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]:

Իսկ թաքնագրությունը ներկայացնում է եղանակ՝ գաղտնի պահելու ինֆորմացիայի գոյության փաստը, բացահայտ թողնելով նրա պարունակությունը [2]:

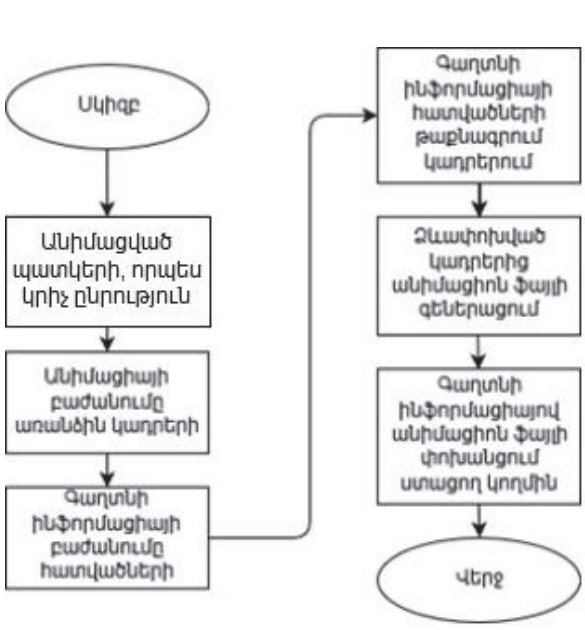
Խնդրի ձևաչափը և մեթոդիկայի հիմնավորումը: Ուսումնասիրելով ինֆորմացիայի անվտանգության ապահովման եղանակները՝ մշակվել է ինֆորմացիայի գրաֆիկական թաքնագրության եղանակ, երբ գաղտնի ինֆորմացիան պահվում է անիմացիայի կադրեր հանդիսացող պատկերի պիքսելների մեջ, բիթերի փոխանակման միջոցով: Այդ եղանակի իրականացման համար կարելի է օգտագործել տարբեր ձևաչափեր, որոնցից են, օրինակ՝ APNG (Animated Portable Network Graphics), WebP, MNG (Multiple Network Graphics) FLIF (Free Lossless Image Format) [3 - 5]: Ընտրվել է GIF ձևաչափը՝ որպես կրիչ-պատկեր, քանի որ այն տարածված է գրաֆիկական դիզայներների և վեբ կայքերում, ինարավորություն ունի պահելու մի քանի պատկեր մեկ ֆայլում: GIF ձևաչափն օգտագործում է առանց կորուստների սեղմման (losless) Lempel-Ziv-Welch (LZW) ալգորիթմը [6]: GIF ձևաչափում ամեն գույնի համար հատկացվում է 8 բիթ հիշողության տարածք, որի արդյունքում ամեն պիքսել գրավում է 24 բիթ հիշողության տարածք: GIF ձևաչափը, մի քանի պատկեր պարունակելու դեպքում, յուրաքանչյուր պատկերի համար հատկացնում է սեփական գունային պալետ, որը բաղկացած է 255 գույնից [6]: Բայց կարելի է ունենալ GIF պատկեր՝ ավելի շատ գույների քանակով: Այդպիսի պատկեր կարելի է ստանալ շատ պարզ եղանակով՝ բաժանելով GIF պատկերի ամեն մի կադր մասերի, որոնցից ամեն մեկը կհանդիսանա որպես նոր կադր: Այդպիսի ձևափոխումից հետո կարելի է ստանալ, օրինակ, 2295 գույն պարունակող գրաֆիկական պատկեր (նկ. 1):

Նկ. 1. 255 գույն ունեցող GIF պատկերի ձևափոխումը 2295 գույն ունեցողի

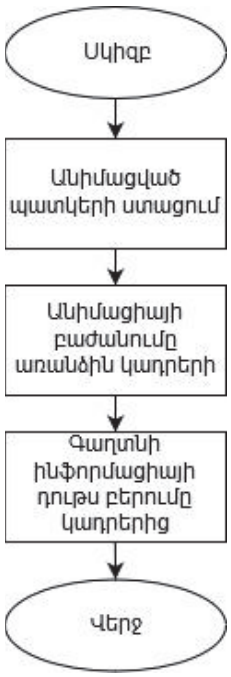
Ընտրված եղանակով, գաղտնի ինֆորմացիան պահվում է անիմացիոն պատկերի յուրաքանչյուր կադրի բայթերի մեջ, օգտագործելով LSB բիթերի փոխարինման մեթոդը: Որպես անիմացիոն պատկեր օգտագործվում է օգտագործողի կողմից ընտրված անիմացված պատկերը, որը բաժանվում է կադրերի: Յուրաքանչյուր կադրի մեջ թաքնագրվում է գաղտնի ինֆորմացիայի մի որոշ հատված, և ձևափոխված կադրերից կազմվում է նոր անիմացված պատկեր՝ ընտրված ձևաչափով, ինչի արդյունքում գեներացված գրաֆիկական անիմա-

ցիան հանդիսանում է կրիչ, որի յուրաքանչյուր կադր պարունակում է գաղտնի ինֆորմացիայի մի որոշակի հատված: Որպես անիմացիոն պատկեր կարող է ընտրվել կամայական գրաֆիկական անիմացիան. մշակված ծրագիրը հնարավորություն ունի աշխատելու վերը նշված ձևաչափերից բոլորի հետ: Տվյալ եղանակի թերությունն է ընտրված անիմացիայի կադրերի քանակը. մեծ ծավալի տվյալ թաքնագրելու դեպքում հնարավոր է անիմացիայի տեսանելիության աղավաղման առաջացում:

Ծրագրի աշխատանքը: Վերը նշված գրաֆիկական թաքնագրման եղանակի իրագործման նպատակով մշակվել է ծրագիր, որը մուտքին ստանում է անիմացված պատկեր, որի մեջ պահվելու է գաղտնի ինֆորմացիան: Տրված անիմացիան բաժանվում է կադրերի, որոնք պահվում են առանձին ֆայլերի տեսքով: Կախված կադրերի քանակից՝ գաղտնի ինֆորմացիան բաժանվում է բլոկների: Այնուհետև յուրաքանչյուր կադրի մեջ գաղտնի ինֆորմացիային համապատասխան բլոկը թաքնագրվում է LSB մեթոդով (նկ. 2 և նկ. 3): Այս մեթոդը ներկայացնում է փոքրագույն նշանակություն ունեցող բիթերի փոխարինումը նոր տվյալի բիթերով:

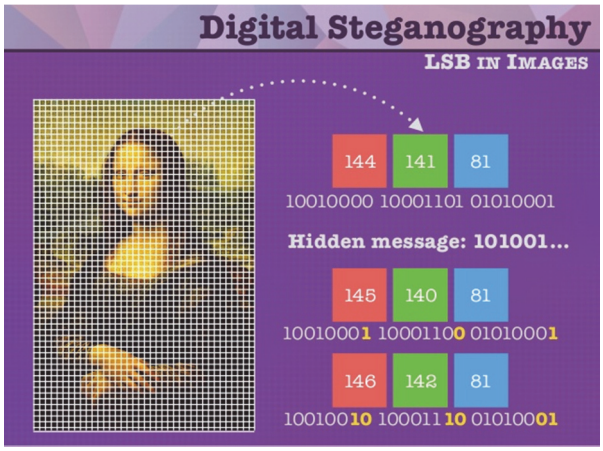


Նկ. 2. Փոխանցող կողմի գործողությունների բլոկ- սխեման



Նկ.3. Ընդունող կողմի գործողությունների բլոկ-սխեման

Կախված թաքնագրվող տվյալների չափսից և կրիչ պատկերի յուրաքանչյուր պիքսելի գույնին հատկացվող բիթերի քանակից՝ LSB-ն կարող է օգտագործել 1 կամ 2 բիթ հիշողության տարածք յուրաքանչյուր գույնից: Կարելի է օգտագործել ավելի մեծ քանակությամբ բիթեր յուրաքանչյուր գույնից, սակայն այդ դեպքում պատկերի վրա կառաջանա տեսանելիության աղավաղում (նկ. 4): Դատարկ և լցված կրիչների մեջ զբաղեցրած հիշողությունը նույնն է, քանի որ ընտրված մեթոդը գաղտնի տվյալներ պահելու համար նոր հիշողություն չի առանձնացնում պատկերի մեջ, ինչը բարձրացնում է թաքնագրված տվյալների գաղտնիության հուսալիությունը [7]: GIF ձևաչափի յուրաքանչյուր կադրի յուրաքանչյուր պիքսելի համար պահվում է սեփական գունային պալետ, որի ամեն գույնի համար հատկացվում է 256 երանգի տեղ: Ներկայումս այս ձևաչափի պատկերներում օգտագործվում է RGB գունային մոդելը: Այս մոդելի ամեն պիքսել կազմված է երեք բայթից՝ կարմիր, կանաչ և կապույտ գույների համար: Յուրաքանրյուր պիքսելի մեջ գաղտնի ինֆորմացիա պահելու համար պիքսելի ամեն գույնի համար պատասխանատու բայթի վերջին մեկ կամ երկու բիթերի արժեքները փոխարինվում են անհրաժեշտ արժեքներով՝ կախված գաղտնի ինֆորմացիայի ծավալից [6, 8]: Այդ քայլերից հետո ստացված կադրերից ստեղծվում է նոր անիմացված ֆայլ՝ ստանալով նախկին անիմացիայի կարգավորումները, որոնցից են անիմացիայի կրկնությունների քանակը և ամեն կադրի ցուցադրման ժամանակահատվածը:



Նկ. 4. LSB մեթոդի կիրառման օրինակ՝ 1 և 2 բիթի փոփոխմամբ

Ստացված արդյունքները: Ներկայացված են կատարված աշխատանքի արդյունքները GIF ձևաչափ ունեցող անիմացված պատկերի կադրերից մեկի օրինակով (նկ. 5 և նկ. 6):

Նկ. 5. Դատարկ կադր ընտրված գրաֆիկական անիմացիայից

Նկ. 6. 16826 բայթ պարունակող կադր՝ ընտրված գրաֆիկական անիմացիայից

Եզրակացություն.

● Մշակված եղանակի շնորհիվ հնարավոր է թաքնագրել ինֆորմացիան, որի գոյության փաստը անհասանելի կլինի կողմանկի անձանց համար:

● Մշակված եղանակի օգտագործման ժամանակ չի փոխվում կրիչ- պատկերի զբաղեցրած հիշողության ծավալը:

● Այս եղանակը հնարավորություն է տալիս՝ աշխատելու տարբեր գրաֆիկական անիմացիաների ձևաչափերով:

● Այս եղանակի թերությունն այն է, որ կողմնակի անձը ամեն դեպքում կարող է տիրանալ թաքնագրված ինֆորմացիային, եթե ունենա կրիչ հանդիսացող անիմացիան կամ դրա կադրերը՝ մինչև ձևափոխումը:

ԳՐԱԿԱՆՈՒԹՅԱՆ ՑԱՆԿ

1. **Կոնհայմ Ջ.Ա.** Համակագչի անվտանգություն և գաղտնագրություն. — ԱՄՆ, Ջոն Վայլի և որդիներ, Inc., 2007. — 516 էջ:
2. **Գրիբունին Վ.Գ., Օկով Ի.Ն., Տուրինցև Ի.Վ.** Թվային թաքնագրություն. — Մոսկվա. Սոլոն-Պրեսս, 2009. — 249 էջ:
3. "APNG Specification". Retrieved 26 May 2015.
4. "WEBP file extension". DotWhat.net. Retrieved 1 October 2010.
5. "FLIF is a New Free Lossless Image Format That Raises the Compression Bar". PetaPixel. 2 October 2015. Retrieved 20 October 2016.
6. **CompuServe Incorporated** Graphics Interchange Format, Version 87. — USA 15 June 1987. Retrieved 13 October 2012.
7. **Բենդեր Ո., Գրալ Դ., Մորիմոտո Ն., Լու Ա.** Տվյալների թաքցման մեթոդներ.— Նյու Յորք, 1996. — էջ 313-336:
8. **Charles A. Poynton** — Digital Video and HDTV: Algorithms and Interfaces, 2003.

Л.А. БАЛАГЕЗЯН

СТЕГАНОГРАФИЯ В КАДРАХ ГРАФИЧЕСКОЙ АНИМАЦИИ

Информация, которой обмениваются две стороны, часто является целью третьей стороны. По этой причине существует проблема сокрытия информации, которая будет недоступна третьим лицам. Для решения этой проблемы проведена работа по изучению сокрытия информации. Разработан метод, позволяющий скрыть конфиденциальную информацию в кадрах с графической анимацией. Кадры извлекаются из выбранной графической анимации, в которых предварительно фрагментированная информация скрыта методом шифрования LSB, что позволяет третьей стороне не знать о существовании конфиденциальной информации. Для доступа к информации получатель должен будет извлечь ее из кадров графической анимации.

Ключевые слова: стеганография секретной информации, стеганография в изображении, изображение контейнера, секретное сообщение, анимированное изображение, метод LSB, модификация цветовой палитры.

L.A. BALAGYOZYAN

STEGANOGRAPHY IN THE FRAMES OF GRAPHICAL ANIMATION

Information shared between two parties is often a target for a third party. For this reason, there is a problem with concealing information making it inaccessible to the third party. To solve this problem, some work was carried out to study the hiding of information and develop a method for hiding confidential information in the frames of graphical animation. The footage comes from selected graphical animations, in which pre-fragmented information is hidden by the LSB encryption method, which does not allow the third party to be aware of the confidential information. The recipient will be required to extract the information from the animation footage to decipher the information.

Keywords: secret information steganography, image steganography, container image, secret communication, animated image, LSB method, color palette modification.