաքցնելու նպատակով: Այս կոնտեյներները կարող են լինել պատկերներ, աուդիո ֆայլեր, վիդեո ֆայլեր, տեքստային ֆայլեր և այլն: Բաժնում վերլուծվում է նաև նշված մեթոդների կայունությունը տարատեսակ հարձակումների նկատմամբ:

Ստեգանոգրաֆիայի առավելությունը գաղտնագրության (cryptography) նկատմամբ կայանում է նրանում, որ ստեգանոգրաֆիկ պաշտպանությամբ հաղորդագրությունները ուշադրություն չեն գրավում: Գաղտնագրության նպատակն է ապահովել հաղորդակցության անվտանգությունը՝ փոխանցվող տվյալները փոփոխելով այնպես, որ հակառակորդները չկարողանան դրանք ձեռք բերել: Ստեգանոգրաֆիկ մեթոդները, մյուս կողմից, թաքցնում են հաղորդագրության գոյության փաստը: Հարկ է նշել, որ այս երկուսը կարող են օգտագործվել միասին, տեղեկատվության պաշտպանությունը բարելավելու համար:

Ջրանշումը հիմնականում օգտագործվում է մտավոր սեփականության պաշտպանության համար: Թվային ջրանիշը ազդանշան է, որը ներդրվում է թվային տվյալների (պատկեր, աուդիո, վիդեո, տեքստ և այլն) մեջ, և որը կարող է հետագայում բացահայտվել՝ տվյալների վավերականությունը հաստատելու համար: Ջրանշանը ներդրվում է տվյալների մեջ այնպես, որ այն չի կարող հեռացվել առանց տվյալները աղավաղելու: Չնայած նրան, որ այս մեթոդը հիմնապես նշում է տվյալները, դրանք շարունակում են մնալ մատչելի և կարող են օգտագործվել նույն նպատակներով: Ջրանշված օբյեկտում թաքցված տեղեկությունը իրենից ներկայացնում է ստորագրություն, որը հղվում է տվյալների ծագմանը կամ ճշմարիտ սեփականատիրոջը և ծառայում է հեղինակային իրավունքների պաշտպանությունն ապահովելուն:

Բաժին 1.4: Այս բաժինը ներկայացնում է հակիրճ ներածություն բանալիների պաշտպանության կենսաչափական մեթոդների վերաբերյալ:

Առաջին գլխի ամփոփումը բերված է ***բաժին 1.5***-ում:

Գլուխ երկրորդ: Աշխատանքի երկրորդ գլուխը նկարագրում է մատնահետքերի վրա հիմնված հեռահար նույնականացման առաջարկվող սխեման, որն օգտագործում է ստեգանոգրաֆիկ միջոցներ՝ մատնահետքային տվյալների անվտանգ փոխանցումը ապահովելու համար: Գլուխը բաղկացած է չորս բաժիններից:

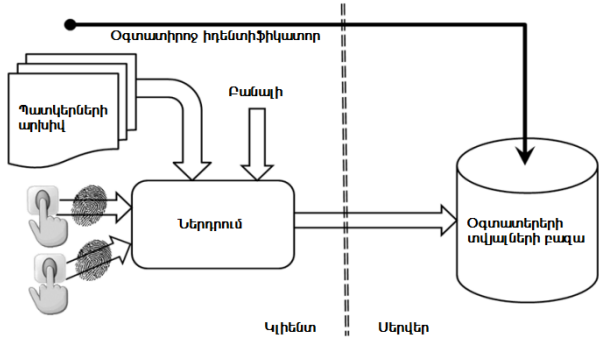
Բաժին 2.1: Բաժինը ներկայացնում է հեռահար նույնականացման պաշտպանության առաջարկվող մեթոդը և մատնանշում է այդ մոտեցման հետ կապված որոշ հնարավոր մարտահրավերներ:

Ենթաբաժին 2.1.1: Ենթաբաժնում առաջարկվում է կենսաչափական տվյալների նույնականացման և ամբողջականության հասկացությունների միավորման գաղափարը՝ սերվերային մասում օգտատիրոջ վավերականության ստուգումը իրականացնելու համար:

Ենթաբաժին 2.1.2: Ենթաբաժինը սխեմատիկորեն նկարագրում է առաջարկվող մեթոդը երեք տարբեր դեպքերի համար՝ օգտատիրոջ գրանցում, օգտատիրոջ նույնականացում կլիենտային մասում և օգտատիրոջ նույնականացում սերվերային մասում:

Օգտատիրոջ գրանցումը կատարվում է քայլերի ստորև թվարկված հաջորդականության միջոցով.

- Համապատասխան սկաների միջոցով ձեռք են բերվում օգտատիրոջ երկու մատների մատնահետքերը, որոնցից առաջինը հետագայում օգտագործվելու է նույնականացման, իսկ երկրորդը՝ ամբողջականության ստուգումները իրականացնելու համար:
- Օգտատիրոջ համակարգչում պահվող արխիվից ընտրվում է պատկեր, որը օգտագործվում է որպես ստեգանոգրաֆիկ կոնտեյներ:
- Երկու մատնահետքերի ձեռք բերված նկարները ներդրվում են ընտրված կոնտեյների մեջ:
- Կոնտեյները և օգտատիրոջ իդենտիֆիկատորը ուղարկվում են սերվերային մաս, որտեղ այդ տվյալները մուտքագրվում են օգտատերերի տվյալների բազա:



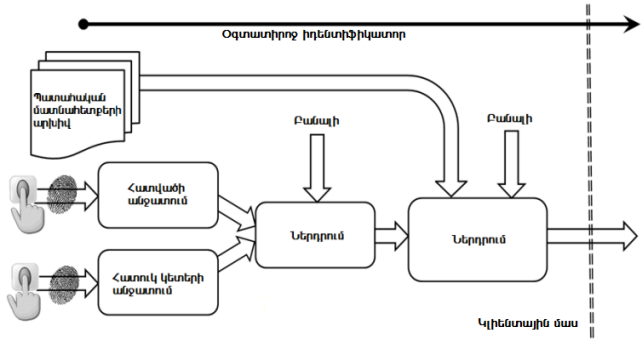
Նկ. 3. Օգտատերերի գրանցման ֆունկցիոնալ սխեման

Նկարագրված հաջորդականությունում որպես կոնտեյներ կարող է օգտագործվել օգտատիրոջ համակարգչում պահվող կամայական պատկերային ֆայլ, որի ձևաչափը համապատասխանում է ընտրված ստեգանոգրաֆիկ ալգորիթմին:

Նույնականացման փուլում, ինչպես կարելի է գուշակել, անհրաժեշտ է ձեռք բերել օգտատիրոջ նույն երկու մատների մատնահետքերը և ապահով կերպով փոխանցել դրանք սերվերային մաս: Ընդ որում, առաջարկվում է առաջին մատնահետքի նկարից անջատված հատուկ կետերը երկուական տեղեկության տեսքով ներդնել առաջին մատնահետքի նկարի մեջ որպես թվային ջրանիշ՝ մատնահետքային տվյալների աղբյուրի ամողջականությունն ապահովելու նպատակով:

Ելնելով վերը նշվածից, առաջարկվում է կլիենտային մասում իրականացվող նույնականացման մեթոդ, որի քայլերի հաջորդականությունը բերված է ստորև.

- Օգտատիրոջ այն երկու մատների նկարները, որոնք օգտագործվել էին գրանցման փուլում, ձեռք են բերվում համապատասխան սկաների միջոցով:
- Օգտատիրոջ համակարգչում պահվող արխիվից ընտրվում է պատկեր, որը օգտագործվում է որպես ստեգանոգրաֆիկ կոնտեյներ:
- Երկրորդ մատնահետքի նկարից անջատվում են հատուկ կետերը:
- Վերոհիշյալ հատուկ կետերը բնութագրող տվյալները ներդրվում են առաջին մատնահետքի նկարի մեջ որպես թվային ջրանիշ՝ օգտագործելով համապատասխան ալգորիթմ և բանալի:
- Առաջին մատնահետքի նկարը ներդրվում է ստեգանոգրաֆիկ կոնտեյների մեջ՝ օգտագործելով համապատասխան ալգորիթմ և բանալի:
- Ստեգանոգրաֆիկ կոնտեյները և օգտատիրոջ իդենտիֆիկատորը փոխանցվում են սերվերային մաս:

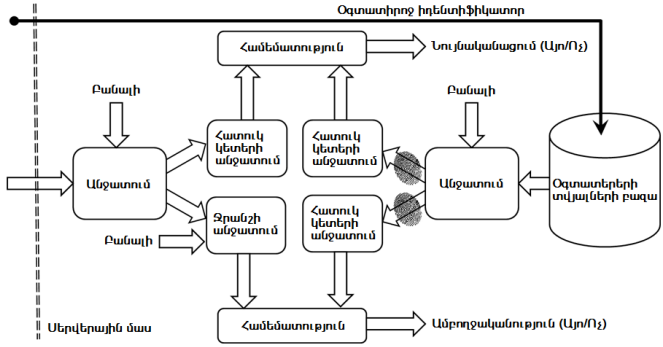


Նկ. 4. Կլիենտային մասում օգտատերերի նույնականացման ֆունկցիոնալ սխեման

Սերվերային մասում ստացված տվյալները մշակվում են քայլերի ստորև բերված հաջորդականությամբ.

- Սերվերային մասում պահվող օգտատերերի տվյալների բազայից ըստ ստացված իդենտիֆիկատորի դուրս է բերվում այն ստեգանոգրաֆիկ կոնտեյները, որը պարունակում է օգտատիրոջ մատնահետքային տվյալները:
- Ներդրված երկու մատնահետքերի նկարները անջատվում են կոնտեյներից:
- Նշված մատնահետքերի նկարներից անջատվում են հատուկ կետերը:

- Կլիենտային մասից ստացված կոնտեյներից անջատվում է օգտատիրոջ առաջին մատնահետքի նկարը:
- Նշված նկարից անջատվում է թվային ջրանիշը, որն իրենից ներկայացնում է օգտատիրոջ երկրորդ մատնահետքի նկարից անջատված հատուկ կետերը բնութագրող տեղեկություն:
- Տվյալների բազայից ստացված երկրորդ մատնահետքի նկարից անջատված հատուկ կետերի բազմությունը համեմատվում է անջատված թվային ջրանշի տվյալների հետ, և համեմատության հիման վրա կատարվում է եզրակացություն տվյալների աղբյուրի ամբողջականության վերաբերյալ:
- Կլիենտային մասից ստացված կոնտեյներից հանված մատնահետքի նկարից անջատվում են հատուկ կետերը:
- Նշված կետերի բազմությունը համեմատվում է տվյալների բազայից ստացված առաջին մատնահետքի նկարից անջատված հատուկ կետերի բազմության հետ, ինչի արդյունքում կատարվում է եզրակացություն տվյալների նույնականության վերաբերյալ:



Նկ. 5. Սերվերային մասում օգտատերերի նույնականացման ֆունկցիոնալ սխեման

Հարկ է նշել, որ ստեգանոգրաֆիկ կոնտեյներների մեջ մատնահետքային տվյալների ներդրման, ինչպես նաև կոնտեյներներից այդ տվյալների անջատման համար անհրաժեշտ է օգտագործել նույն բանալին: Նմանապես, նույն բանալին պետք է օգտագործել նաև թվային ջրանիշերի ներդրման և անջատման համար:

Ենթաբաժին 2.1.3: Ենթաբաժնում բերվում են առաջարկվող սխեմայի անվտանգությանը վերաբերվող որոշ դիտարկումներ: Չնայած մատնահետքերերի վրա հիմնված նույնականացման համակարգերը զբաղեցնում են գերիշխող դիրքեր կենսաչափական նույնականացման համակարգերի շուկայում, դրանք հաճախ ենթարկվում են հարձակումների նույնականացման գործընթացի տարբեր էտապներում: Հարձակումների ամենատարածված տեսակներից է մատնահետքերի կեղծ նկարների օգտագործումը: Այս կեղծ նկարները կարող են արտատպվել տարատեսակ մակերևույթներից, որոնց դիպել է իրական օգտատերը (օրինակ՝ ապակիներ, դռների բռնակներ և այլն): Նշված հարձակումների նկատմամբ խոցելիությունը միշտ համարվել է մատնահետքերի վրա հիմնված նույնականացման համակարգերի հիմնական թերությունը:

Առաջարկվող մեթոդը ինչ որ չափով մեղմում է նշված խոցելիությունը: Դիտարկենք համակարգի անվտանգությունը այնպիսի հակառակորդի (attacker) տեսանկյունից, ում հասանելի է հաղորդակցության ուղին և ով անօրինականորեն ձեռք է բերել իրական օգտատիրոջ մատնահետքի նկարը: Ենթադրենք, որ հակառակորդը որևէ կերպ կարողացել է կոտրել մատնահետքային նկարի՝ կոնտեյների մեջ տեղադրման ալգորիթմը, ինչը, իր հերթին, ստեգանոգրաֆիկ ալգորիթմի պատշաճ ընտրության դեպքում շատ դժվար է իրականացնել: Շնորհիվ առաջարկվող մեթոդի յուրահատկությունների, իրական օգտատիրոջ անունից հաջող նույնականացում անցնելու համար հակառակորդից կպահանջվեն հետևյալ լրացուցիչ քայլերը.

- գուշակել մատնահետքի նկարում թվային ջրանշի առկայության անհրաժեշտությունը,
- ձեռք բերել իրական օգտատիրոջ երկրորդ մատի հատուկ կետերի տվյալները, ինչը ակնհայտորեն ավելի բարդ խնդիր է, քան որևէ մակերևույթից պարզապես մատնահետքի նկարը արտատպելը,
- կոտրել թվային ջրանշման ալգորիթմը, ձեռք բերված հատուկ կետերի տվյալները առաջին մատնահետքի նկարում ներդնելու նպատակով, ինչը, ալգորիթմի պատշաճ ընտրության դեպքում նույնպես շատ բարդ խնդիր է:

Այսպիսով, կարելի է եզրակացնել, որ առաջարկվող սխեման մատնահետքերի վրա հիմնված նույնականացման համակարգին ավելացնում է անվտանգության լրացուցիչ շերտ:

Բաժին 2.2: Բաժինը ներկայացնում է մատնահետքի նկարից առավելագույն տեղեկություն պարունակող հատվածի անջատման և այդ հատվածում պարունակվող տեղեկության քանակության բարելավման առաջարկվող մեթոդները:

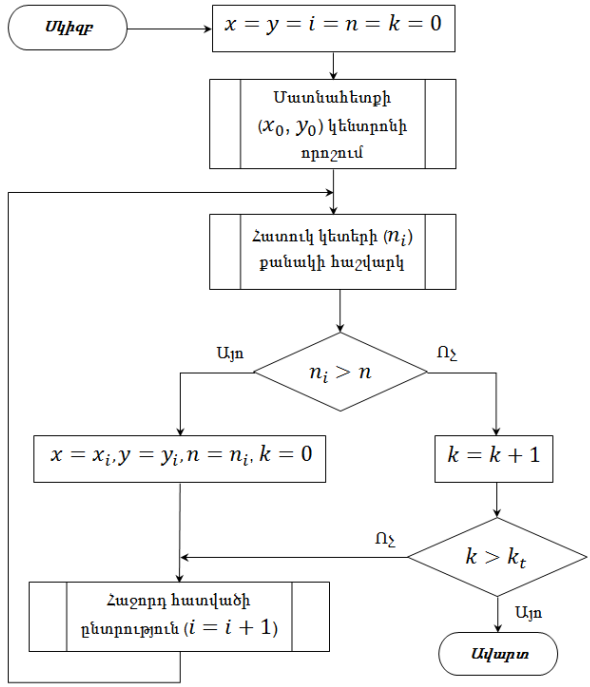
Ենթաբաժին 2.2.1: Ենթաբաժնում քննարկվում է մատնահետքի հատվածի երկրաչափական ձևը, և ապացուցվում է հատվածի՝ քառակուսու տեսքով ընտրության անհրաժեշտությունը:

Ենթաբաժին 2.2.2: Ենթաբաժնում բերվում են որոշ դիտարկումներ մատնահետքի հատվածի չափերի վերաբերյալ և եզրակացվում է, որ հատվածի կողմը պետք է որոշվի որպես $\lfloor\sqrt{P}\rfloor$, որտեղ P-ն ստեգանոգրաֆիկ կոնտեյների թողունակությունն է:

Ենթաբաժին 2.2.3: Ենթաբաժինը ներկայացնում է մատնահետքի նկարից առավելագույն տեղեկություն պարունակող հատվածի անջատման առաջարկվող մեթոդը: Հետագայում հնարավորինս ճշգրիտ նույնականացում ապահովելու համար հատվածը մատնահետքի նկարի վրա պետք է տեղադրվի այնպես, որ այն ընդգրկի առավելագույն քանակությամբ հատուկ կետեր: Հայտնի է, որ սովորաբար հատուկ կետերը հիմնականում կենտրոնացած են մատնահետքի կենտրոնական մասում, և եզրերի մոտ դրանց քանակը կտրուկ նվազում է: Այս պատճառով առաջարկվում է առավելագույն տեղեկություն պարունակող հատվածի որոնումը իրականացնել ընդլայնվող պարույրանման հետագծով, սկսելով մատնահետքի երկրաչափական կենտրոնից, ինչպես ցույց է տրված նկ. 6-ում:

Նկ. 6. Առավելագույն տեղեկություն պարունակող հատվածի որոնում

Առավելագույն տեղեկություն պարունակող հատվածի որոնման առաջարկվող ալգորիթմի բլոկ-սխեման ցուցադրված է նկ. 7-ում: Նախ զրոյական ելակետային արժեքներ են վերագրվում որոնելի հատվածի կենտրոնի x և y կոորդինատներին, ինչպես նաև ընթացիկ հատվածի համարին (i), ընթացիկ հատվածում հատուկ կետերի քանակին (n_i) և իտերացիաների քանակին (k):

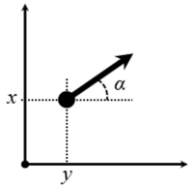


Նկ. 7. Առավելագույն տեղեկություն պարունակող հատվածի որոնման ալգորիթմ

Սխեմայում n-ով նշանակված է հատուկ կետերի այն առավելագույն քանակը, որը հանդիպել է արդեն դիտարկված հատվածներից որևէ մեկում: Հաջորդ քայլում որոշվում են մատնահետքի նկարի երկրաչափական կենտրոնի կոորդինատները և դրանք վերագրվում են սկզբնական հատվածի կոորդինատներին: Այնուհետև սկսվում է հատվածի որոնման ցիկլը: Հաշվարկվում է ընթացիկ հատվածում պարունակվող հատուկ կետերի n_i քանակը, որն այնուհետև համեմատվում է արդեն դիտարկված հատվածներում հատուկ կետերի առավելագույն n քանակի հետ: Եթե $n_i > n$ պայմանը տեղի ունի, ապա որոնելի հատվածի կենտրոնի x և y կոորդինատներին, ինչպես նաև դրանում պարունակվող հատուկ կետերի n քանակին վերագրվում են ընթացիկ հատվածի համապատասխան արժեքները (x_i, y_i, և n_i), և իտերացիաների k քանակը զրոյացվում է: Այլապես ($n_i \leq n$), իտերացիաների k քանակը ավելացվում է մեկով և համեմատվում է տրված k_t շեմի հետ: Եթե $k > k_t$ պայմանը տեղի ունի, ապա որոնման գործընթացը ավարտվում է, այլապես ալգորիթմը սկսում է դիտարկել հաջորդ հատվածը ($i = i + 1$): Որոնման գործընթացի ավարտից հետո x-ի և y-ի արժեքները որոշում են առավելագույն տեղեկություն պարունակող հատվածի կենտրոնի կոորդինատները: Գործնական կիրառություններում k_t շեմի արժեքը կարելի է ընտրել հատվածի սխալ ընտրման վիճակագրության հիման վրա:

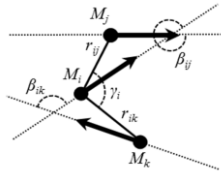
Ենթաբաժին 2.2.4: Ենթաբաժինը ներկայացնում է ընտրված հատվածում պարունակվող տեղեկության քանակի բարելավման առաջարկվող մեթոդը: Մատնահետքի նկարից հատվածի անջատման գործընթացում որոշակի քանակությամբ հատուկ կետեր դուրս են մնում ընտրված հատվածից, ինչը չի կարող բացասական ազդեցություն չունենալ սերվերային մասում իրականացվող նույնականացման գործընթացի վրա: Հատուկ կետերի նշված կորուստը փոխհատուցելու համար անհրաժեշտություն է առաջանում բարելավել ընտրված հատվածում պարունակվող տեղեկության քանակը:

Հատուկ կետը սովորաբար բնութագրվում է կոորդինատներով և կողմնորոշման անկյունով, ինչպես ցույց է տրված նկ. 8-ում:



Նկ. 8. Հատուկ կետի բնութագրիչները

Մատնահետքի նկարում պարունակվող տեղեկության քանակի բարելավման տեսանկյունից նպատակահարմար է դիտարկել հարևան հատուկ կետերի փոխադարձ դիրքը: $M_i(x_i, y_i, \alpha_i)$ հատուկ կետի դիրքը իրեն ամենամոտ գտնվող $M_j(x_j, y_j, \alpha_j)$ և $M_k(x_k, y_k, \alpha_k)$ հատուկ կետերի նկատմամբ (նկ. 9) տրվում է $V_i(r_{ij}, r_{ik}, \beta_{ij}, \beta_{ik}, \gamma_i)$ վեկտորի միջոցով, որտեղ r_{ij}-ն և r_{ik}-ն M_i հատուկ կետի հեռավորություններն են համապատասխանաբար M_j և M_k հատուկ կետերից, β_{ij}-ն և β_{ik}-ն հատուկ կետերի համապատասխան զույգերի կողմնորոշման անկյունների տարբերություններն են, իսկ γ_i-ն M_iM_j և M_iM_k սեգմենտների միջև կազմված սուր անկյունն է:



Նկ. 9. M_i հատուկ կետի դիրքը իրենից ամենափոքր հեռավորության վրա գտնվող M_j և M_k հատուկ կետերի նկատմամբ

Նկ. 9-ը ցույց է տալիս, որ V_i վեկտորը միարժեքորեն նկարագրում է M_i հատուկ կետը և կարող է օգտագործվել որպես լրացուցիչ տեղեկություն հատուկ կետերի բազմությունների համեմատության ընթացքում: Հետևաբար, փոխադարձ դասավորության $V_i(r_{ij}, r_{ik}, \beta_{ij}, \beta_{ik}, \gamma_i)$ վեկտորի դիտարկումը $M_i(x_i, y_i, \alpha_i)$ հատուկ կետի հիմնական բնութագրիչների հետ միասին թույլ է տալիս մեծացնել այն պարամետրերի քանակը, որոնք միարժեքորեն բնութագրում են հատուկ կետը: Սա նշանակում է, որ նկարագրված մոտեցումը հնարավորություն է տալիս իրականացնել նույն ճշգրտության նույնականացում՝ օգտագործելով ավելի քիչ քանակով հատուկ կետեր:

Ենթաբաժին 2.2.5: Ենթաբաժնում բերվում են առաջարկվող նույնականացման համակարգի անվտանգության որոշ գնահատականներ: Սերվերային մասում իրականացվող նույնականացման գործընթացում մատնահետքի նկարի հատվածից անջատված հատուկ կետերի բազմությունը անհրաժեշտ է համեմատել մատնահետքի ամբողջական նկարից անջատված հատուկ կետերի բազմության հետ: Կարելի է ենթադրել, որ սա կարող է ոչ միայն նվազեցնել նույնականացման գործընթացի որակը, այլ նաև մեծացնել համակարգի խոցելիությունը հատարկման եղանակով հարձակումների (brute force attacks) նկատմամբ:

Մատնահետքի նկարից անջատված հատվածի չափի ազդեցությունը համակարգի անվտանգության վրա գնահատելու համար օգտագործվել է մաթեմատիկական մոդել, որի նպատակն է մատնահետքերի վրա հիմնված նույնականացումը գաղտնաբառային նույնականացման հետ համեմատելը: Ըստ այս մոդելի, մատնահետքի նկարում դիրքերի առավելագույն քանակությունը, որտեղ կարող են գտնվել հատուկ կետեր, կարող է որոշվել հետևյալ բանաձևի միջոցով՝

$$N_m = \frac{X \times Y}{T^2},$$

որտեղ X-ը և Y-ը մատնահետքի նկարի չափերն են, արտահայտված պիքսելներով, իսկ T-ն մատնահետքի նկարի վրա հարակից ծալքերի միջև միջին հեռավորությունն է, նույնպես արտահայտված պիքսելներով:

Բացի կոորդինատներից, հատուկ կետերը տարբերվում են նաև ուղղությամբ, հետևաբար՝ անհրաժեշտ է հաշվի առնել նաև հատուկ կետի հնարավոր տարբեր ուղղությունների D թիվը: Ակնհայտ է, որ D թվի մեծացումը, նույնականացման որակը բարելավելու հետ միասին, կարող է զգալիորեն բարդացնել իրականացվող հաշվարկները: Ընդհանուր առմամբ, հավանականությունը, որ մատնահետքից անջատված հատվածի վրա պատահականորեն գեներացված հատուկ կետը կհամընկնի մատնահետքի ամբողջական նկարից անջատված հատուկ կետի հետ, կարող է որոշվել հետևյալ բանաձևով՝

$$P = \frac{N_p}{(N_m - N_f + 1) \times D},$$

որտեղ N_p-ն և N_f-ը հատուկ կետերի քանակություններն են համապատասխանաբար մատնահետքի ամբողջական նկարում և դրանից անջատված հատվածում:

Հավանականությունը, որ հենց t պատահականորեն գեներացված հատուկ կետեր կհամընկնեն մատնահետքի ամբողջական նկարից անջատված հատուկ կետերի հետ, կարող է որոշվել հետևյալ բանաձևով՝

$$P_t = P^t(1-P)^{N_f - t}:$$

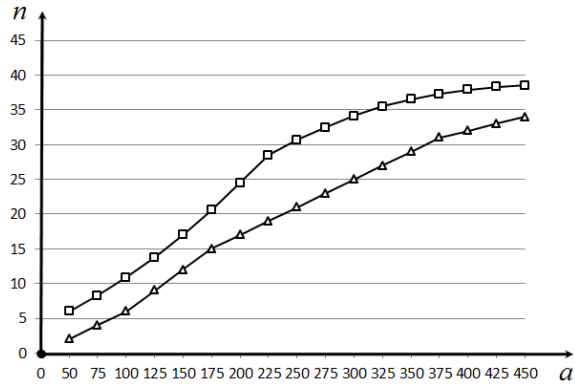
Մյուս կողմից, մատնահետքի ամբողջական նկարից անջատված հատուկ կետերի բազմությունից կարելի է ընտրել t կամայական հատուկ կետ $C_t^{N_p}$ եղանակներով: Հետևաբար՝ հաջող նույնականացման գումարային հավանականությունը՝ տրված t_t շեմի համար, կարող է որոշվել հետևյալ բանաձևով՝

$$P_a = \sum_{t=t_t}^{N_f} C_t^{N_p} \times P_t:$$

Մատնահետքի նկարից անջատված հատվածի հիման վրա գործող նույնականացման համակարգի անվտանգության համեմատական գնահատման համար նպատակահարմար է օգտվել բիթային b_s հզորության հասկացությունից, որը համապատասխանում է այնպիսի տեքստային բաղտնաբառի բիթերի քանակին, որն ունակ է ապահովել միևնույն մակարդակի անվտանգություն: Բիթային հզորությունը սահմանվում է հետևյալ կերպ՝

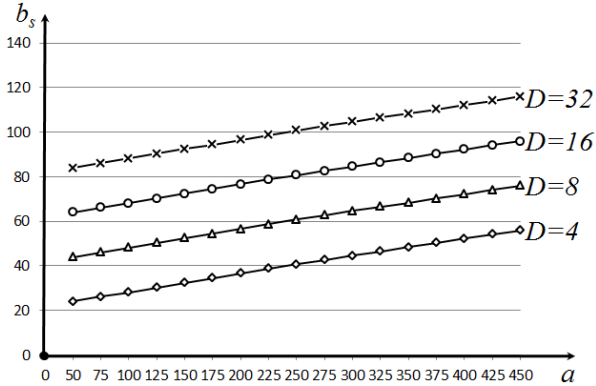
$$b_s = -\log_2 P_a:$$

Ենթաբաժին 2.2.6: Ենթաբաժնում բերվում են առաջարկվող լուծումների գործնական արդյունավետության գնահատականները: Այս նպատակով օգտագործվել է մատնահետքերի նկարների նմուշների FVC2004-DB1_B տվյալների բազան: Այս բազան պարունակում է 10 տարբեր մարդկանց մատնահետքերի նկարներ, յուրաքանչյուրը սկանավորված 8 անգամ՝ CrossMatch V300 օպտիկական սկաների միջոցով: Նկարները իրենցից ներկայացնում են 640x480 չափի, 500 dpi խորության և TIFF ձևաչափի պատկերներ: Մատնահետքի նկարից առավելագույն տեղեկություն պարունակող հատվածի որոշման մեթոդի արդյունավետությունը գնահատելու նպատակով տվյալների բազայում պահվող մատնահետքերի 10 բազային նկարներից յուրաքանչյուրից անջատվել են 50-ից 450 պիքսել չափի քառակուսային հատվածներ՝ 50 պիքսել քայլով: Նկ. 10-ում պատկերված է անջատված հատվածներում պարունակվող հատուկ կետերի n միջին քանակության կախվածությունը հատվածի կողմի a չափից երկու դեպքերում՝ երբ հատվածի տեղաբաշխումը մատնահետքի նկարի վրա ընտրվել է կամայականորեն և երբ այն ընտրվել է համաձայն առաջարկվող մեթոդի: Նկարից հստակ երևում է, որ հատվածների հավասար չափերի դեպքում առավելագույն տեղեկություն պարունակող հատվածի որոնման առաջարկվող մեթոդը ապահովում է ավելի մեծ քանակությամբ հատուկ կետեր, ինչի հաշվին կարող է ապահովել նույնականացման ավելի բարձր ճշգրտություն:



Նկ. 10. Անջատված հատուկ կետերի n միջին քանակության կախվածությունը հատվածի կողմի a չափից հատվածի կամայական (-△-) և ըստ առաջարկվող մեթոդի (-□-) ընտրությունների դեպքում

Նկ. 11-ը պատկերում է բիթային b_s հզորության կախվածությունը առավելագույն տեղեկություն պարունակող հատվածի a չափից՝ հատուկ կետերի հնարավոր ուղղությունների D քանակի տարբեր արժեքների դեպքում:

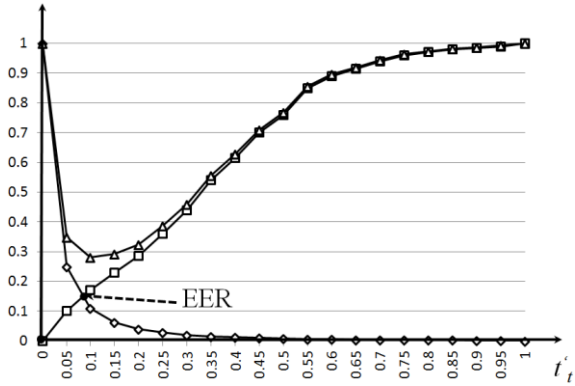


Նկ. 11. Բիթային b_s հզորության կախվածությունները առավելագույն տեղեկություն պարունակող հատվածի a չափից՝ հատուկ կետերի հնարավոր ուղղությունների D քանակի տարբեր արժեքների դեպքում

Վերլուծելով նկ. 11-ը՝ կարելի է նշել, որ հատվածի նույնիսկ փոքրագույն չափի (50 պիքսել) և $D = 16$ արժեքի դեպքում հատարկման եղանակով հարձակումների նկատմամբ նույնականացման համակարգի պաշտպանվածության աստիճանը համեմատելի է 8 կամայական նիշերից կազմված գաղտնաբառի պաշտպանվածության աստիճանի հետ, ինչը բավարար ցուցանիշ է գործնական կիրառությունների մեծամասնության համար: Նկ. 11-ից երևում է նաև, որ մեծացնելով հատվածի չափը կարելի է ապահովել համակարգի անվտանգության ավելի բարձր աստիճան:

Նույնականացման ճշգրտությունը սովորաբար գնահատվում է սխալ նույնականացման (false acceptance) և սխալ մերժման (false rejection) գործակիցների միջոցով:

Նույնականացման t_t շեմը որոշելիս նպատակահարմար է օգտվել նաև բացարձակ սխալի գործակցի (total error rate) հասկացությունից, որը սահմանվում է որպես սխալ նույնականացման և սխալ մերժման գործակիցների գումար: Նկ 12-ում պատկերված է նշված գործակիցների հաշվարկված կախվածությունը նույնականացման նվազեցված շեմից, որը սահմանվում է հետևյալ կերպ՝ $t'_t = t_t/N_f$:

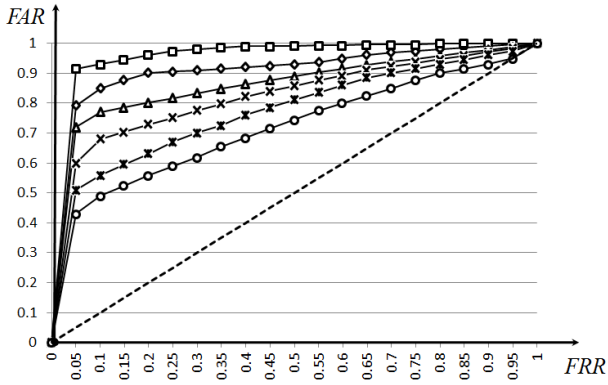


Նկ. 12. Սխալ նույնականացման (◆), սխալ մերժման (□) և բացարձակ սխալի (△) գործակիցների կախվածությունը նույնականացման նվազեցված t'_t շեմից

Ընդհանուր առմամբ, ճանաչման ալգորիթմը կայացնում է դրական կամ բացասական որոշում՝ ելնելով t'_t շեմի արժեքից: Ինչպես երևում է նկ. 12-ից, այս շեմը փոքրացնելիս նվազում է նաև սխալ մերժման գործակիցը, սակայն աճում է սխալ նույնականացման գործակիցը: Եվ ընդհակառակը՝ շեմի մեծացումը հանգեցնում է սխալ նույնականացման գործակցի նվազեցմանը, դրանով իսկ բարելավելով համակարգի անվտանգությունը, սակայն նվազեցնում է համակարգի օգտագործման հարմարավետությունը, քանի որ աճում է սխալ մերժման գործակիցը: Նկ. 12-ը ցույց է տալիս նույնականացման համակարգի մեկ այլ կարևոր բնութագրիչ, որն իրենից ներկայացնում է սխալ նույնականացման և սխալ մերժման գործակիցների կորերի հատման կետը, և կոչվում է հավասար սխալի գործակից (equal error rate):

Հաշվի առնելով այն փաստը, որ նույնականացման համակարգի կոնկրետ կիրառությունը հիմնականում նախորոք հայտնի չի լինում, ցանկալի է գնահատել համակարգի արդյունավետությունը շեմի բոլոր արժեքների դեպքում: Այս նպատակով սովորաբար օգտագործվում է սխալ նույնականացման և սխալ մերժման գործակիցների կախվածության կորը: Այս կորը կոչվում է ընդունիչ գործառնական բնութագիր (receiver operating characteristic): Այն հնարավորություն է տալիս համեմատել նույնականացման համակարգերը ընդհանուր անկախ չափանիշի հիման վրա:

Նկ. 13-ը պատկերում է հատուկ կետերի հնարավոր ուղղությունների քանակի $D = 8$ արժեքի պարագայում համակարգի ընդունիչ գործառնական բնութագիրը՝ առավելագույն տեղեկություն պարունակող հատվածի a չափի տարբեր արժեքների և մատնահետքի ամբողջական նկարի վրա հիմնված ավանդական նույնականացման դեպքում:



Նկ. 13. Ընդունիչ գործառնական բնութագիրը հատվածի կողմի տարբեր չափերի՝ a=50 (-O-), a=100 (-X-), a=200 (-Δ-), a=300 (-◇-), a=400 (-□-) և ավանդական նույնականացման (-✱-) դեպքում

Ինչպես երևում է նկ. 13-ից, հատվածի հիման վրա նույնականացման առաջարկվող մեխանիզմը հատվածի չափի 100 պիքսել նվազագույն արժեքի դեպքում ապահովում է ավելի մեծ ճշգրտություն, քան մատնահետքի ամբողջական պատկերի վրա հիմնված նույնականացումը: Ընդ որում, հատվածի չափի 50 պիքսել արժեքի դեպքում նույնպես համակարգի ճշգրտությունը ընդունելի է: Ընդհանուր առմամբ, ինչքան մոտ է ընդունիչ գործառնական բնութագրի կորը գծային ֆունկցիային, այնքան ավելի փոքր է նույնականացման համակարգի ճշգրտությունը:

Բաժին 2.3: Բաժնում բերվում է գոյություն ունեցող ստեգանոգրաֆիկ ալգորիթմների և անվտանգության պոտենցիալ սպառնալիքների վերլուծություն, և այդ վերլուծության հիման վրա ընտրվում է ստեգանոգրաֆիկ մեթոդ, որն ունակ է ապահովել կենսաչափական տվյալների անվտանգ փոխանցումը և պահպանումը: Բացի այդ, բաժնում փորձնականորեն ցուցադրվում է ընտրված մեթոդի արդյունավետությունը նույնականացման բոլոր փուլերում:

Ենթաբաժին 2.3.1: Ենթաբաժինը ներկայացնում է ստեգանոգրաֆիկ մեթոդների ընտրության հնարավորությունները՝ դասակարգելով այդ մեթոդները և վերլուծելով դրանց կիրառելիությունը առաջարկվող սխեմայում:

Ենթաբաժին 2.3.2: Ենթաբաժնում շեշտվում են հնարավոր սպառնալիքները և ստեգանոգրաֆիկ համակարգերի դեմ հնարավոր հարձակումները: Բացի այդ, ներկայացվում են նշված հարձակումների երկու ամենատարածված տեսակները՝ երկրաչափական և հաճախականային հարձակումները:

Ենթաբաժին 2.3.3: Ենթաբաժնում առաջարկվում է օգտագործել J3 ստեգանոգրաֆիկ ալգորիթմը մատնահետքի ամբողջական նկարի մեջ մեկ այլ մատնահետքի հատվածի ներդրման համար: Կատարվում է լցված և դատարկ ստեգանոգրաֆիկ կոնտեյներների փորձնական համեմատություն, ինչի արդյունքների հիման վրա եզրակացվում է, որ օգտագործելով մատնահետքային պատկեր, որպես ստեգանոգրաֆիկ կոնտեյներ և J3 ալգորիթմը, որպես տվյալների ներդրման մեթոդ, կարելի է ստանալ համակարգի բավականաչափ բարձր ստեգանոգրաֆիկ թողունակություն, ինչը թույլ կտա թաքցնել

մատնահետքի բավականաչափ մեծ հատված և իրականացնել ընդունելի ճշգրտության նույնականացում:

Ենթաբաժին 2.3.4: Ենթաբաժինը քննարկում է զանազան ստեգանոգրաֆիկ մեթոդների օգտագործման հնարավորությունները հատուկ կետերը բնութագրող տվյալները մատնահետքի նկարի հատվածի մեջ ներդնելու համար: Բերվում է նշված մեթոդների օգտագործմամբ գործնական փորձարկումների արդյունքների համեմատություն, ինչի հիման վրա եզրակացվում է, որ այս դեպքում նույնպես J3 ալգորիթմը կարող է արդյունավետորեն օգտագործվել հատուկ կետերի տվյալները մատնահետքի հատվածում ներդնելու նպատակով:

Երկրորդ գլխի ամփոփումը բերված է ***բաժին 2.4***-ում:

<u>Գլուխ երրորդ:</u> Գլուխը ներկայացնում է նույնականացման սխեմայի գործնական ծրագրային իրականացման արդյունքները: Գլուխը բաղկացած է չորս բաժիններից:

Բաժին 3.1: Բաժնում բերվում է վեբ ծառայություններում (web services), և մասնավորապես՝ WCF համակարգում օգտագործվող ավանդական նույնականացման մեխանիզմների հակիրճ նկարագիր:

Բաժին 3.2: Բաժինը ներկայացնում է առաջարկվող մեթոդի ծրագրային իրականացումը: Ստեղծված համակարգը բաղկացած է երկու առանձին մասերից՝ կլիենտային և սերվերային մոդուլներից: Սերվերային մոդուլը իրենից ներկայացնում է WCF կիրառություն, որը գործում է IIS 7 վեբ սերվերի միջավայրում: Գրանցված օգտատերերի տվյալները պահվում են Microsoft SQL Server 2008 R2 համակարգի ղեկավարությամբ գործող տվյալների բազայում: Կլիենտային մոդուլը իրենից ներկայացնում է WPF կիրառություն, որն օգտագործում է սերվերային կիրառության տրամադրած մեթոդները:

Բաժին 3.3: Բաժինը ներկայացնում է մատնահետքային պատկերների մշակման տարբեր ալգորիթմների իրականացումները առանձին ծրագրային մոդուլների տեսքով: Այդ մոդուլները օգտագործվում են ստեղծված ծրագրային համակարգի կլիենտային և սերվերային մասերում՝ մատնահետքերի հատուկ կետերի անջատման գործընթացի որակի բարելավման նպատակով:

Երրորդ գլխի ամփոփումը բերված է ***բաժին 3.4***-ում:

ԱՏԵՆԱԽՈՍՈՒԹՅԱՆ ՀԻՄՆԱԿԱՆ ԱՐԴՅՈՒՆՔՆԵՐԸ

1. Առաջարկվել է մատնահետքերի վրա հիմնված նույնականացման նոր սխեմա, որն օգտագործում է օգտատիրոջ երկու մատնահետքերը՝ անապահով կապուղով փոխանցված տվյալների նույնականությունը և ամբողջականությունը ստուգելու համար [1]:
2. Առաջարկվել է մատնահետքի նկարից առավելագույն տեղեկություն պարունակող հատվածի անջատման մեթոդ, որը թույլ է տալիս նվազեցնել տվյալների այն քանակությունը, որն անհրաժեշտ է փոխանցել կապուղով՝ նույնականացումը իրագործելու համար [2]:

3. Առաջարկվել է ընտրված հատվածում պարունակվող տեղեկության քանակության բարելավման մեթոդ, որը հնարավորություն է տալիս փոխհատուցել հատվածի անջատման փուլում տեղի ունեցած տեղեկության կորուստը և իրագործել ընդունելի ճշգրտության նույնականացում [2]:
4. Մշակվել են առաջարկվող նույնականացման սխեման կլիենտային և սերվերային մասերում իրականացնող ծրագրային մոդուլներ [3,4]:
5. Մշակվել են մատնահետքի նկարից առավելագույն տեղեկություն պարունակող հատվածի ընտրման, ինչպես նաև այդ հատվածում պարունակվող տեղեկության քանակի բարելավման առաջարկվող մեթոդները իրականացնող ծրագրային մոդուլներ [4]:

ԱՏԵՆԱԽՈՍՈՒԹՅԱՆ ԹԵՄԱՅՈՎ ՀՐԱՊԱՐԱԿՈՒՄՆԵՐԻ ՑԱՆԿ

[1] G. Khachatrian, N. Malkhasyan, Overview of Methods of Biometric Based Key Protection // Transactions of IIAP of NAS of RA “Mathematical Problems of Computer Science”, 2012, vol. 37, pp. 83-87.
[2] N. Malkhasyan, Authentication Based on a Selected Fingerprint Fragment // Proceedings of Engineering Academy of Armenia, 2012, vol. 9, pp. 863-871.
[3] N. Malkhasyan, Steganographic Data Protection for Fingerprint Based Authentication // Proceedings of Engineering Academy of Armenia, 2013, vol. 10, pp. 154-159.
[4] N. Malkhasyan, Securing Fingerprint Based Authentication Using Steganographic Techniques // “CyberSecurity for the Next Generation” International Student Conference, Russia & CIS Round, Conference Papers, Kaspersky Academy, Yerevan, 2013.

Malkhasyan Narek Ararat

SOME SECURITY ASPECTS OF FINGERPRINT DATA PROCESSING

ABSTRACT

The increasing computerization of society and the prevalence of the internet and "cloud" technologies lead to the fact that both organizations and individuals increasingly rely on modern informational tools. The increasingly complex IT infrastructure of enterprises and organizations, along with the changing nature of the threats and risks make information security a vital issue. However, quite different and effective information security methods can be practically useless if they are not reinforced by convenient and reliable means of authentication (identity establishment) of consumers of information services.

Recent years are characterized by steady increase in interest in biometric authentication methods, which are based on physiological and behavioral characteristics of the user, and which are far better than traditional means, such as passwords, ID cards, etc. One main reason for this popularity is the ability of biometric technology to relatively simply and easily distinguish legitimate users from hackers attempting to fraudulently obtain access rights to information resources. Currently the most common biometric based authentication technologies are the ones based on fingerprints, as these are the most convenient to use and the most cost-effective.

At the same time, an analysis of possible attacks on authentication systems based on fingerprints shows that one of the major challenges is ensuring the security and integrity of biometric data. It's obvious that the biometric data, despite having a high degree of uniqueness, in practice are poorly protected against copying, misuse and modification. Essentially, a biometric authentication system can work properly only if it is able to ensure that during enrollment and authentication data have been received from the relevant user and have not been subjected to external influence. Therefore, from the point of view of facilitating widespread use of biometric authentication methods, the task of protecting biometric data, in particular fingerprint data, becomes critical.

The implementation of the mentioned protection of biometric data through the use of steganographic techniques seems to be fairly promising. While cryptography is primarily focused on techniques designed to make the encrypted information meaningless to outsiders, steganography is based on the concealment of the fact of secret information existence. Steganographic techniques can be used to protect fingerprints, providing both security and integrity of data transmitted from the client to the server, or stored on the server. This can significantly reduce the chance of unauthorized acquisition of biometric data, thus reducing the likelihood of misuse or alteration.

Objective of the Work

The main objective of the work is to research and develop methods for securing fingerprint based remote authentication systems in all stages of functioning using steganographic techniques. The following issues are addressed in the work for achieving the mentioned goal:

- Construct a fingerprint based remote authentication method with steganographic data protection in all stages of functioning, which provides both security and integrity of the fingerprint data being transferred through an insecure channel.
- Develop a method for selecting the most informative fragment of a given size from the fingerprint image.
- Construct a method for increasing the informativeness of the selected fragment.
- Select appropriate steganographic algorithms for using them in the suggested authentication scheme.

Main Results of the Dissertation

1. A novel fingerprint based authentication scheme has been suggested, which uses the user's two fingerprints to check the authenticity and integrity of the fingerprint data transmitted through an insecure channel [1].
2. A method of selecting the most informative fragment from the fingerprint image has been presented, which allows reducing the amount of data that is required for performing authentication [2].
3. A method of increasing the informativeness of the selected fragment has been suggested, which allows compensating the loss of some amount of minutiae points at the stage of fragment selection, and performing authentication with an acceptable level of quality [2].
4. Software modules have been developed that are implementing the suggested authentication scheme for client and server parts [3,4].
5. Software modules have been developed that are implementing the presented method of most informative fingerprint fragment selection as well as the method of increasing the informativeness of the selected fragment [4].

Малхасян Нарек Араратович

НЕКОТОРЫЕ АСПЕКТЫ БЕЗОПАСНОСТИ ОБРАБОТКИ ДАННЫХ ОТПЕЧАТКОВ ПАЛЬЦЕВ

РЕЗЮМЕ

Растущая компьютеризация общества наряду с широким распространением интернет и “облачных” технологий приводит к тому, что повсеместно как организации, так и частные лица при решении своих насущных проблем вынуждены все больше полагаться на современные информационные средства. При этом постоянно усложняющаяся информационная инфраструктура предприятий и организаций наряду с изменяющейся природой угроз и рисков делают обеспечение информационной безопасности жизненно необходимой проблемой. Однако достаточно разнообразные и эффективные средства защиты информации могут оказаться практически бесполезными, если они не будут подкреплены удобными и надежными средствами аутентификации (установления подлинности) потребителей информационных услуг.

Последние годы характеризуются устойчивым повышением интереса к биометрическим средствам аутентификации, основанным на физиологических и поведенческих особенностях пользователя, которые выгодно отличаются от традиционных средств, таких как пароли, идентификационные карты и т.д. Одной из главных причин такой популярности является способность биометрических технологий, относительно просто и удобно, отличать легитимных пользователей от злоумышленников, пытающихся обманным путем получить права доступа к информационным ресурсам. В настоящее время наиболее распространенными остаются технологии, основанные на отпечатках пальцев, как самые удобные для использования и малозатратные.

При этом, как показывает анализ возможных атак на системы аутентификации на основе отпечатков пальцев, одной из основных проблем остается обеспечение безопасности и целостности биометрических данных. Можно заметить, что биометрические данные, обладая достаточно высокой степенью уникальности, практически мало защищены от копирования, неправомерного использования или изменения. По существу системы биометрической аутентификации могут работать корректно, только если они в состоянии гарантировать, что при регистрации и самой аутентификации данные поступили от соответствующего пользователя и не подверглись внешнему воздействию. В связи с этим, с точки зрения способствования широкому распространению биометрических методов, актуальным становится задача защиты биометрических данных, в частности отпечатков пальцев.

Защита отпечатков пальцев с использованием методов стеганографии представляется довольно перспективным. В то время как криптография в основном сосредоточена на методах, призванных сделать зашифрованную информацию бессмысленной для посторонних лиц, стеганография основана на сокрытии самого факта наличия секретной информации. Методы стеганографии могут использоваться для защиты отпечатков пальцев, с одинаковым успехом обеспечивая как безопасность, так и целостность данных,

передаваемых от клиента к серверу или хранимых на сервере. При этом существенно уменьшаются шансы овладения посторонними лицами биометрическими данными, следовательно, уменьшается вероятность их неправомерного использования или изменения.

Основная цель работы

Основной целью работы является исследование и разработка методов обеспечения безопастности систем дистанционной аутентификации на основе отпечатков пальцев на всех этапах функционирования с использованием стеганографических техник.

Для достижения данной цели в работе необходимо решить следующие задачи:

- Спроектировать метод удаленной аутентификации на основе отпечатков пальцев со стеганографической защитой данных на всех этапах функционирования, который обеспечивает безопасность и целостность данных отпечатков пальцев, передаваемых через незащищенный канал.
- Разработать метод выбора наиболее информативного фрагмента данного размера на поверхности отпечатка пальца.
- Спроектировать метод повышения информативности выбранного фрагмента.
- Выбрать соответствующие стеганографические алгоритмы для использования их в предложенной схеме аутентификации.

Основные результаты диссертации

1. Предложена новая схема аутентификации на основе отпечатков пальцев, которая использует отпечатки двух пальцев пользователя для проверки аутентичности и целостности данных в отдельности [1].
2. Предложен метод выбора наиболее информативного фрагмента на поверхности отпечатка пальца, который позволяет сократить объем данных, необходимых для выполнения аутентификации [2].
3. Предложен метод повышения информативности выбранного фрагмента, что позволяет компенсировать потерю некоторого количества точек минуций на этапе выбора фрагмента, а также выполнение аутентификации с приемлемым уровнем качества [2].
4. Разработаны программные модули, реализующие предложенную схему аутентификации на клиентской и серверной частях [3,4].
5. Разработаны программные модули, реализующие предложенный метод выбора наиболее информативного фрагмента на поверхности отпечатка пальца а также метод повышения информативности выбранного фрагмента [4].