ONE ALGORITHM FOR SPECTANOGRAPHY BASED ON THE SPATIAL AREA

Stanislava Biserova Pavlova, Dian Valentinov Velev

National military university" Vasil Levski"

Abstract: *We construct and implement a new Steganography algorithm based on spatial domain to hide a large amount of information into color BMP image. It utilizes the arrangement of the secret data to compensate distortion, which is called fixed LSBs(Least Significant Bits) substitution methods.*

Keywords*: BMP image; steganography; spatial domain;*

ЕДИН АЛГОРИТЪМ ЗА СТЕГАНОГРАФИЯТА, БАЗИРАН ВЪРХУ ПРОСТРАНСТВЕНАТА ОБЛАСТ

Станислава Бисерова Павлова, Диан Валентинов Велев

Национален военен университет "Васил Левски", Факултет „Общовойскови"

Въведение

Стеганографията е наука за скриване на тайна информация и включва предаване й чрез привидно безобидни файлове. Целта е не само съобщението да бъде скрито, но да бъде предадено без да бъде засечено. Стеганографията поддържа скриване на съобщенията сред огромния обем на интернет трафика, в медийни файлове, където добавянето на тайно съобщение трудно се открива с човешкото око, дори файлът да бъде обстойно прегледан [1].

Внедряването на нови по-ефикасни средства за скриване и защитено предаване на конфиденциална информация, би предотвратило изтичането на данни и чувствителна информация [15]. Стеганографията може да се комбинира с криптография за да се постигне по-добра защита на информацията. Скриване на информация вътре в изображенията е популярна техника в днешно време.

Най-често срещаните методи за извършване на тези промени включват използването на най-младшия значещ бит (LSB least significant bit) разработен от Chandramouli в [2], маскиране, филтриране и трансформации върху изображението на прикриващия обект. В [3] е представен алгоритъм за откриване на LSB стеганография. В [4] авторите изграждат математически рамки, базирани на сложни теоретични възгледи, които търсят границите на стеганографията. Конструкцията на HweeHwa Pang в [5], използва хеш стойност, която се получава от името на файла и паролата и по този начин се открива скритият файл. Този подход се използва с нови модификации. Следващото интересно приложение на стеганографията е разработено в [6], където съдържанието е криптирано с един ключ и може да бъде декриптирано с няколко други клавиша, относителната ентропия между криптиране и един специален ключ за декриптиране съответства към количеството информация. Заради непрекъснатите промени в стеганографията и големите количества информация, с които се разполага се предлага използването на техники за машинно обучение за характеризиране изображенията като подозрителни или не, разработени от [7]. В [8] се използва ентропийна техника за откриване на подходящите области в изображението, където информацията може да бъде вградена с минимално изкривяване. C. Zhang et al. [9] косвено скрива тайните битове информация заедно с някои избрани графични изображения, базирани на алгоритъм за невронни мрежи, за да се получат битове за шифроване. Този подход се разглежда

в доклада. Когато се използва 24-битов цвят от изображение, малко от всеки червен, зелен и син цвят могат да се използват всяка от компоненти. Именно за това могат да се съхраняват общо 3 бита на всеки пиксел. По този начин изображение с размери 800 × 600 пиксела може да съдържа общо количество от 1440000 бита (180000 байта) тайна информация. Така че основната цел на доклада е да се намери решение, как да се вмъкне повече от един бит на всеки байт в един пиксел на прикриващия обект и той да дава резултати като LSB [2], [3].

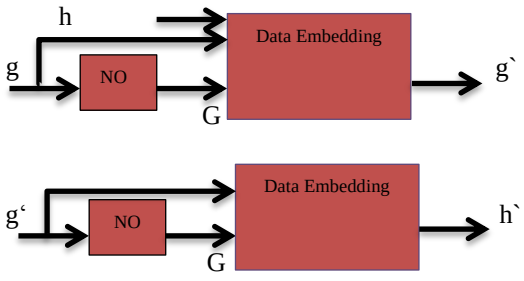
Докладът има за цел да анализира един нов алгоритъм за стеганография, базиран на интелигентна система за скриване на голямо количество от всякакъв вид информация чрез растерно изображение [4], [6] чрез използване максимален брой битове на байт за всеки пиксел. Има два вида атаки, които биха обезпокоили процесът на вграждане на информацията, първият е да се работи срещу визуални атаки [7], [10] - способността на хората неразбираемо да успяват да различът шума и визуални модели, а втората опасност се отнася до работата срещу статистическите атаки [3], [8], [11], [12] .

Стеганографията в изображения, които включват най-младшите битове

В [13] се предлага метод за скриване на данни, който се нарича адаптивен номер на LSB, базирани на човешката визуална система. Те приемат, че тайните данни са под формата на двоични потоци, които могат да компресирани мултимедии, или просто серия от текстове, предаващи съобщения за предаване в хост изображенията. Този метод се основава на човешката визуална система. Сивият цвят промяна стойността на всеки пиксел в изображението на хоста и след вграждането е извън човешкото възприятие. В допълнение към този метод, вградените тайни данни могат да бъдат извлечени без познаване на първоначалния образ. Преди да се разгледа този метод се е използвал друг, който е за вграждане на мултимедийна информация в прикриващо изображение. Тази адаптивност може да бъде създадена като номерата на LSB за вграждане се използват без допълнителни разходи от модифицираната стойност на пикселите. Има функция за картографиране, която е подложена на човешка визуална чувствителност и се използва за постигането на тази цел.

При въвеждане на тази основна функция, **Ng()** е LSB-mapping функция. Тя дава броя на LSBs, които могат да бъдат вградени за всяко едно възможно сиво ниво ***g***. След вграждането се означават с ***g'***, тогава състоянието на за тази адаптация е- ***N()g*** стойностите преди и след промяната на пикселите трябва да остане непроменена. Пример за това е ***Ng***.

На фигура 1, е показана концепцията и като с ***h*** се обозначава вградената тайна информация. Така, според формулата ***N(),*** се слага променлива ***g*** в N() и се получава ***g'***. По този начин се добавят няколко бита. От друга страна ***g*** може да бъде извлечена, когато приемникът използва формула N(), за да получите вградени данни.



Фигура 1. Концепцията за самостоятелен брой на LSB за вграждане и извличане на данни.

Таблица 1. Брой използвани LSBs

i	Интервал	Брой използвани LSBs
		1 бит
0	0~87	2 бита
	88~191	3 бита
	192~255	4 бита

Съгласно функцията LSB-mapping Ng () (1) и оценената k_i, определен в Таблица 1, лесно се изчислява колко бита може да се вградят в един пиксел. Резултатът показва, че ако g е поставен между 0 и 87, се използват два LSBs. Може да се заключат три и четири LSBs.

Алгоритмичен подход на стеганографията. Анализиран алгоритъм

При този метод се въвежда използвания символ в алгоритъма от таблица 2 с номенклатурата. Алгоритъмът се разделя на три части. Първата част е предварителна обработка; секретни данни b_i трябва да бъдат първоначално модифицирани. Втората част е скриването на данни; заменя се k от LSB на оригиналната стойност на пиксела в сивата скала на първо място. Новата стойност на пискела трябва да е по-малък от оригиналната. Изважда се някаква стойност от y. След това допълнително се компенсира променената стойност y_i за подходяща стойност чрез сравняване с отношението между двете модифицирани тайни съобщения s_i. След като се премине през тези две части се получава стегообраз. Последната част е свързана с извличането на данни. Когато получателят получи това изображение по открит канал, той може да използва временна стойност като съхранява първите извлечени битове. От предишните части също може напълно да се извлече тайното послание стъпка по стъпка. Методът може да се разгледа на фигура 2.

Таблица 2. Номенклатура

Съкращение	Описание
y_i	-тия пиксел на изображението на прикриващ обект, [0,255] yi
N	- Общо пиксели в прикриващия обект
Y_i	-i-тия пиксел на стего изображението, [0,255] yi ∈
b_i	- Скрити данни, bi ∈ [1,0]
S_i	- Променени са тайни данни
k	- Бита на замяната в скриването на данни
m	- Всеки m пиксели наведнъж m $N_m \leq N$
LSB	Най-малък значещ бит
LSB_i	i-ти най-малък значещ бит

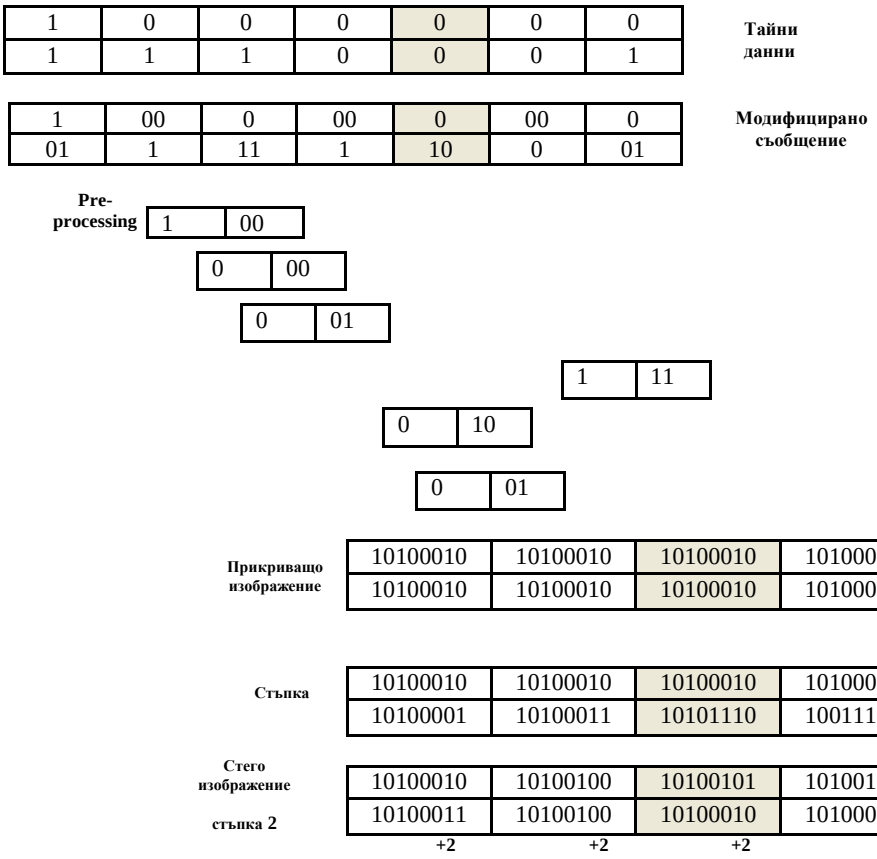
Изпълнение на алгоритъма

Оценка на качеството на изображението

Може грубо да бъде разделена на две части около оценка на качеството на изображението, което се променя от компресията или скриване на данни. Първият метод директно използва човека с визуална система. Това е просто система за човешко виждане като например корекция на гладката област в изображението. Трудно е обаче най-вече за човешките очи, за да открият малката разлика на две изображения в допустим диапазон. Освен това, усещането за зрението във всеки човек не е същото, така че е трудно да се установи един общ стандарт. Съотношението (PSNR) за измерване на качеството на изображението е друг обективен стандарт за оценка. Формулата е показана по-долу [19]:

(1) $$PSNR = 10 \times \log\left(\frac{255}{MSE}\right)$$

(2) $$\mathrm{MSE} = \frac{1}{m \times n}\sum_{i-1}^{m \times n}(Si - Ci)2$$



Фигура 2. Пример за скриване на данни при m=8 и k=2

Във формули (1) и (2):

- MSE е средна квадратна грешка на оригинално изображение и модифицирано изображение [19];
- S_i и C_i отделно представят оригиналния пиксел и променения пиксел в същата позиция на изображението;
- m и n са на ширината и височината в изображението.

По този начин по-високият PSNR показва по-добро качество на изображението. Трудно е човешките очи да разграничи разлика между двете изображения, когато PSNR е по - голяма от 30 db. По-високият PSNR не е достатъчен, за да покаже, че качеството на изображението е по-добро като се разглежда в детайли.

Резултати от алгоритъма

В доклада се използва произволно генериран битов поток, който да бъде тайно съобщение [15]. Избрано е едно от четирите класически изображения, наричащо се "F16", което се състи от 512 до 512 пиксела. На фигура 3 са показани оригиналното и стего изображение с k = 3.

(а) Оригинално изображение (б) Стего изображение

Фигура 3. Оригинално и стего изображение с к=3

Капацитетът се определя, като се задържат битове на пиксел. По-високата стойност на k е ниската PSNR, която е показана в таблица 3.

Таблица 3. Резултатите от вграждането на случайното съобщение

Прикриващо изображение	k	Капацитет	PNSR (m-S)	Капацитет	PNSR (m=16)	Капацитет	PNSR (m=512)
Lena	2	1,75	46,7440	1,875	46,5587	1,996	46,3950
	3	2,625	41,1411	2,8125	40,9261	2,994	40,7452
	4	3,5	35,2325	3,75	35,0138	3,994	34,8128
Baboon	2	1.75	16,7406	1,875	46,5562	1,994	45,3891
	3	2,625	41,1538	2,8125	40,9174	2,994	40,7412
	4	35,2416	35,2416	3,75	35,0043	3,996	34,8033
F16	2	46,7528	46,7528	1,875	46,5627	1,996	46,3653
	3	41,1425	41,1425	2,8125	40,9448	2,994	40,7282
	4	35,2383	35,2383	3,75	35,0235	3,992	34,8119
Pepper	2	46,7402	46,7402	1,875	46,5540	1,996	46,3698
	3	41,1346	41,1346	2,8125	40,9374	2,994	40,7421
	4	35,2418	35,2418	3,75	35,0278	3,992	34,8069

В доклада се категоризира методът на фиксиран LSB заместващ метод и след това се сравнява с друг подобен, който е разгледан в таблица 4. За да бъде сравняването максимално актуално [16], m трябва да се зададе като максималната стойност с размер 512* 512. Размерът на тайното послание е по-малко от ***k*** бита, отколкото другите две схеми и стойността на капацитета е почти близо до ***k***.

Таблица 4. Сравнителен анализ на OPAP и LSB

Прикриващо изображение	k	(m=512*512)	OPAP [3]	LSB
Lena	2	46,38	45,37	44,15
	3	40,72	38,73	37,92
	4	34,81	32,83	31,78
Baboon	2	46,37	44,37	44,15
	3	40,72	38,37	37,92
	4	34,80	32,80	31,86
F16	2	46,37	45,37	44,15
	3	40,72	38,73	37,92
	4	34,80	32,80	31,86
Pepper	2	46,37	45,37	44,15
	3	40,72	38,73	37,89
	4	34,80	32,81	31,85

В таблица 4 колоната, обозначена като OPAP [14], предлага метод с оптимален процес на настройка на пикселите; колоната, обозначена с LSB, е прост LSB заместващ метод.От таблицата и според [17], [18] се вижда, че ефективността е по-добра от OPAP и LSB.

Заключение

Стеганографията е ефективен начин за прикриване на информация и скриването ѝ. Настоящият алгоритъм позволява на дадено лице да скрие информацията в друга информация с надеждата, че никой не би помислил да разгледа съдържанието на файла. Алгоритъмът, който е разгледан представлява псевдокод и е възможно да се приложи алгоритъм за стеганография, за да се скрие голямо количество информация в растерно изображение като носител.

Установено е, че настоящият алгоритъм е привлекателен и резултатите, постигнати от него, са ефикасни в областта на вграждане на информация (стеганография). Изпълнени са три вида сравнение: първите две сравняват настоящия алгоритъм в 4 bitmap по размер и добавен шум.

Направено е сравнение на PSNR и с други методи. Именно това сравнение показва, че предложеният метод е по-добър от OPAP и LSB методите.

References:

[1] S-tools(http://digitalforensics.champllain.edu/download/s-tools4.zip).

[2] Chandramouli, R. and N. Memon,. "Analysis of LSB based image steganography techniques," Proc. of ICIP, Thessaloniki, Greece, pp. 7-10, Oct. 2001.

[3] Dumitrescu, S., W. Xiaolin and Z. Wang, "Detection of LSB steganography via sample pair analysis," In: LNCS, Springer-Verlag, New York, Vol. 2578/2003, pp: 355–372, 2003.

[4] Ahn, L.V. and N.J. Hopper, "Public-key steganography. In Lecture Notes in Computer Science of Advances in Cryptology," EUROCRYPT 2004, Vol. 3027 / 2004, Springer-Verlag Heidelberg, pp: 323–341, 2004.

[5] Pang, H.H., K.L. Tan and X. Zhou, "Steganographic schemes for file system and b-tree," IEEE Trans. on Knowledge and Data Engineering, Vol. 16, pp.701–713, 2004.

[6] Dobsicek, M., "Extended steganographic system," In: 8th Intl. Student Conf. on Electrical Engineering. FEE CTU. 2004

[7] Mittal, U. and N. Phamdo, "Hybrid digital-analog joint source-channel codes for broadcasting and robust communications," IEEE Trans. On Info. Theory, vol. 48, pp. 1082 –1102, 2002.

[8] Pavan, S., S. Gangadharpalli and V. Sridhar, "Multivariate entropy detector based hybrid image registration algorithm," IEEE Intl. Conf. on Acoustics, Speech and Signal Processing, pp: 18-23, 2005.

[9] C. Zhang, H.W. Guesgen, W.K. Yeap "Neural Based Steganography, Lecture note in computer science Computational Intelligence. Neural Networks," LNAI 3157, pp. 429–435, Springer-Verlag Berlin Heidelberg 2004.

[10] Moulin, P. and J.A. O’Sullivan, "Information-theoretic analysis of information hiding," IEEE Trans. on Info. Theory, vol. 49, pp. 563–593, 2003.

[11] Amin, P., N. Liu and K. Subbalakshmi, "Statistically secure digital Image data hiding," IEEE Multimedia SignalProcessing MMSP05, China, 2005.

[12] Jackson, J., G. Gunsch, R. Claypoole and G. Lamont, "Detecting novel steganography with an anomaly- based strategy," J. Electr. Imag. Vol. 13, 860– 870, 2004.

[13] W.N. Lie and L.C. Chang, “Data hiding in images with adaptive numbers of least significant bits based on the human visual system”. Proc.IEEE Internat. Conf. Image Process.1,286-290,1999.

[14] C.K. Chan and L.M. Cheng, “Hiding data in images by simple LSB substitution”, Pattern Recognition 37,469-474, 2004.

[15] Стоянова В., Възможности за изпращане на тайни съобщения през Интернет, CIOбр.7,2015, http://cio.bg/7294_vazmozhnosti_za_izprashtane_na_tajni_saobshteniya_prez_internet, [accessed June 30, 2018]

[16] C.C.Chang and W.C. Wu, “A steganographic method for hiding secret data using side match vector quantization”, IEICE Trans.Inf.Syst., Vol.E88-D,no.9,pp.21592167, 2005.

[17] ISO/IEC JTC1 CD 11544: Coded representation of picture and audio information-progressive bi-level image compression, 1993.

[18] Y.Q. Shi, Z.Ni, D. Zou, C. Liang and G. Xuan, “Lossless data hiding: fundamentals, algorithms and applications”, IEEE ISCAS 2004.

[19] Stoyanova, Veselka; Tasheva, Zhaneta. RESEARCH OF THE CHARACTERISTICS OF A STEGANOGRAPHY ALGORITHM BASED ON LSB METHOD OF EMBEDDING INFORMATION IN IMAGES, 2015.