ՀՀ ԳԱԱ ԻՆՖՈՐՄԱՏԻԿԱՅԻ ԵՎ ԱՎՏՈՄԱՏԱՑՄԱՆ ՊՐՈԲԼԵՄՆԵՐԻ ԻՆՍՏԻՏՈՒՏ

Խասիկյան Հովիկ Գառնիկի

ԿԵՆՍԱՉԱՓԱԿԱՆ ՏՎՅԱԼՆԵՐԻՑ ԳԱՂՏԱԲԱՌԵՐԻ ԳԵՆԵՐԱՑՄԱՆ ԱՐԴՅՈՒՆԱՎԵՏ ԵՂԱՆԱԿՆԵՐԻ ՄՇԱԿՈՒՄ

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

ՍԵՂՄԱԳԻՐ

Երևան – 2015

ИНСТИТУТ ПРОБЛЕМ ИНФОРМАТИКИ И АВТОМАТИЗАЦИИ НАН РА

Хасикян Овик Гарникович

РАЗРАБОТКА ЭФФЕКТИВНЫХ СХЕМ ГЕНЕРАЦИИ ПАРОЛЕЙ ИЗ БИОМЕТРИЧЕСКИХ ДАННЫХ

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՝ տեխ.գիտ. դոկտոր Դ.Գ.Ասատրյան
տեխ.գիտ.թեկնածու Ս.Բ.Ալավերդյան

Առաջատար կազմակերպություն՝
Հայաստանի պետական ճարտարագիտական համալսարան

Պաշտպանությունը կայանալու է 2015թ. Հունիսի 18-ին, ժ. 15.00-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.А. Хачатрян
Официальные оппоненты: доктор тех. наук Д.Г. Асатрян
кандидат тех. наук С.Б. Алавердян

Ведущая организация: Государственный инженерный университет Армении

Защита состоится 18-го июня 2015г. в 15.00 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 արդիականությունը: Ծածկագրական համակարգերում օգտագործվում են գաղտնի և բաց բանալիներ, որոնց իմացությունը պետք է լինի հստակ՝ համակարգի ճիշտ աշխատանքի համար: Սակայն այդ բանալիները չափազանց երկար են որպեսզի մարդիկ կարողանան հիշել: Այդ պատճառով այս բանալիները հիմնականում պաշտպանվում են մարդու հորինած գաղտնաբառով, որոնք մարդիկ կարող են հիշել:

Մարդկանց հորինած գաղտնաբառերը կարող են գուշակվել այն մարդկանց կողմից, ովքեր նրանց ճանաչում են կամ ունեն ինֆորմացիա նրանց անձնական տեղեկությունների մասին: Գաղտնաբառերը գուշակելու համար հաճախ օգտագործվում են նաև բառարանային հարձակումներ, քանի որ մարդիկ հորինում են իմաստալից ծածկագրեր: Ծածկագրերի մեկ այլ թերությունն այն է, որ մարդիկ կարող են դրանք մոռանալ:

Գաղտնի բանալիների պաշտպանության համար առաջարկվել է օգտագործել մարդու կենսաչափական տվյալները՝ այնպիսի մի բան, ինչը որ մարդն ունի և միշտ իր հետ է: Կենսաչափական տվյալները ի տարբերություն ծածկագրերի՝ շատ ավելի բարդ են և դրանք հնարավոր չէ գուշակել: Այս պատճառով բարձր անվտանգություն պահանջող համակարգերում, նույնականացման և ինքություն ճանաչման համար օգտագործվում են անձանց կենսաչափական տվյալները:

Նման համակարգերում ճանաչման համար պահվում են անձի կենսաչափական տվյալից ստացված բնութագրիչները: Որպես հետևանք այս համակարգերում կա ինֆորմացիայի արտահոսք, քանի որ պահոցին մուտք ունեցող անձը կամ հարձակվողը կարող է ձեռք տեսնել անձի կենսաչափական տվյալի բնութագրիչները և օգտագործել այս ինֆորմացիան իր անձնական նպատակների համար:

Անձի կենսաչափական տվյալի նմուշի և գաղտնի բանալու միաժամանակյա պաշտպանության համար առաջարկվել են կենսաչափական տվյալներից բանալիների գեներացման սխեմաներ, ինչպես նաև կենսաչափական տվյալների և գաղտնագրական բանալու զուգակցման սխեմաներ: Սակայն այս սխեմաները ունեն թերություններ, մասնավորապես վերծանման համար պահանջվող գործողությունների քանակը բավականին մեծ է, պահանջում են կենսաչափական տվյալի նախնական տեղաշտկում, ինչը բարդ խնդիր է մասնավորապես մատնահետքերի համար, ինչպես նաև պահվող հղումային ինֆորմացիան բավականին ապահով չէ և կարող է տալ ինֆորմացիայի ահտահոսք:

Այսպիսով պարզ է դառնում այնպիսի մի կենսաչափական համակարգի մշակման կարիքը, որը՝

- Կլինի հնարավորինս ճշգրիտ,
- Կլինի տեղաշտկումից անկախ,

- Պահվող հղումային տվյալներից ինֆորմացիայի արտահոսք չի լինի,
- Կունենա վերծանման պարզ մեխանիզմ,
- Թույլ է կտա կապել անձի կենսաչափական տվյալը գաղտնի բանալու հետ՝ տրամադրելով ինքնության անմերժելիություն,
- Կապահովի բարձր անվտանգություն:

Աշխատանքի նպատակն է մշակել ծածկագրական այնպիսի համակարգեր, որոնք չեն պահանջում կենսաչափական տվյալի տեղաշտկում, ինչպես նաև մշակել գաղտնի բանալու վերծանման տեսակետից պարզ կառուցվածք ունեցող սխեմա, որը կապահովի կենսաչափական տվյալի և գաղտնի բանալու կապ: Միևնույն ժամանակ ցանկալի է, որ այս սխեմաները լինեն հնարավորինս անվտանգ և արդյունավետ:

Հետազոտման մեթոդները: Աշխատանքում օգտագործված են մատնահետքերի մշակման, ձեռքի ափի երակների մշակման, բանալու կցմամբ գաղտնագրման համակարգերի անվտանգության վերլուծության մեթոդները:

Արդյունքների գիտական նորույթը

- Մշակվել է մատնահետքերից գաղտնաբառերի գեներացման նոր համակարգ:
- Մշակվել են ոչ հստակ բանալիային պահոցով սխեմայի բարձր արդյունավետությամբ և տեղաշտկումից ազատ տարբերակները:
- Մշակվել է պատահականորեն գեներացված գաղտնի բանալին և կենսաչափական տվյալների պարամետրերը զուգակցող արդյունավետ սխեմա և նրա հիման վրա ստեղծվել է ծրագրային համակարգ, որի միջոցով ստուգվել են առաջարկված սխեմաների արդյունավետությունը և անվտանգության աստիճանը:

Ստացված արդյունքների կիրառական նշանակությունը: Ստացված արդյունքների հիման վրա կառուցվել է կենսաչափական տվյալի և գաղտնագրական բանալու զուգակցման սխեմա, որը թույլ է տալիս կապ հաստատել օգտատիրոջ գաղտնի բանալու և նրա կենսաչափական տվյալի միջև: Այս սխեման օգտագործվել է մատնահետքի պատկերներով ինքնության ճանաչում իրականացնող համակարգ մշակելու համար:
Առաջարկված համակարգում գրանցվող կենսաչափական տվյալներից ստացված հղումային տվյալները ինֆորմացիայի արտահոսք չեն տալիս: Մատնահետքերից բնութագրիչ ինֆորմացիան ստանալուց հետո գաղտնի բանալու վերծանման և ստուգման գործընթացը բավականին արագ է (մեկ անձի համար 64 համեմատման գործողություն և հեշավորման համար պահանջվող գործողությունների քանակը կախված օգտագործվող հեշավորման ֆունկցիայի ընտրությունից): Մշակված

համակարգը թույլ է տալիս կատարել արդյունավետ և անվտանգ ինքնության ճանաչում տվյալների մեծ պահոցների համար:

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

Աշխատանքի արդյունքների ներդրումը: Ատենախոսության շրջանակներում մշակված կենսաչափական տվյալներից գաղտնաբառերի գեներացման եղանակների գաղտնագրման համակարգը ներդրվել է Հայաստանի ամերիկյան համալսարանում և օգտագործվում է այնտեղ դասավանդվող «Կիրառական Կրիպտոգրաֆիա» դասընթացների ընթացքում:

Պաշտպանության են ներկայացված հետևյալ դրույթները.

1. Կենսաչափական տվյալներից գաղտնի բանալիների գեներացման սխեման;
2. Ոչ հստակ բանալիային պահոցով սխեմայի բարձր արդյունավետությամբ և տեղաշտկումից ազատ տարբերակները:
3. Գաղտնի բանալու և կենսաչափական տվյալների զուգակցման սխեման, որը կապ է հաստատում օգտատիրոջ և իր կենսաչափական տվյալի միջև, ինչպես նաև ինքնության ստուգման համար պահանջում է գործողությունների փոքր քանակ: Այս սխեմայի հիման վրա մշակվել է անձի ինքնության ճանաչման գաղտնագրական համակարգ:

Աշխատանքի արդյունքները զեկուցվել են. Հայկական մաթեմատիկական միության տարեկան նստաշրջանում (2014թ., Երևան), ՀՀ ԳԱԱ ինֆորմատիկայի և ավտոմատացման պրոբլեմների ինստիտուտի ընդհանուր սեմինարում, ինչպես նաև ինստիտուտի Կոդավորման և ազդանշանների մշակման բաժնի մասնագիտական սեմինարներում:

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

Աշխատանքի կառուցվածքը և ծավալը: Ատենախոսությունը բաղկացած է ներածությունից, չորս գլուխներից, եզրակացությունից և 78 անուն օգտագործված գրականության ցուցակից: Աշխատանքի ընդհանուր ծավալն է 100 էջ՝ ներառյալ 46 նկար:

ԱՇԽԱՏԱՆՔԻ ԲՈՎԱՆԴԱԿՈՒԹՅՈՒՆԸ

Ներածության մեջ հիմնավորված է աշխատանքի արդիականությունը, ձևակերպված են աշխատանքի նպատակներն ու խնդիրները, բերված են պաշտպանության ներկայացվող հիմնական դրույթները:

Աշխատանքի **առաջին գլխում** նկարագրված են տարբեր տիպի կենսաչափական տվյալներ, դրանց առանձնահատկությունները, այդ տվյալներով աշխատող համակարգերի յուրահատկությունները և դերը նույնականացման մեջ: Այս գլխում առավել մանրամասն են դիտարկվել ձեռքի ափի երակները և մատնահետքերը, քանի որ այս կենսաչափական տվյալները կիրառվել են աշխատանքում առաջարկված սխեմաների իրագործման և փորձարկումների մեջ: Նկարագրվել է այս կենսաչափական տվյալներից բնութագրիչ կետերի ստացման ալգորիթմը:

Աշխատանքի **երկրորդ գլխում** դիտարկվել են կենսաչափական տվյալներից գաղտնաբառերի գեներացման սխեմաներ: Մասնավորապես վերլուծվել է Միխայիլ Մասլեննիկովի կողմից առաջարկված սխեման[1]: Այս համակարգը աշխատում է հետևյալ կերպ՝

- Սկանավորվում է անձի մատնահետքը, որն իրենից ներկայացնում է մոխրագույն, 8 բիթ խորությամբ մոխրագույն նկար
- Դրա վրա ընտրվում են համապատասխան քառակուսի նկարներ, որոնք օգտագործվում են ճանաչման փուլում և համակարգը փորձում է դրանք տեղադրել նույն տեղերում՝ ինչ – որ օրիգինալ մատնահետքի դեպքում:

Եթե այս քառակուսիների տեղադրությունները նույնն են ինչ գրանցման մատնահետքի դեպքում, ապա այս մատնահետքը համարվում է ճիշտ: Այս տեղադրությունները հետագայում օգտագործվում են գաղտնաբառերի գեներացման համար:

Սակայն նշված համակարգի ճշգրտությունը ցածր է և մեծ չափի բանալի գեներացնելու համար օգտատերը ստիպված է տրամադրել իր մատնահետքը մի քանի անգամ: Ճանաչման համար պահանջվող ժամանակը ևս բավականին երկար է և 3ԳՀց հաճախականությամբ անձնական համակարգիչների դեպքում պահանջում է մոտ 60 վայրկյան:

Աշխատանքում մեր կողմից կատարված բարեփոխումների արդյունքում Մասլեննիկովի համակարգի սխալ մերժման գործակիցը և սխալ ընդունման գործակիցը լավացվել են: Գրանցման փուլը տևում է 17 վրկ՝ նախկին 5 րոպեի փոխարեն, իսկ

[1] Масленников М.Е., “Практическая криптография”, БХВ-Петербург, 2003

նույնականացման փուլը 1 վայրկյանից ավելի քիչ, նախկին 10 վայրկյանի փոխարեն (ավելի փոքր չափսերով բնութագրիչ ընտրելու և շեմային արժեքի կիրառման շնորհիվ): Կատարվել է բնութագրիչ նկարների տեսքի օպտիմիզացում: Փորձերը ցույց են տալիս, որ քառակուսի տեսքով նկարները լավագույն արդյունքները չեն ցուցաբերում: Առաջարկվել են նոր տեսքով ավելի փոքր մակերեսով բնութագրիչ պատկերներ, որոնց օգնությամբ սխեման տալիս է ավելի բարձր ճշգրտություն և արագություն:

Նկատենք, որ նախկինում բնութագրիչ հատվածի յուրահատկությունը հաշվելու համար այդ բնութագրիչը համեմատվում էր նկարի մեջ մյուս բոլոր բնութագրիչների հետ 1 պիքսել քայլով: Այնուամենայնիվ, փորձերը ցույց տվեցին, որ սա անհրաժեշտ գործընթաց չէ: Բնութագրիչի յուրահատկությունը հաշվելու համար կարևոր հատվածները, որոնք որոշում են բնութագրիչի յուրահատկության աստիճանը, գտնվում են այդ բնութագրիչ պատկերից որոշ հեռավորության սահմաններում: Այս հատկությունը օգտագործելու համար ալգորիթմը աշխատում է հետևյալ կերպ՝

1. Յուրաքանչյուր բնութագրիչի համար հաշվվում է դրա յուրահատկությունը, այն համեմատելով իր հարևանների հետ,
2. Այս բնութագրիչները դասավորվում են յուրահտկության արժեքի նվազման կարգով,
3. Երբ բոլոր բնութագրիչները դասավորված են, մենք ընտրում ենք ամենայուրատուկ հատվածները և ստուգում դրանց ճշգրտությունը,
4. Բնութագրիչը տեղակայվում է նկարի վրա և գտնվում են դրան ամենամոտ բնութագրիչները,
5. Եթե շատ նման բնութագիրչ է գտնվում օրիգինալ բնութագրիչից ավելի հեռու, քան սահմանված հեռավորությունը, այդ բնութագրիչը համարվում է անվավեր և տեղափոխվում է համապատասխան իր նոր յուրահատկության արժեքի,
6. Ըստ յուրահատկության հաջորդ բնութագրիչն է դիտարկվում հետագա քայլերի համար:
7. Այս գործողությունները կատարվում են այնքան ժամանակ, մինչև գտնվեն անհրաժեշտ քանակությամբ պատկերներ:

Ճանաչման փուլում, բնութագրիչ պատկերը տեղայնացնելու համար առաջարկվել է մի նոր ալգորիթմ: Գրանցված բնութագրիչը նոր պատկերի վրա փնտրելու ժամանակ համեմատվում են բնութագրիչ պատկերի և հավակնորդ բնութագրիչ պատկերի առաջին տողերը: Սա ցույց է տալիս, թե արդյոք երկու բնութագրիչները ունեն նմանություն, թե համակարգը պետք է շարունակի որոնումները և դիտարկի հաջորդ հավակնորդ պատկերը:

Տրված կոորդինատներից բանալիներ գեներացնելու համար մշակվել է մոտարկման նոր մեթոդ: Նոր նկարից ստացված կոորդինատները մոտարկելու համար որոշվում են $((X_{օրիգինալ} - X_{նոր})\ mod\ 10)$ և $((Y_{օրիգինալ} - Y_{նոր})\ mod\ 10)$ արժեքները և պահվում տվյալների պահոցում հղումային նկարների հետ միասին (X, Y – ը բնութագրիչի պատկերի վերին ձախ կետի կոորդինատներն են):

Կատարվել է համակարգի կողմից գեներացված գաղտնաբառերի էնտրոպիայի վերլուծություն, որի արդյունքում առաջարկվել է գրանցման փուլում կատարել ևս մեկ լրացուցիչ գործողություն՝ բոլոր բնութագրիչ նկարները գտնելուց հետո դրանց ինդեքսները պատահականորեն խառնվում են, ինչի արդյունքում մեծանում է գաղտնաբառերի էնտրոպիան (պատահականությունը):

Անվտանգության կարևոր խոդիր է նաև մատնահետքի կեղծումը, որից խուսափելու համար խորհուրդ է տրվում օգտագործել գրանցված սկաներներ, որոնք կարող են ճշտել, թե արդյոք մատնահետքը ծածկված է արհեստական շերտով, թե ոչ[2,3]:

Աշխատանքի **երրորդ գլխում** դիտարկվել են կենսաչափական տվյալների և գաղտնագրական բանալիների զուգակցման սխեմաներ: Գլխի առաջին մասում նկարագրվում է «Ոչ հստակ բանալիային պահոցով» սխեման[4], որը գաղտնի բանալու կենսաչափական տվյալներով պաշտպանման ամենատարածված և բարձր արդյունավետություն ունեցող կիրառական սխեմա է: Ոչ հստակ բանալիային պահոցով սխեմայի անվտանգությունը հիմնված է չբերվող բազմանդամի վերականգնման խնդրի վրա: Այս սխեման նախատեսված է կենսաչափական տվյալներից ստացվող բնութագրիչների չկարգավորված խմբի հետ աշխատելու համար: Որպես այդպիսի բնութագրիչներ հանդես են գալիս, օրինակ մատնահետքի մինուցիայի կամ ձեռքի ափի երակների մինուցիաների կետերը:

Ենթադրենք այս համակարգում օգտագործողը ցանկանում է իր կենսաչափական տվյալներով պաշտպանել իր գաղտնագրական K բանալին: Դիտարկվում է 2^n – էլեմենտանոց վերջավոր F դաշտը և

[2] Antonelli, A., Cappelli, R., Maio, D., and Maltoni, D. (2006), "Fake Finger Detection by Skin Distortion Analysis," IEEE Transactions on Information Forensics and Security 1(3), 360–373 (2006).
[3] D. Baldisserra, A. Franco, D. Maio, and D. Maltoni, "Fake fingerprint detection by odor analysis," in Proc. Int. Conf. on Biometric Authentication (ICBA06) (2006).
[4] A. Juels and M. Sudan, "A fuzzy vault scheme," in Proceedings of IEEE International Symposium of Information Theory, Lausanne, Switzerland, p. 408, 2002.

1. Գեներացվում է K գաղտնի բանալին;
2. Այնուհետև օգտագործելով գաղտնի բանալին ստացվում են գաղտնի *p(x)* բազմանդամը

$$p(x) = a_0 + a_1x + a_2x^2 + a_3x^3 \dots$$

որտեղ $a_0, a_1, a_2 \dots$ գործակիցները n երկարության բիթային հաջորդականություններ են:

3. Սկանավորվում է կենսաչափական նմուշը և ստացվում է $w = \{x_1, x_2, \dots, x_s\}$ վեկտորը, որտեղ $x_0, x_1 \dots$ կենսաչափական տվյալի բնութագրիչ կետերն են և դրանք դիտարկվում են որպես չկարգավորված խումբ, որտեղ $x_i \in F$:
4. Համակարգը հաշվում է *p(x)* բազմանդամի արժեքները կենսաչափական տվյալ w – ի բոլոր էլեմենտների համար՝

$$y_i = p(x_i), \ \ i = 1, 2, \dots s$$

5. Ընտրվում են $r - s$ Fդաշտի պատահական էլեմենտներ (r-ը պահոցի չափն է), որոնք չեն պատկանում w-ին (կեղծ էլեմենտներ են)՝ $x_{s+1}, \dots, x_r$:
6. Այս կեղծ էլեմենտների համար ընտրվում են պատահական արժեքներ, այնպես որ, այդ արժեքները հավասար չեն բազմանդամի արժեքին այդ կեղծ կետում՝

$$y_i \neq p(x_i), \ \ i = s+1, s+2, \dots r$$

7. Այնուհետև այս էլեմենտները և իրենց համապատասխան արժեքների զույգերը՝ $\{(x_1, y_1), (x_2, y_2), \dots, (x_r, y_r)\}$ խառնվում են և գրանցվում տվյալների պահոցում: Գրանցվում է նաև K գաղտնի բանալու հեշ արժեքը՝ Hash(K):

Ոչ հստակ բանալիային պահոցով սխեմայում նույնականացումը իրականացվում է հետևյալ քայլերի միջոցով.

1. Օգտատերը կրկին սկանավորում է իր կենսաչափական տվյալը, որից գեներացվում է $w' = \{x'_1, x'_2, \dots, x'_s\}$ վեկտորը:
2. Համակարգը փնտրում է ստացված կետերը գրանցված պահոցում և ընտրում դրանց ամենամոտ գտնվող կետերի զույգերը:
3. Եթե ընտրված են բավականաչափ ճիշտ կետեր (n+1 Լագրանժի ինտերպոլյացիա իրականացնելու համար), ապա օգտագործելով (x_i, y_i) զույգերը, որոնցից մի մասը ճիշտ զույգեր են՝ համակարգը կարող է վերականգնել գաղտնի բազմանդամը, այսինքն գաղտնի բանալին, քանի որ գաղտնի բանալին կազմված է հենց բազմանդամի գործակիցներից:

4. Համակարգը ստուգում է վերականգնված գաղտնի բանալու ճշտությունը համեմատելով այն հղումային տվյալում գրանցված բանալու հեշ արժեքի հետ:

Ոչ հստակ բանալիային պահոցով սխեման մատնահետքերի համար իրագործվել է բազում հեղինակների կողմից: Մասնավորապես, բարձր արդյունքներ են ստացվել “Fuzzy vault for fingerprints” աշխատանքում[5], որտեղ որպես բնութագրիչ կետեր դիտարկվել են մինուցիայի կետերը, որոնք բաղկացած են X, Y կոորդինատից և θ անկյունից:

Գլխի երկրորդ մասում ներկայացվել է ոչ հստակ բանալիային պահոցով սխեմայի ձևափոխված տարբերակը: Ոչ հստակ բանալիային պահոցով սխեմայի վերլուծությունը ցույց է տվել, որ վերջինս կարող է ցուցաբերել ավելի ցածր սխալ մերժման գործակից, եթե կիրառվեն որոշ ձևափոխություններ: Տվյալների պահոցի կառուցման ժամանակ նախնական սխեմայում կարիք կար կենսաչափական տվյալների չափը կրճատելու, որը ինֆորմացիայի կորուստ է և ազդում է համակարգի ընդհանուր արդյունավետության վրա: Այս խնդիրը լուծելու համար աշխատանքում մշակվել է ոչ հստակ բանալիային պահոցով սխեմայի ձևափոխված նոր տարբերակ:

Ինչպես օրիգինալ Ոչ հստակ բանալիային պահոցով սխեմայում, այստեղ ևս F -ը n - չափանի վերջավոր դաշտ է: Գրանցման համար կենսաչափականշ նմուշը $w = \{x_1, x_2, \dots, x_s\}$, սակայն այս սխեմայում $x_i \in F$ պարտադիր պայման չէ: Գաղտի բազմանդամը $P(v)$ է: Բազմանդամի աստիճանը՝ n և գործակիցները պատկանում են F-ին: Գրանցման և նույնականացման փուլերը հետևյալն են:

Գրանցման փուլ

1. Գեներացվում է գաղտնի բանալի K
2. Օգտագործելով գաղտնի բանալու բիթերը ստացվում են գաղտնի բազմանդամ *p(v)*- ի գործակիցները՝
$$p(v) = a_0 + a_1 v + a_2 v^2 + a_3 v^3 \dots$$
3. Սկանավորվում է կենսաչափական նմուշը և ստացվում է $w = \{x_1, x_2, \dots, x_s\}$ վեկտորը, որտեղ $x_1, x_2 \dots$ կենսաչափական տվյալի բնութագրիչ կետերն են և դրանք դիտարկվում են որպես չկարգավորված խումբ: Այստեղ $x_i \in F$ պայմանը պարտադիր չէ:

[5] U. Uludag, S. Pankanti, and A. K. Jain, “Fuzzy vault for fingerprints” in Proceedings of Audio- and Video-Based Biometric Person Authentication, Rye Town, NY, pp. 310–319, July 2005.

4. Գեներացվում են s տարբեր պատահական արժեքներ՝ $q = (v_1, v_2, \dots, v_s)$:
5. Հաշվվում է *p(v)* բազմանդամի արժեքները q - ի բոլոր էլեմենտների համար՝

$$y_i = p(v_i), \quad i = 1, 2, \dots s$$

6. q հաջորդականությանը կցվում են պատահականորեն ընտրված $r - s$ կետեր $v_{s+1}, \dots, v_r$:
7. w հաջորդականությանը կցվում են պատահականորեն ընտրված $r - s$ կետեր $\{x_{s+1}, \dots, x_r\}$:
8. Ընտրել $r - s$ պատահականորեն տարբերվող արժեքներ՝ $y_i \in F, \quad i = s + 1 \dots r$ այնպես, որ $y_i \neq P(v_i)$
9. Պահպանել տեղերով խառնված $\{(x_1, y_1, v_1), \dots, (x_i, y_i, v_i)\}$ եռյակները որպես հղում տվյալների պահոցում: Նշանակենք այս պահոցային ինֆորմացիան $ms(w)$: Պահոցում գրանցվում է նաև K գաղտնի բանալու հեշ արժեքը՝ Hash(K):

Նույնականացման փուլի նպատակը գաղտնի բազմանդամ $P(v)$-ի վերականգումն է, որից կարելի ստանալ գաղտնի բանալին (քանի որ բազմանդամի գործակիցները գաղտնի բանալու բիթերն են): Այսպիսով նույնականացման փուլի գործողությունները հետևյալն են՝

1. Օգտատերը սկանավորում է իր կենսաչափական տվյալը և համակարգը որոշում է կենսաչափական տվյալը բնութագրող $w' = \{x'_1, x'_2, \dots, x'_s\}$ վեկտորը:
2. Համակարգը փնտրում է ստացված կետերը գրանցված պահոցում և ընտրում դրանց ամենամոտ գտնվող կետերի խումբը:
3. Եթե w'-ը համընկնում է հղումային $ms(w)$ տվյալի հետ առնվազն $n + 1$ կետերում, ընտրվում են համապատասխան (x_i, y_i, v_i) եռյակները բազմանդամի վերականգնման համար:
4. Օգտագործելով (y_i, v_i) զույգերը համակարգը վերականգնում է բազմանդամը օգտագործելով Լագրանժի ինտերպոլյացիան:
5. Համակարգը ստուգում է գաղտնի բանալու ճշտությունը համեմատելով այն հղումային տվյալում գրանցված բանալու հեշ արժեքի հետ:

Այս սխեմայի առավելությունն այն է, որ կարիք չկա տվյալների կրճատման, ինչը կատարվում է ոչ հստակ բանալիային պահոցով աշխատող կենսաչափական տվյալների

մեծ մասի դեպքում[6,7,8]: Պետք է նշել նաև որ նկարագրված սխեմայի դեպքում օգտագործողը ազատ է ընտրել, թե որ Գալուայի դաշտի վրա է ցանկանում կառուցել սխեման: Եվ, որպես այս ձևափոխությունների արդյունք, այլևս տեղի չի ունենա ինֆորմացիայի կորուստ գրանցման փուլում, ինչի արդյունքում այս սխեմայում ստանում ենք նույնականացման առավել բարձր արդյունավետության:

Երրորդ գլխի երրորդ մասում ներկայացված է ոչ հստակ բանալիային պահոցով սխեմայի տեղաշտկումից ազատ տարբերակը: Մատնահետքի համար ոչ հստակ բանալիային պահոցով սխեման իրականացնելու համար անհրաժեշտ է կատարել մատնահետքի տեղաշտկում, որը պատկերի մշակման բարդ խնդիր է: Այս խնդիրը ոչ հստակ բանալիային պահոցով սխեմայի համար դեռևս սպառիչ լուծում չի ստացել, մասնավորապես այն պատճառով, որ տեղաշտկման համար գրանցվող տվյալները պետք է մատնահետքի մինուցիաների մասին ինֆորմացիան չտան: Այդ պատճառով այս գլխում առաջարկվել է ոչ հստակ բանալիային պահոցով սխեմայի տեղաշտկումից ազատ տարբերակը: Առաջարկվող մեթոդում, որպես պահոցի կողպման/բացման միավոր դիտարկվում է մինուցիայի կետերի շրջակայքում գտնվող տեղային տեքստուրային բնութագրիչները: Մինուցիայի կետերի ստացումից հետո, դիտարկվում է 32x32 չափի պատկերներ, որոնց վերին ձախ անկյան կետը համընկնում է մինուցիայի կետին, իսկ վերին կողի դիրքը համընկնում է մինուցիայի կետի անկյան ուղղությանը:
Երբ օգտատերը նույնականացման համար սկանավորում է իր մատնահետքը, այն կարող է ունենալ տարբեր դիրքեր, սակայն յուրաքանչյուր մինուցիային առընթեր կորի ուղղությունը մատնահետքի համեմատ մնում է նույնը, ինչը նշանակում է, որ ստացված 32x32 չափի բնութագրիչ պատկերի տեսքը կախված չէ մատնահետքի դիրքից: Սկանավորման ժամանակ արտաքին գործոնների ազդեցությամբ պատկերը աղմուկոտ է ստացվում, որը ֆիլտրվում է մատնահետքի նկարի նախամշակման փուլում:
Ստացված բնութագրիչները քվանտացվում են օգտագործելով տեղային բնութագրիչի նկարագրության ֆունկցիան (*Local Texture Descriptors, LTD*) [9]: *LTD* ֆունկցիան որպես մուտք վերցնում է 32x32 չափի բնութագրիչ պատկեր, որը բինար մատրից է և հաշվարկում է 16

[6] U. Uludag, S. Pankanti, and A. K. Jain, “Fuzzy vault for fingerprints” in Proceedings of Audio- and Video-Based Biometric Person Authentication, Rye Town, NY, pp. 310–319, July 2005.

[7] Y. J. Lee, K. Bae, S. J. Lee, K. R. Park, and J. Kim, “Biometric key binding: fuzzy vault based on iris images,” in Proceedings of 2nd International Conference on Biometrics, Seoul, South Korea, pp. 800–808, August 2007.

[8] A. Kumar and A. Kumar, “Development of a new cryptographic construct using palmprint-based fuzzy vault,” in EURASIP Journal on Advances in Signal Process, December 2009.

[9] S. Chikkerur, S. Pankanti, A. Jea, N. Ratha, and R. Bolle, —Fingerprint representation using localized texture features‖ International Conference on Pattern Recognition, 521-524, 2006

բիթ կոդ այդ մուտքային մատրիցի համար: Հաշվարկված կոդը համարվում է պահոցի կողպման/բացման միավոր: Սխեմայի աշխատանքում մնացած գործողությունները կատարվում են նույն կերպ, ինչպես ոչ հստակ բանալիային պահոցով սխեմայի դեպքում:

Երրորդ գլխի չորրորդ մասում ներկայացվում է ոչ հստակ բանալիային պահոցով սխեմայի անվտանգության վերլուծությունները, որոնք ցույց են տալիս, որ այս սխեմայի անվտանգությունը մատնահետքերի համար 39 բիթ է (չհաշված վերծանման համար պահանջվող գործողությունները, մոտ 2^{20} գործողություններ): Ոչ հստակ բանալիային պահոցով սխեման վերծանման գործողությունների մեծ քանակության պատճառով 1000 օգտատեր ունեցող պահոցում անձի ինքնության ճանաչում իրականացնելու համար պահանջում է մոտ 5 րոպե՝ 3 Գեգահերց (ԳՀց) հաճախականությամբ համակարգչի դեպքում: Հաշվի առնելով անվտանգության պարամետրերը, ինչպես նաև այն, որ որոշ գաղտնագրական համակարգերում կարևոր է լուծել անձի ինքնության ճանաչման խնդիրը, այս գլխի հինգերորդ մասում առաջարկվել է կենսաչափական տվյալների և գաղտնագրական բանալու զուգակցման նոր սխեմա: Այս բաժնում ներկայացված նոր սխեման հետապնդում է մի քանի նպատակ:

- պաշտպանել որևէ պատահական թվերի գեներացման ալգորիթմով ստացված գաղտնի բանալին օգտատիրոջ կենսաչափական տվյալով և
- կապել անձի կենսաչափական տվյալը իր բաց կամ գաղտնի բանալու հետ:

Ցույց է տրվել, թե որքան արդյունավետ կարելի է զուգակցել պատահականորեն գեներացված գաղտնի բանալին: Այս համակարգում առաջին քայլը օգտատիրոջ $B = (b_1, b_2, \dots, b_N)$ կենսաչափական տվյալի ծածկագրումն է $S = (s_1, s_2, \dots, s_N)$ գաղտնի բանալիով, որի արդյունքում ստացվում է հղումային $R = (r_1, r_2, \dots, r_N)$ վեկտորը: Այստեղ $r_i = ((b_i + (1 - s_i) * a/2) \bmod a)$, $i = 1, 2, \dots, N$, a–ն կենսաչափական կորի ամպլիտուդն է:

Վերծանման փուլում սկանավորվում է $B' = (b'_1, b'_2, \dots, b'_N)$ նոր կենսաչափական տվյալը: Օգտագործելով B' վեկտորը և R ծածկագրված հղումային տվյալը, սխեման վերականգնում է S գաղտնի բանալին, օգտագործելով հետևյալ բանաձևը՝

$$s_i = \left\lceil \frac{|r_i - b_i| - t}{a} \right\rceil$$

Այս սխեման փորձարկվել է մատնահետքերի համար: Բնութագրիչ կետերի ստացման համար մատնահետքի մոխրագույն նկարը ենթարկվում է նախամշակման և դրանից ստացվում է բինար պատկեր: Այս բինար մատրիցից ալգորիթմը ընտրում է այսպես կոչված հետաքրքրության տիրույթ (*region of interest, ROI*), որը մատնահետքի կենտրոնական և ամենաինֆորմատիվ մասն է (M_e մատրից): M_e մատրիցի վերին ձախ անկյունը նշանակվում է որպես բնութագրիչների հաշվարկման զրոյական կոորդինատ: 30x30 չափի առաջին ենթամատրից M_0-ի համար հաշվարկվում է մինիմալ Հեմինգյան հեռավորություն (H_0) նույն չափի բոլոր մատրիցների միջև, որոնց վերին ձախ անկյունի կոորդինատը գտնվում է M_0 մատրիցի զրոական կոորդինատից 3-ից 11 կետ վեր, ներքև, աջ և ձախ: Երկու մատրիցների միջև (M_p և M_r) Հեմինգյան հեռավորության հաշվարկի համար օգտագործվել է հետևյալ բանաձը՝

$$\sum_{i,j}(a_{i,j}^{p} \oplus a_{i,j}^{r})$$

որտեղ $a_{i,j}^{p}$ և $a_{i,j}^{r} \subset (0,1)$ համապատասխանաբար M_p և M_r մատրիցների կետեր են:
Ստացված մինիմալ Հեմինգյան հեռավորություն H_0-ն դիտարկվում է որպես զրոյական կոորդինատի արժեք: Հաջորդ կետը, որի համար հաշվարկվում է H_1-մինիմալ Հեմինգյան հեռավորությունը, գտնվում է առաջին կետից 10 կետ աջ: H_1-ի հաշվարկման համար կատարվում են նույն գործողությունները իր հարևանների հետ: $H_0, H_1, \dots, H_7$ առաջին 8 էլեմենտները գտնվում են M_e մատրիցի առաջին տողում: Հաջորդ 8 էլեմենտները ($H_7, H_8, \dots, H_{15}$) գտնվում են առաջին տողից 10 պիքսել ներքև, և այսպես շարունակ: Արդյունքում, սխեման մատնահետքի պատկերից հաշվարկում է 64 արժեք: Այս 64 կետերը պետք է գտնվեն միմյանցից բավականաչափ հեռու, այնպես որ դրանց միջև կապ չլինի, ինչը թույլ կտա հարձակվողին գուշակել գաղտնի բանալու բիթերը: Պետք է ստուգել, որ ընդհանուր դեպքում այն կետերը, որոնց արժեքների միջև տարբերությունը կենսաչափական տվյալի տատանման ամպլիտուդի 1/4-ից ավելի մեծ են (կամ 1/4-ից փոքր) գրեթե հավասարաչափ են բաշխված և կուտակումներ չունեն:

Այս սխեմայում գաղտնի բանալու վերականգնման համար պարտադիր չէ գրանցել գաղտնի բանալու հեշ արժեքը, իսկ գաղտնի բանալու վերծանման համար պահանջվող գործողությունների քանակը շատ փոքր է (ընդամենը 64 համեմատություն մատնահետքերից ստացված բնութագրիչ կետերի համար): Սա կարևոր առավելություն է, քանի որ անձի ինքնության ճանաչում իրականացնող համակարգերում վերծանման գործողությունների քանակը պետք է լինի հնարավորինս փոքր:

Ոչ հստակ բանալիային պահոցով սխեման կենսաչափական տվյալը մշակելուց հետո ստանում է մինուցիայի կետերի խումբը, որոնց օգնությամբ փորձում է բացել

օգտատիրոջ ծածկագրական բանալին: Բանալին վերծանելու համար սխեման պետք է պահոցից ընտրի մինուցիայի կետերին մոտ զույգեր և օգտագործելով այդ կետերն ու նրանց համապատասխան արժեքները, փորձի վերականգնել գաղտնի բանալին: Բազմանդամի գործակիցների վերականգնման գործողությունների քանակը փորձնականորեն գնահատվել է 2^{20}, ինչը 3ԳՀց հաճախականությամբ համակարգչի դեպքում տևում է մոտ 1.5 վայրկյան:

Այսպիսով, 200 օգտատեր պարունակող տվյալների պահոցի դեպքում անձի ինքնության ճանաչումը տևում է մոտ 300 վայրկյան կամ 5 րոպե: Սա նպատակահարմար արագություն չէ կիրառական համակարգերում ներդրման համար: Մյուս կողմից առաջարկվող բանալիային կցման սխեման նախամշակման և կենսաչափական բնութագրիչների ստացումից հետո պահանջում է կատարել 2^6 համեմատման գործողություններ: Արդյունքում նույն պահոցի համար անձի ինքնության ճանաչումը տևում է մոտ 1 վայրկյան:

Չորրորդ գլխում բերվում է մատնահետքերով աշխատող FingerGram գաղտնագրական համակարգի նկարագրությունը, որը թույլ է տալիս՝

- Բաշխված բաժանմունքներ ունեցող կազմակերպություններում գրանցել աշխատակիցներին, անձնական տվյալների և մատնահետքի և գաղտնի բանալու զուգակցման արդյունքում ստացված հղումային ինֆորմացիայի հետ միասին: Այս հղումային տվյալը օգտատիրոջ մատնահետքի մասին ինֆորմացիա չի տալիս, սակայն նրա օգնությամբ կարելի է միարժեքորեն որոշել անձի ինքնությունը;
- Վերահսկել աշխատակիցների մուտքը և ելքը, սկանավորելով նրանց մատնահետքը և ստուգելով սերվերից ստացված պատասխանը անձի մատնահետքի համընկման մասին:

Համակարգը կառուցված է այնպես, որ եթե նույնիսկ հարձակվողին հաջողվի ձեռք բերել սերվերում գրանցված անձանց տվյալները բաց տեսքով, նա միևնույն է չի կարող վերծանել օգտատիրոջ գաղտնի բանալին կամ կենսաչափական տվյալը: Համակարգը բաղկացած է երեք հիմնական մասերից՝ սերվերից, ադմինիստրատորի պատուհանից և հաճախորդային պատուհանից (բոլորը գրված են Java լեզվով):
Այս համակարգը իրականացնում է անձի ինքնության ճանաչում, որն ի տարբերություն նույնականացման ալգորիթմի, առավել խիստ պահանջներ է դնում օգատգործվող սխեմայի ռեսուրսատարության վրա, քանի որ ինքնության ճանաչման համար համակարգը պետք է համեմատի նոր սկանավորված մատնահետքի

համապատասխանությունը պահոցում գրանցված բոլոր օգտատերերի մատնահետքերի հետ:

Այս համակարգի կառուցման համար օգտագործվել է երրորդ գլխի հինգերորդ բաժնում նկարագրված կենսաչափական տվյալների և գաղտնի բանալիների զուգակցման սխեման: Այս սխեման կարող է պաշտպանել 64 բիթանոց գաղտնի բանալի, որն առավել անվտանգ է, քան ոչ հստակ բանալիային պահոցով սխեմայի անվտանգությունը (59 բիթ՝ անվտանգության 39 բիթ + վերծանման 20 բիթ): Ոչ հստակ բանալիային պահոցով սխեման այստեղ նպատակահարմար չէ նաև վերծանման համար պահանջվող գործողությունների մեծ քանակի պատճառով:

Չնայած մատնահետքի նախամշակումը երրորդ գլխի հինգերորդ բաժնում բերված սխեմայում տևում է մոտ 1 վայրկյան, բանալու վերծանման համար պահանջվում է ընդամենը 2^6 գործողություններ: Սա նշանակում է, որ 1000 օգտատերերի բանալիների վերծանման և ստուգման համար կպահանջվեն մոտ 2^{16} համեմատության գործողություն և 1000 հեշավորման գործողություն:

Չնայած 64 բիթը ժամանակակից գաղտնագրական համակարգերում բանալու անվտանգ չափ չի համարվում, համակարգը կարող է աշխատել երկու մատնահետքերով, որի դեպքում կապվող բանալու բիթերի քանակը կլինի 128 բիթ:

ԱՇԽԱՏԱՆՔԻ ՀԻՄՆԱԿԱՆ ԱՐԴՅՈՒՆՔՆԵՐԸ

- Մշակվել է մատնահետքերից գաղտնաբառերի գեներացման նոր ընթացակարգ [1]:

- Մշակվել են ոչ հստակ բանալիային պահոցով սխեմայի բարձր արդյունավետությամբ և տեղաշտկումից ազատ տարբերակներ [2,4]:

- Մշակվել է պատահականորեն գեներացված գաղտնի բանալու և կենսաչափական տվյալների պարամետրերի զուգակցման արդյունավետ սխեմա, որի հիման վրա մշակվել է անձի ինքնության ճանաչում իրականացնող ծրագրային համակարգ [3]:

[1]. G. Khachatryan, H. Khasikyan. “Correlation-Based Password Generation from Fingerprints” International Journal "Information Models & Analyses" (IJIMA) Volume 1 Number 2, 2012, pp. 123-133

[2]. G. Khachatryan, A. Jivanyan, H. Khasikyan. “Alignment-Free Fuzzy Vault Scheme for Fingerprints” Computer Science and Information Technologies, IEEE, 2013, pp. 1-6

[3] G. Khachatryan, H. Khasikyan. “Binding secrets with biological data: How close can we get?” Fundamental Concepts in Information Theory” (Asian Europian Worksopp 8) year 2013, pp. 32-38, Kamakura, Kanagawa, JAPAN

[4]. H. Khasikyan. “*A Modified Fuzzy Vault Scheme for Increased Accuracy*”, Transactions of IIAP NAS RA, Mathematical Problems of Computer Science, vol. 43, 2015, pp. 47-51.

РЕЗЮМЕ

Хасикян Овик Гарникович

“Разработка эффективных методов генерации паролей из биометрических данных”

В данной работе исследуется проблема связывания криптографических паролей с биометрическими данными. Автоматические системы для биометрического распознавания используются в течении последних нескольких десятилетий. Тем не менее, эти системы хранят биометрические данные пользователей в открытом виде, что создает проблемы конфиденциалности и утечки информации.

В работе рассматриваются два разных типа решения – генерация паролей из биометрических данных и связывание криптографических ключей с биометрическими данными пользователей.

Для генерация паролей из биометрических данных была рассмотрена и усовершенствована схема генерации паролей из отпечатков пальц, основанная на корелляции рисунков. В предлагаемой схеме система выбирает уникальние образцы из изображения отпечатка пальца и использует их координаты для получения пароля защиты криптографического ключа.

Эта схема генерирует пароль с длиной 84 бит из отпечатка пальца. Система сохраняет небольшие части биометрических шаблонов в базе данных с другой информацией пользователя и использует их для восстановления правильного пароля, когда пользователь сканирует свои пальцы.

Были рассмотрены схемы связывания криптографических ключей с биометрическими данными пользователя, в частности “нечетких множеств”. Эта схема используется для работы с неупорядоченными наборами характеристик биометрических данных и, поэтому, очень хорошо подходит для использования минуций (для отпечатков пальцев, вен, ладоней и т.д.). Для этой схемы были предложены несколько методов, которые дают возможность обойти необходимость выравнивания отпечатков пальц и получить более высокую оценку точности.

В следующей части работы была введена новая схема для связывания криптографических ключей с биометрическими данными. Эта схема обеспечивает более высокую безопасность, чем схемы “нечетких множеств”. Кроме того предложенная схема требует гораздо меньше операций для проверки личности, чем схемы “нечетких множеств”. И, поэтому, она была использована построения криптографического программного обеспечения безопасной идентификации личности.

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

- Разработана новая методология для генерации паролей из отпечатков пальцев [1].
- Предложены и разработаны модифицированные версии схем "нечетких множеств" с более низкими оценками ложных отказов и не требующими выравнивания отпечатков [2,4].
- Разработана новая схема связывания криптографического ключа с параметрами биометрических данных и на ее основе разработано программное обеспечение безопасной идентификации пользователей для больших баз данных с использованием отпечатков пальцев [3].

ABSTRACT

Hovik G. Khasikyan

“Development of effective methods for password generation from biometric data”

In this paper the problem of securing cryptographic constructions with biometric data is investigated. Automatic biometrics matching systems have been used for the last decades for making secure identification of the registered users. However, these systems keep the biometric data of the users openly, which is a privacy issue and an information leakage.

To overcome these issues, in this paper two different approaches to this problem are analyzed - password generation from biometric data and binding cryptographic keys with biometric data of the users.

For password generation from biometric data, in this paper a correlation-based password generation scheme for fingerprints was analyzed and enhanced. In the syggested scheme, the system chooses unique patterns from fingerprint images and uses their locations to obtain a password which is being used to protect cryptographic key.

This scheme is developed for fingerprints and the length of the password obtained from fingerprint data is 84bit. This system keeps small parts of biometric templates as references, which are then used to reconstruct the correct password when the users scan their biometric data.

As a key binding scheme, was analyzed the "fuzzy vault” scheme. This scheme uses order invariant characteristics of biometric data to make enrollment and generates reference data which gives no information about the biometric template and the secret key. At the authentication step these characteristics are obtained again and the system tries to open the secred key using these characteristics and reference data. Systems allows some of the characteristics to be wrong or to be missed, therefore it is very suitable to use with minutie data (fingerpint, palm-vein, etc.).

For this scheme there have been proposed several methods that make it possible to bypass the alignment step for the fingerprint authentication. In addition, a modified version of this scheme was suggested, which shows better estimates for the false rejection rate of this scheme.

In the next part if the work, a new scheme was developed for binding cryptographic keys with biometric data. This scheme provides higher security than the fuzzy-vault scheme. In

addition, the suggested scheme requires much less operations for authentication than the fuzzy vault scheme and therefore it was used to develop a cryptographic construction for fingerprint based identification, which is also described in this work.

During the research carried within this study, the following results were obtained:

- A new correlation-based password generation methodology was developed for fingerprint data [1].
- Modificated versions of the “Fuzzy-Vault” shceme were developed, one of which dos not require alignment and the other version allows to receive lower false non-mtach rate (FRR) [2,4].
- A new scheme was developed for binding biometric data of users with their cryptographic secret, on the base of this scheme software solution was developed to allow secure identification of the registered users within large databases [3].