Informatics

MƏXFİ İNFORMASİYANIN ÖTÜRÜLMƏSİNDƏ İNFORMASİYA GİZLƏDİLMƏ METODU

Ababil Faxrəddin qızı Nağıyeva
Azərbaycan Texnologiya Universiteti, Bakı, Azərbaycan

THE METHOD OF HIDING INFORMATION IN THE TRANSMISSION OF CONFIDENTIAL INFORMATION

Ababil Fakhreddin Nagiyeva
Azerbaijan Technology University, Baku, Azerbaijan: ababil.nagiyeva@mail.ru
https://orcid.org/0000-0003-3071-1105

Abstract. Steganography, the most important area of secret information hiding, can be classified as hiding secret information inside an image. The purpose of steganography is to hide the presence of information. Confidential information requested to be sent is hidden in any other object, preventing third parties from knowing about the existence of the sent information. Steganography: it is applied in three fields namely text, image and voice steganography.

The article discusses the main concepts and provisions of steganography, examines the principles of building digital stego-systems, and proposes a new more effective algorithm based on the knowledge gained.

The main principles in the construction of steganographic systems are the visual indistinguishableness of stego-images and container images, as well as increasing the volume of hiding secret information bits and ensuring their integrity. Considering all this, the explanation of the proposed new algorithm, which includes these qualities, is given extensively in the article.

Keywords: *Steganography, quorum function, secret information hiding.*

Giriş

Məlum olduğu kimi steqanoqrafiyanın əsas şərtlərindən biri odur ki, ilkin təsvir ilə içərisinə məxfi informasiya gizlədilmiş steqo−təsvir arasında vizaul oxşarlıq maksimum olmalıdır. Lakin ilkin təsvir üzərində aparılan hər bir dəyişiklik onun vizual dəyişməsinə səbəb olur. Eyni zamanda ilkin təsvirin interpolyasiya edilərək konteyner təsvirinin yaradılması zamanı da ilkin təsvir üzərində aparılan əməliyyatlar onun müəyyən dərəcədə dəyişilməsinə səbəb olur [1,2,3]. Dəyişilmənin səbəbindən ilkin təsvir və steqo−təsvir arasında hesablanan PSNR qiymətləri aşağı olur. Steqo−təsvirdən məxfi informasiya çıxarıldıqdan sonra konteyner təsvirin yenidən bərpa olunması üzrə aparılan tədqiqatlar PSNR və daha çox məxfi informasiya gizlətmə qabiliyyəti baxımından bir-birindən fərqlənən bir çox işlərə həsr edilmişdir [4]. Bu bölmədə təklif etdiyimiz alqoritm mövcud oxşar alqoritmlər ilə müqayisədə yuxarıda qeyd olunan göstəricilər (PSNR və HC) üçün yaxşı nəticələr verir [5, s .85-92].

Məxfi informasiyanı göndərən tərəf onu konteyner içərisinə gizlətməzdən əvvəl AES alqoritmi ilə şifrləyir [6,7]. Şifrlənmiş məxfi informasiya bitləri kvorum funksiyası əsasında təklif edilən yeni alqoritm ilə konteyner təsvirinə gizlədilir və beləliklə steqo−təsvir yaranmış olur.

Məxfi informasiyanın steqo−təsvirdən çıxarılması prosesi isə gizlədilmə alqoritminin əksi olan alqoritmdən istifadə olunaraq həyata keçirilir [8, 9, 10].

Tədqiqatın məqsədi, məsələnin qoyuluşu

Təklif olunan alqoritm ilkin təsvirin vizual keyfiyyətinə təsir etmədən məxfi informasiyaların daxil edilməsini və ilkin təsvirin yenidən bərpa olunmasını təmin edir.

Aşağıda təqdim edilən bölmələrdə təklif olunan alqoritmin daha geniş izahı, yəni məxfi informasiyanın konteyner təsvirinə gizlədilməsi və yaradılmış steqo−təsvirdən məxfi informasiyanın çıxarılma prosesinin addımları göstərilmişdir.

İşlənilib təklif edilən 3-girişli kvorum funksiyası əsaslı informasiya gizlətmə alqoritminin steqo-hücumlara dayanıqlılığını, yəni təhlükəsizliyini təmin etmək məqsədi ilə məxfi informasiyanın şifrlənməsindən istifadə edilib. Şifrlənmə kriptoqrafiyada özünə geniş yer tapmış AES şifrləmə standartı ilə aparılıb.

Məsələnin həlli üsulları

AES əsasında məxfi informasiyanı aşağıda göstərilən ardıcıllıqla şifrləyirik:

Şifrləmə addımları.

Məxfi informasiya bitinin ilkin bloku $A(x)$ massivi şəkilində verilmişdir və $C(x)$ açar massivimiz var. Bu işdə 128 bit açarın istifadəsi kifayyət edir. Bildiyimiz kimi 128 bit açar istifadə edilən zaman dövrlərin sayı 10 olur.

Addım 1. Açarın əlavə edilməsi. $A(x)$ massivi ilə $C(x)$ açar massivnin 2 moduluna görə cəmi (XOR) hesablanır.

$$A(x)=\begin{bmatrix} 32 & 88 & 31 & e0 \\ 43 & 5a & 31 & 37 \\ f6 & 30 & 98 & 07 \\ a8 & 8d & a2 & 34 \end{bmatrix} \qquad C(x)=\begin{bmatrix} 26 & 28 & ab & 09 \\ 7e & ae & f7 & cf \\ 15 & d2 & 15 & 4f \\ 16 & a6 & 88 & 3c \end{bmatrix}$$

$$A(x)=A(x)\oplus C(x)$$

$$A(x)=\begin{bmatrix} 19 & a0 & 9a & e9 \\ 3d & f4 & c6 & f8 \\ 3e & e2 & 8d & 48 \\ be & 2b & 2a & 08 \end{bmatrix}$$

Addım 2. Baytların əvəz edilməsi. Əldə edilən $A(x)$ massivi baytların əvəz edilməsi prosesində istifadə edilir. Bunun üçün bizə S-bloku lazımdır. S -blokundakı elementlər ilə $A(x)$ massivinin elementləri əvəzlənir. S-bloku şəkil 1-də verilib.

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

Şəkil 1. S-bloku

$A(x)$ massivinin birinci elementi 19-dur. Bu element S-blokunun 1-ci sətri ilə 9-cu sütununun kəsişməsində duran elementlə əvəz edilir. Əvəz etmə prosesi bu şəkildə $A(x)$ massivinin bütün elementlərinə tətbiq olunur. Və növbəti addıma keçirilir.

Addım 3. Sətirlərin sürüşdürülməsi. $A(x)$ massivinin axırıncı üç sətri müxtəlif sayda baytlarla dövri sürüşdürülür. Sətr 1-C_1 bayt, sətr 2-C_2 bayt, sətr 3-C_3 bayt sürüşdürülür. C_1 C_2 C_3 sürüşmələrinin qiyməti blokun uzunluğu N_b-dən asılıdır. Onların qiyməti cədvəldə göstərilir.

Sətirlərin sürüşdürülməsi

N_b	C_1	C_2	C_3
4	1	2	3
6	1	2	3
8	1	3	4

Axırıncı üç sətrin sürüşməsi əməliyyatı **ShiftRows (State)** kimi işarə edilir. Beləliklə $A(x)$ massivinin elementləri aşağıdakı kimi olacaq.

$$A(x)=\begin{bmatrix} d4 & e0 & b8 & le \\ bf & b4 & 41 & 27 \\ 5d & 52 & 11 & 98 \\ 30 & ae & f1 & e5 \end{bmatrix}$$

Sonra növbəti addıma keçirilir.

Addım 4. Sütunların qarışdırılması. Bu addımda $A(x)$ masivinin sütunlarına $GF(2^8)$ meydanı üzərindəki çoxhədlilər kimi baxılır. Çevirmə sütunun x^4+1 moduluna görə müəyyən edilmiş

$$c(x)=\{03\}x^3+\{01\}x^2+\{01\}x+\{02\}$$

çoxhədilisinə vurulmasından ibarətdir:

$$b(x)=c(x)\cdot a(x)(\text{mod } x^4+1) \tag{1}$$

Burada $c(x)$ çoxhədlisi x^4+1 ilə qarşılıqlı sadədir və buna görə vurmanın tərsi var. Tərs çevirmə x^4+1 moduluna görə $c(x)$ -in multiplikativ tərsi olan

$$d(x)=\{0B\}x^3+\{0D\}x^2+\{09\}x+\{0E\} \tag{2}$$

çoxhədlisinə vurmaqdan ibarətdir.

$A(x)$ massivini $C(x)$ massivi ilə 2 moduluna görə cəmini hesablayırıq. Hesablama zamanı $A(x)$ massivinin sütun elementləri ardıcıl olaraq $C(x)$ massivi ilə 2 moduluna görə cəmlənir .

$$A(x)=\begin{bmatrix} d4 & e0 & b8 & 1e \\ bf & b4 & 41 & 27 \\ 5d & 52 & 11 & 98 \\ 30 & ae & f1 & e5 \end{bmatrix}$$

$$\oplus \qquad B(x)=\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}\bullet\begin{bmatrix} d4 \\ bf \\ 5d \\ 30 \end{bmatrix}=\begin{bmatrix} 04 \\ 66 \\ 81 \\ e5 \end{bmatrix}$$

$$C(x)=\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$$

Bu addımın nəticəsində $A(x)$ masivinin elementləri aşağıdakı kimi olacaq.

$$A(x) = \begin{bmatrix} 04 & e0 & 48 & 28 \\ 66 & cb & f8 & 06 \\ 81 & 19 & d3 & 26 \\ e5 & 9a & 7a & 4c \end{bmatrix}$$

Addım 5. Açarın dövrə əlavə edilməsi. Bildiyimiz kimi hər dövrdə açar hesablanaraq yeni qiymətlər alır. Dövrə açarın əlavə edilməsi ilə $A(x)$ state massivinin hər bir açar massivinin uyğun baytı ilə 2 moduluna görə bütün bitlərin toplanması ilə həyata keçirilir. Bu çevirmə öz özünün tərsidir. Açarın əlavə edilməsi prosesi aşağıdakı kimidir

$$A(x) = \begin{bmatrix} 04 & e0 & 48 & 28 \\ 66 & cb & f8 & 06 \\ 81 & 19 & d3 & 26 \\ e5 & 9a & 7a & 4c \end{bmatrix}$$

$$\begin{bmatrix} 04 \\ 66 \\ 81 \\ e5 \end{bmatrix} \oplus \begin{bmatrix} a0 \\ fa \\ fe \\ 17 \end{bmatrix} = \begin{bmatrix} a4 \\ 9c \\ 7f \\ 2f \end{bmatrix}$$

Beləliklə $A(x)$ massivinin elementlərinə açar əlavə edilir və aşağıdakı qiymətləri alır.

$$A(x) = \begin{bmatrix} a4 & 68 & 6b & 02 \\ 9c & 9f & 5b & 6a \\ 7f & 35 & ea & 50 \\ f2 & 2b & 43 & 49 \end{bmatrix}$$

Bu addımların dövrlərinin sayı 10-dur. Sonuncu dövrdə sütunların qarışdırılması prosesi olmur.

Alınan nəticələrin tətbiqi

Yuxarıda göstərilən addımlar yerinə yetirilərək Rijindel alqoritmi vasitəsilə məxfi informasiya bitləri tam şifrlənir və növbəti başlıqda təqdim edilən alqoritm vasitəsilə konteyner təsviri içərisinə gizlədilir. Təklif olunan steqanoqrafik alqoritmin yerinə yetirilmə ardıcıllığı aşağıdakı kimidir.

Məxfi informasiyanın konteyner təsvirinə gizlədilməsi:

Addım 1. Rijindel alqoritmindən istifadə edərək məxfi informasiya bitləri şifrlənir

$$B = b_1, b_2 b_3, \ldots\ldots b_n$$

Addım 2. Konteyner təsvir 2x2 bloklara bölünür (Şəkil 2)

a_{11}	a_{12}
a_{21}	a_{22}

Şəkil 2. Konteyner təsvir

Addım 3. Ən aşağı dəyəri olan piksel digər 3 pikseldən çıxılır.

$$\begin{aligned} c_{12} &= a_{12} - \min \\ c_{21} &= a_{21} - \min \\ c_{22} &= a_{22} - \min \end{aligned} \tag{3}$$

Alqoritm də məxfi informasiyaların daxil edilməsi və çıxarılması üçün 3 girişli kvorum funksiyasından istifadə edirik. Kvorum funksiyası (QF), Bul cəbrində, heş funksiyasında və s. geniş istifadə olunur. Kvorum funksiyası aşağıdakı kimi verilir [1].

$$QF(x_1, x_2, ...x_n) = \begin{cases} 1, \sum_{i=1}^{n} x_i \geq \frac{n}{2}, \\ 0 \end{cases} \tag{4}$$

Konteyner təsvirin c_{12}, c_{21}, c_{22} piksellərinin son 3 ən az əhəmiyyətli bitində məxfi informasiyaların yerləşdirilməsi üçün kvorum funksiyasından istifadə edilmişdir. Bunun üçün (5) düsturu ilə üç girişli kvorum funksiyasını (3QF) istifadə etmək mümkündür.

$$3QF(x_1, x_2, x_3) = (x_1 \wedge x_2) \oplus (x_1 \wedge x_3) \oplus (x_2 \wedge x_3) \tag{5}$$

burada $3QF(x_1, x_2, x_3)$ kvorum funksiyasının giriş qiymətləridir. Giriş qiymətləri kimi konteyner təsvirin müvafiq piksellərinin son 3 ən az əhəmiyyətli biti istifadə olunur. Məlumdur ki, bu qiymətlər 0 və yaxud 1 ola bilər. Əgər funksiyanın giriş qiymətləri 1-ə bərabər olarsa onda kvorum funksiyasının çıxış qiyməti də 1-ə bərabər olur. Əgər giriş qiyməti 0-a bərabər olarsa, kvorum funksiyasının çıxış qiyməti 0-a bərabər olacaqdır. Üç girişli kvorum funksiyasından (3QF) istifadə edərək məxfi informasiyanın gizlədilməsi proseduru aşağıda ətraflı təsvir edilmişdir.

Fərz edək ki, məxfi informasiya bitləri B=101111001110 verilmişdir. Məxfi informasiyanın birinci biti B (1) =1 bərabərdir. Fərz edək ki, konteyner təsvirin müvafiq pikselinin qiyməti (125=(1111101))-dir və burada son 3 bitin qiyməti (101)-dir. 3 girişli kvorum funksiyasının qiymətləri [1]- də verilmişdir. Qiymətlər cədvəlinə əsasən tapırıq ki, giriş qiyməti 101 olarsa onda 3QF=1 bərabər olur. Belə olan halda konteyner pikselinin qiymətini dəyişmədən steqo−təsvir pikseli kimi qəbul edirik. Bu zaman steqo−təsviri qəbul edən şəxs pikselin son 3 qiymətinin kvorum funksiyasına əsasən 1-ə bərabər olduğunu tapır ki, bu da məxfi informasiya biti ilə üst üstə düşür.

Əks halda, yəni 3QF çıxış qiyməti ilə məxfi bitin qiymətləri arasında bərabərsizlik olarsa, məxfi bitlərin qiymətinə uyğun gələn 3QF-nin məqbul çıxış qiyməti (2) tənliyi ilə müəyyən edilir və müəyyən edilən bitlər konteyner təsvirin müvafiq pikselinin son 3 bitləri ilə əvəz edilir.

Birinci bloka məxfi informasiya bitlərinin bir qismi gizlədildikdən sonra alqoritm növbəti bloku seçir və yuxarıda qeyd olunan prosedur və müvafiq bit mübadiləsi əməliyyatı başa çatdıqdan sonra blokların piksellərinə minimum piksel əlavə edilir.

Məxfi informasiyanın steqo−təsvirdən çıxarılması prosesi

Addım 1. Steqo–təsvir 2x2 bloklara bölünür (Şəkil 3).

S_{11}	S_{12}
S_{21}	S_{22}

Şəkil 3. Steqo−təsvir bloku

Steqo−təsvirin hər blokunda birinci pikseldə heç bir məxfi informasiya biti gizlədilməmişdir. Məxfi informasiya bitləri digər üç pikselə gizlədilmişdir.

Addım 2. Digər üç pikseldən minimum piksellər çıxarılır.

$$\begin{aligned} s'_{12} &= s_{12} - \min \\ s'_{21} &= s_{21} - \min \\ s'_{22} &= s_{22} - \min \end{aligned} \tag{6}$$

Addım 3. Fərq qiymətləri s'_{ij} ikilik say sisteminə çevrilir və onların son 3 biti 3QF-ə funksiyasına əsasən hesablanır (6). Beləliklə, məxfi informasiya bitlərini çıxarmaq mümkün olur .

Nəticə

Məqalədə Kvorum funksiyası əsasında yeni məxfi informasiya gizlədilmə alqoritmi işlənilib. Məqalədə məxfi informasiyanın konteyner təsvirinə gizlədilmə və steqo - təsvirdən çıxarılma prosedurlarının rəqəmsal nümunələri verillib. Nümunələrdən məlum olur ki, təklif edilən alqoritmlərdə mürəkkəb hesablamalar olmadığı üçün sadə, istifadəsi isə rahatdır. Bu da həmin alqoritmlərin realizəsi üçün az vaxtın tələb olunmasını göstərir. Təqdim edilən alqoritmdə heç bir pozuntu və maneə olmadan məxfi informasiya bitlərini rəqəmsal təsvirdə gizlədilməsini və çıxarılmasını təmin etməklə yanaşı steqo-hücumlara qarşı dayanıqlı olması üçün də işlər aparılıb. Bu da məxfi informasiyaların icazəsi olmayan şəxslər tərəfindən ələ keçirilməməsini təmin edir.

ƏDƏBİYYAT

1. Govind S. P., Bindiya M. V., Judy M.V. A high imperceptible data hiding technique using quorum function. Multimedia tools and applications, 2021. № 80, pp. 527 – 545.
2. Ahmad A.M., Al-.Haj A., Farfoura M. An improved capacity data hidin technique based on image interpolation. Multimedia Tools and Applications, 2019, № 78, p.7181-7205.
3. Chen Y., Sun W., Li L. Chang X., Wang C. An efficient general data hiding scheme based on image interpolation. Journal of Information Security and Applications, 2020. № 54, p.271–350.
4. Chin Y., Shen H., Cheonshik K. Improving stego image quality in image interpolation based data hiding. Computer Standards & Interfaces,2017. № 10, p. 209-215.
5. Шелухин О.И., Канаев. С.Д. Steganography. Москва, “Горячая линия – Телеком”, 2017, 582 с.
6. Нагиева, А.Ф., Вердиев, С.К., Гусейнов, З.Н. Симметричное (одноключевое) шифрование данных при защите информации в компьютерных сетях. Технические науки в России и за рубежом: материалы VII Международная научная конференция. Москва, Молодой ученый, 31 ноябрь, 2017, с. 5-7.
7. Нагиева А.Ф., Вердиев С.К. О возможностях использования стандарта AES в Корпоративных сетях для защиты информации. Инфокоммуникационные технологии, 2017, № 4, с. 6-9.
8. Hu J., Li T. Reversible steganography using extended image interpolation technique. Computer Electric Engineering, 2015, № 46, p. 447–455.
9. Hussain M., Wahab A., Jung K., Noman J. Recursive information hiding scheme through LSB, PVD shift, and MPE. IETE Technical Review, 2017, № 35, p.53–63.
10. Jana B. Giri D. Mondal S.K. Weighted Matrix based Reversible Data Hiding Scheme using Image Interpolation. Computational Intelligence in Data Mining, 2015, №2, p. 239-248.

MƏXFİ İNFORMASİYANIN ÖTÜRÜLMƏSİNDƏ İNFORMASİYA GİZLƏDİLMƏ METODU

A.F.Nağıyeva

Xülasə. Məxfi informasiyanın gizlədilməsinin ən vacib sahəsi olan steqanoqrafiya, bir təsvirin içərisinə məxfi informasiyanın gizlədilməsi kimi təsnif oluna bilər. Steqanoqrafiyanın məqsədi məlumatın varlığının gizlədilməsidir. Göndərilməsi tələb olunan məxfi informasiya hər hansı bir başqa obyektdə gizlədilərək üçüncü şəxslərin göndərilən informasiyanın varlığından xəbəri olmasını əngəlləyir. Steqanoqrafiya: mətn, təsvir və səs steqanoqrafiyası olmaq üzrə üç sahədə tətbiq edilir.

Məqalədə steqanoqrafiyanın əsas anlayışları və müddəalarının müzakirələri, rəqəmsal steqo-sistemlərin qurulması prinsiplərinin araşdırılması nəticəsində və əldə edilən biliklər əsasında yeni daha effektiv alqoritm təklif olunur.

Steqanoqrafik sistemlərin qurulmasında əsas prinsiplər steqo−təsvirlərin və konteyner təsvirlərin vizual olaraq fərqlənə bilməməsi, həmçinin məxfi informasiya bitlərinin gizlədilməsi həcminin artırılması və bütövlüyünün təmin olunmasıdır. Bütün bunlar nəzərə alınaraq bu keyfiyyətləri özündə birləşdirən, təklif edilən yeni alqoritmin izahı məqalədə geniş verilmişdir.

Açar sözlər: *Steqanoqrafiya, kvorum funksiyası, məxfi informasiyanın gizlədilməsi.*

Accepted: 30.11.2023