Л.К. АНДРЕАСЯН

ПРОЕКТИРОВАНИЕ СЕТИ НА ОСНОВЕ FOG ДЛЯ СБОРА И ОБРАБОТКИ МЕДИЦИНСКИХ ДАННЫХ

Представлено проектирование сети на основе технологии Fog to Cloud (F2C) для организации процессов сбора и обработки больших медицинских данных с различных датчиков и гаджетов.

Ключевые слова: F2C, Fog узел, сенсоры, гаджеты, оконечные устройства, большие данные.

L.K. ANDREASYAN

FOG-BASED NETWORK DESIGN FOR COLLECTING AND PROCESSING OF MEDICAL DATA

The network design based on Fog to Cloud (F2C) technologies for collecting and processing big medical data from different sensors and gadgets is introduced.

Keywords: F2C, Fog node, sensors, gadgets, edge devices, big data.

ՀՏԴ 004.056.5

Ռ.Գ. ՀԱԿՈԲՅԱՆ

ԹԱՔՆԱԳՐՈՒԹՅՈՒՆ՝ ՊԱՏԿԵՐԻ ՄԵՋ ԿԻՐԱՌԵԼՈՎ ՄԱԹԵՄԱՏԻԿԱԿԱՆ ՖՈՒՆԿՑԻԱՆ ՈՐՊԵՍ ԲԱՆԱԼԻ

Ուսումնասիրվում է ինֆորմացիայի փոխանցումը, որը թաքնագրվում է պատկերի մեջ մաթեմատիկական ֆունկցիայի միջոցով որոշված տեղերում՝ LSB թաքնագրման մեթոդով, ինչի շնորհիվ երրորդ կողմը տեղյակ չի լինում գաղտնի ինֆորմացիայի փոխանակման և նրա դիրքի մասին: Ինֆորմացիան վերծանելու համար ստացող կողմից կպահանջվի իմանալ թաքցված ինֆորմացիայի դիրքը պատկերի մեջ:

Առանցքային բառեր. թաքնագրություն, թաքնագրություն պատկերի մեջ, գաղտնի հաղորդակցություն, մաթեմատիկական ֆունկցիա, LSB մեթոդ, գունային պալիտրայի ձևափոխում:

Ներածություն: Ներկա ժամանակում, երբ ինֆորմացիայի տարածումը կատարվում է արագ և մեծ ծավալներով, ինֆորմացիայի անվտանգության և ամբողջականության պահպանումը լուրջ խնդիր է: Խնդիրը լուծելու համար անհրաժեշտ է ինֆորմացիայի պաշտպանություն:

Տվյալների պաշտպանությունը կազմակերպվում է երկու հիմնական մոտեցմամբ.

1. գաղտնագրություն,
2. թաքնագրություն:

Գաղտնագրության ժամանակ ինֆորմացիան բացահայտորեն տեղափոխվում է, բայց փոխակերպված է լինում անընթեռնելի տվյալների, որոնց ապակոդավորումը անհնար է՝ առանց հատուկ բանալու [1]:

Թաքնագրությամբ գաղտնի է պահվում տվյալների գոյությունը, ոչ թե դրանց պարունակությունը, ինչը իր հերթին չի գրավում ավելորդ ուշադրություն, պահպանում է տվյալները ամբողջական և սահամափակում է հասանելիությունը [2]:

Խնդրի ձևաչափը և մեթոդիկայի հիմնավորումը: Աշխատանքում օգտագործված է թաքնագրության եղանակը, երբ գաղտնի ինֆորմացիան պահվելու է պատկերի պիքսելների մեջ բիթերի փոխանակման միջոցով:

Որպես կրիչ-պատկերի ձևաչափ ընտրվում է .TIFF-ը, քանի որ այն օգտագործվում է մեծ չափերով և բարձր որակով պատկերների պահպանման և աշխատանքի համար: TIFF ձևաչափը կարող է չսեղմվել կամ օգտագործել առանց կորուստների սեղմման (lossless) ալգորիթմ, ինչի շնորհիվ այս ձևաչափը տարածված է գրաֆիկական դիզայներների և լուսանկարիչների շրջանում, տպագրական մեդիայում:

.TIFF ձևաչափում ամեն գույնի համար հատկացվում է 8 բիթ, սակայն բարձրորակ պատկերների համար ամեն գույնին կարող է հատկացվել նաև 16 բիթ, և այդպիսով TIFF ձևաչափի պատկերների ամեն պիքսել զբաղեցնում է 24 կամ 48 բիթ համապասխանաբար [3]:

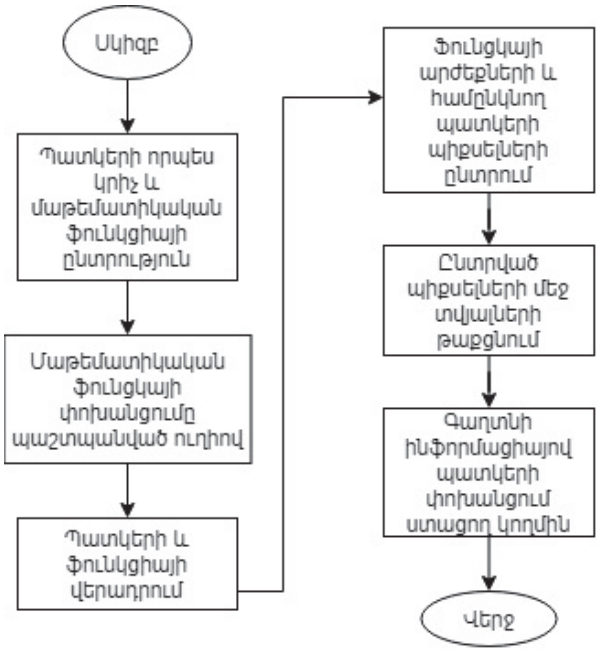
Այդ նպատակով մշակվել է եղանակ, որը պատկերի բիթերի մեջ կպահպանի գաղտնի տվյալներ, օգտագործելով գաղտնի մաթեմատիկական ֆունկցիայի արժեքները, որոնք կապահովեն բարձր թաքնակայունություն:

Որպես գաղտնի բանալի օգտագործվելու է նախապես ընտրված f(x) ֆունկցիան, որի գրաֆիկը մտացածին ծածկելու է պատկերը :

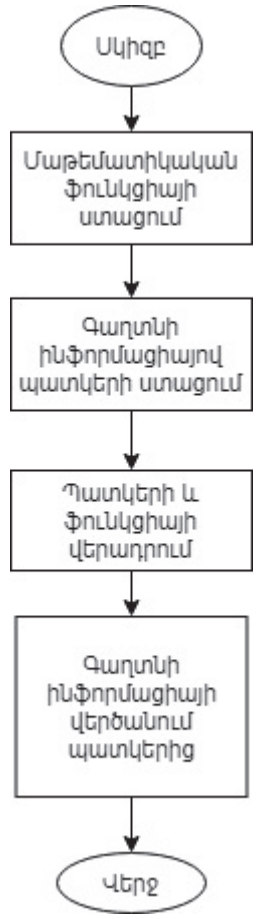
Արդյունքում կրիչի վրա կունենանք երևակայան գիծ, որի արժեքների պիքսելների մեջ կպահվի գաղտնի ինֆորմացիան: Որպես f(x) ֆունկցիա կարող է ընտրվել կամայական ֆունկցիա. այս դեպքում հիմնական խնդիրը տվյալը թաքցնելու ժամանակ ամբողջ թվերի առկայություն է՝ փոփոխվող պիքսելների ընտրության համար, ֆունկցիայի լուծումների բազմությունում:

Թաքնագրված ինֆորմացիան բացահայտելու համար անհրաժեշտ է գաղտնիորեն փոխանցել f(x) ֆունկցիան ինֆորմացիայի հասցեատիրոջը: Դա կարելի է իրագործել անմիջական հանդիպման ժամանակ կամ RSA ալգորիթմի միջոցով, ժամանակ առ ժամանակ փոփոխելով գաղտնի ֆունկցիան:

Թաքնագրող ծրագրի աշխատանքը: Թաքնագրող ծրագիրը ստանում է օգտագործողից մաթեմատիկական ֆունկցիան, գաղտնի ինֆորմացիան և պատկերը, որի մեջ պահվելու է գաղտնի ինֆորմացիան (նկ. 1 և 2):



Նկ. 1. Ուղարկող կողմի գործողությունների բլոկ-սխեման



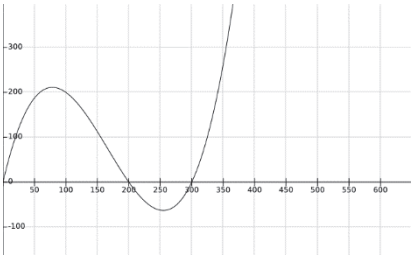
Նկ. 2. Սրացող կողմի գործողությունների բլոկ-սխեման

Կարդացվում է գաղտնի ինֆորմացիան, ամեն սիմվոլ փոխարինվում է ASCII կոդի, և հաշվվում են նրանց բիթային չափերը: Օգտագործելով մաթեմատիկական ֆունկցիան՝ ստեղծվում է գրաֆիկը, որը հետագայում կվերադրվի կրիչ-պատկերի վրա: Գրաֆիկը վերադրելով պատկերի վրա՝ ստանում ենք պիքսելների բազմություն, որը համապատասխանում է ֆունկցիայի արժեքների բազմությանը: Սակայն տվյալ մեթոդով պիքսելների ընտրության հետ առաջանում են որոշակի բարդություններ, քանի որ ֆունկցիայի ոչ բոլոր արժեքներն են

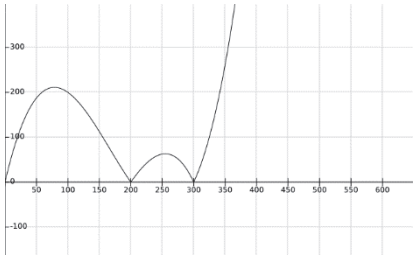
տեղավորվում պատկերի տարածքում, կամ ամբողջ և դրական թվեր են: Տվյալ խնդիրը լուծվում է մաշտաբավորման, մոդուլավորման և ամբողջացման միջոցով:

Մաշտաբավորման ժամանակ ֆունկցիայի մաքսիմալ արժեքը բաժանվում է պատկերի ուղղահայաց պիքսելների քանակի վրա, որից ստացվում է մաշտաբավորման գործակիցը, որով մաշտաբավորվում է ամբողջ կորը:

Ինչ-որ դեպքերում ֆունկցիայի արժեքները կարող են ստացվել բացասական: Այդ դեպքում մինչ մաշտաբավորումը կատարվում է արժեքի մոդուլավորում: Նկ. 3 և 4-ում ցուցադրված են արժեքները մինչև մոդուլավորումը և մոդուլավորումից հետո համապատասխանաբար:



Նկ.3. Արժեքները՝ առանց մոդուլավորման



Նկ.4.Արժեքները՝ մոդուլավորումից հետո

Ծրագիրը կարդում է պատկերը, ստացվում են նրա չափերը, ձևաչափը և գունային մոդելը: Գունային մոդելից կախված՝ հայտնի է դառնում, թե քանի շերտից է կազմված յուրաքանչյուր պիքսել:

Հաշվելով հասանելի պիքսելների քանակը և բազմապատկելով շերտերի քանակով, ստանում ենք հասանելի բիթերի քանակը: Համեմատելով դրանք գաղտնի ինֆորմացիայի չափերի հետ, ստուգում ենք, որպեսզի ինֆորմացիայի չափերը չգերազանցեն թաքցնելու համար նախատեսված բիթերի քանակը:

Այս գործողություններից հետո սկսվում է ընտրված պիքսելների՝ բայթերի փոխարինումը LSB մեթոդով: Այս մեթոդի իմաստը կրիչի (նկար, աուդիո ձայնագրություն կամ տեսանյութ) փոքրագույն նշանակություն ունեցող բիթերի փոխարինումն է, որից հետո փոփոխությունը կլինի անըմբռնելի մարդու զգայական օրգանների համար [4]:

RGB գունային մոդելի դեպքում ամեն պիքսել բաղկացած է երեք բայթից, որոնցից յուրաքանչյուրը պատասխանատու է մեկ գույնի համար՝ կարմիր, կանաչ և կապույտ: Պիքսելի մեջ ինֆորմացիա թաքցնելու համար պիքսելի ամեն բայթի վերջին բիթի արժեքը փոխարինվում է անհրաժեշտ արժեքով:

Վերոնշյալ գործողություններից հետո ստացված պատկերը չի ունենում չափերի փոփոխության և տեսողական տարբերություններ (նկ. 5 և 6):

Նկ. 5. Կրիչ-պատկերը՝ մինչև ինֆորմացիայի թաքնագրումը

Նկ. 6.Կրիչ-պատկերը՝ ինֆորմացիայի թաքնագրումից հետո

Եզրակացություն: Մշակված եղանակով հնարավոր է փոխանցել ինֆորմացիան ստացողին՝ առանց երրորդ կողմի՝ ինֆորմացիայի դիրքի մասին կամ նույնիսկ նրա գոյության մասին տեղեկացված լինելու: Համակարգի թերությունն այն է, որ երրորդ կողմը ամեն դեպքում կարող է վերծանել թաքցված ինֆորմացիան, եթե ունենա կրիչ-պատկերը մինչև ձևափոխումը կամ ուժային գրոհի միջոցով:

ԳՐԱԿԱՆՈՒԹՅԱՆ ՑԱՆԿ

1. **Կոնհայմ Ջ.Ա.** Համակարգչի անվտանգություն և գաղտնագրություն. - ԱՄՆ, Ջոն Վայլի և որդիներ, Inc., 2007. - 516 էջ:
2. **Al-Omari, Zaid & Al-Taani, Dr. Ahmad.** A Survey on Digital Image Steganography // 7th International Conference on Information Technology (ICIT 2015) /Al-Zaytoonah University. - Amman, Jordan, May 2015. - P. 1-8.
3. **Biman E., Qem N., Hemilton D.** TIFF Revision 6.0 Final. - Սիեթլ, Ալդուս Քորպորաշիոն, 1992. - 120 էջ:
4. **Garg Mukesh, Gurudev Zagra A.P.** An Overview of Different Type of Data Hiding Scheme in Image using Steganographic Techniques // International Journal of Advanced Research in Computer Science and Software Engineering. - 2014. - P. 746-751.

Р.Г. АКОПЯН

СТЕГАНОГРАФИЯ В ИЗОБРАЖЕНИИ С ИСПОЛЬЗОВАНИЕМ В ВИДЕ КЛЮЧА МАТЕМАТИЧЕСКОЙ ФУНКЦИИ

Исследуется передача информации, которая скрыта в изображении в точках, определенных математической функцией, с помощью метода шифрования LSB. Это не позволяет третьей стороне узнать об обмене конфиденциальной информацией и ее местонахождении. Получатель должен знать местоположение скрытой информации на изображении, чтобы декодировать информацию.

Ключевые слова: стеганография, стеганография в изображении, секретная коммуникация, математическая функция, метод LSB, модификация цветовой палитры.

R.G. HAKOBYAN

STEGANOGRAPHY IN IMAGE USING THE MATHEMATICAL FUNCTION AS A KEY

The transmission of information hidden in the image in places designated by the mathematical function using the LSB encryption method is studied. This does not allow the third party to be aware of the exchange of confidential information and its location. The recipient is required to know the location of the hidden information in the image to decode the information.

Keywords: *s*teganography, image steganography, secret communication, mathematical function, LSB encryption method, color palette modification.

ՀՏԴ 004.056.5

Լ.Ա. ԲԱԼԱԳՅՈՉՅԱՆ

ԹԱՔՆԱԳՐՈՒԹՅՈՒՆ ԳՐՍՖԻԿԱԿԱՆ ԱՆԻՄԱՑԻԱՅԻ ԿԱԴՐԵՐՈՒՄ

Երկու կողմերի միջև փոխանակվող ինֆորմացիան հաճախ թիրախ է դառնում երրորդ կողմի համար: Ուստի առաջանում է խնդիր ինֆորմացիան անհասանելի պահել երրորդ կողմից: Այդ խնդրի լուծման համար ուսումնասիրվել է ինֆորմացիայի թաքնագրումը, և մշակվել է մեթոդ՝ ինֆորմացիան թաքնագրելու անիմացված պատկերի կադրերի մեջ: Կադրերը ստացվում են ընտրված գրաֆիկական անիմացիայից, որոնց մեջ թաքնագրվում է նախապես մասնատված ինֆորմացիան LSB թաքնագրման մեթոդով, ինչի շնորհիվ երրորդ կողմը տեղյակ չի լինում գաղտնի ինֆորմացիայի առկայության մասին: Ինֆորմացիան վերծանելու համար ստացող կողմից կպահանջվի դուրս բերել այն անիմացիայի կադրերից:

Առանցքային բառեր. գաղտնի ինֆորմացիայի թաքնագրություն, թաքնագրություն պատկերի մեջ, կրիչ-պատկեր, գաղտնի հաղորդակցություն, անիմացիոն պատկեր, LSB մեթոդ, գունային պալիտրայի ձևափոխում:

Ներածություն: Ինֆորմացիան կարևորագույն ռեսուրսներից մեկն է, ուստի առաջանում է անհրաժեշտություն՝ այն ապահով պահելու կողմնակի անձանցից: Դրան հասնելու համար կան բազմաթիվ եղանակներ, որոնցից տարածված են ինֆորմացիայի գաղտնագրությունը կամ թաքնագրությունը: Գաղտնագրությունը ներկայացնում է ինֆորմացիայի ձևափոխումն այնպես, որ այն լինի անընթեռնելի կողմնակի անձանց համար: Այդ տեսքի ինֆորմացիան ընթեռնելի դարձնելու համար անհրաժեշտ է ունենալ յուրահատուկ տվյալ՝ գաղտնի բանալի, տվյալ ինֆորմացիայի ընթերցման համար: Գաղտնագրության դեպքում ձևափոխված ինֆորմացիան պահվում է բացահայտ տեսքով և հասանելի է բոլորին [1]: