УДК 004.056.5: 518: 512.624.3

Informatics and Mathematical Methods in Simulation
Vol. 4 (2014), No. 1, pp. 44-49

SINGULAR VALUES DECOMPOSITION AS A TOOL ENHANCING THE EFFICIENCY OF STEGANOGRAPHIC ALGORITHM

M.A. Melnyk

Odessa National Polytechnic University,
1 Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: ritochek@yandex.ua

A technique for singular value decomposition of blocks of a cover matrix was improved to enhance the efficiency of decoding the additional information by a "robust to compression attacks" steganographic algorithm which has been developed earlier by the author. The proposed algorithm design ensures reliability of perception of the image. The results of computational experiment are presented to confirm the decrease in sensitivity of the formed stego message to computational error.

Keywords: steganographic algorithm, singular values decomposition, computational error, robustness against lossy compression, matrix

Introduction

In her earlier work [1], the author has proposed $A2$, a "robust against lossy compression, in particular, with significant coefficients" steganographic algorithm based on perturbations of singular vectors (SNVC) corresponding to maximum singular values (SNVL) of blocks of a cover matrix obtained by standard decomposition [2]. It was established that the main disturbing impact for the stego message (SM) obtained with the help of $A2$ and affecting the decoding of auxiliary information (AI; otherwise called secret message) is caused not by compression but by rounding operations involved in generation of the SM. Let us assume that B is an 8×8 block (submatrix) of a cover matrix, $\overline{B}$ is a result of embedding AI in B, $\overline{\overline{B}}$ is a SM block that corresponds to B. In the general case $\overline{\overline{B}} \neq \overline{B}$. This is due to the rounding of values of $\overline{B}$ elements to integers within 0 to 255 range during generation of the SM. It is the computational error that is mostly responsible for errors when decoding AI with the $A2$ algorithm [1].

In her earlier work [3], the author has proposed a technique to reduce the influence of rounding errors on the robustness of the $A2$ algorithm. Let us assume that $\sigma_1 \geq ... \geq \sigma_8 \geq 0$ are singular values (SVs) of an arbitrary B block. The technique involves what is called a singular value decomposition (SVD). Given the fact that post-stego-transformation rounding-off operations disturb mostly the SNVCs corresponding to the smallest SNVLs [4] due to low separateness of these SNVLs (here, by separateness $svdgap(i, B)$ of SNVL σ_i of B matrix we understand $svdgap(i, B) = \min_{i \neq j} |\sigma_j(B) - \sigma_i(B)|$ [5]), the reduction in the sensitivity of such SNVCs (and, therefore, that of a stego message in total) was obtained through artificial increase in the separateness of $\sigma_6, \sigma_7, \sigma_8$ by changing them to

$$\sigma_5 - h, \sigma_5 - 2h, \sigma_5 - 3h, \qquad (1)$$

where $h = (\sigma_5 - \sigma_8)/3$ did not affect the reliability of image perception. However, the results of testing the modified $A2$ algorithm [3] have shown that the value of influence of rounding-off operations on the efficiency of decoding AI in this algorithm requires further reduction.

Purpose of the Work and Problem Setting-up

The *purpose* of the work is improve the efficacy of decoding AI with $A2$, an earlier developed "robust against lossy compression" steganographic algorithm, by reducing the sensitivity of stego message generated by this algorithm to computational errors.

To accomplish the purpose, the following *problems* are to be solved:

1. To determine the causes of remaining (as per [3]) sensitivity of stego message to rounding-off errors, and find the way to further reduction of this sensitivity,
2. To refine the SVD technique, given the requirement to ensure the appropriate reliability of perception of the resultant image.

Body of the Work

In general, the SVD technique proposed in [3] showed some improvement as it ensured the increase in efficiency of decoding AI with the $A2$ algorithm. However, the meticulous investigation of SVD operation related to a separate block has established that reduction of the sensitivity to computational errors occurs not in all the cases. Indeed, if the pattern presented in Fig. 1(a) is observed in the block, than, with the SVD operation performed as per formula (1), the separateness of non-minimal SNVL is reduced (refer to Fig.1b, SNVL σ_6), thus impairing the sensitivity of the block. Therefore, the SVD technique proposed in [3] requires improvement, with the proposed procedure given below.

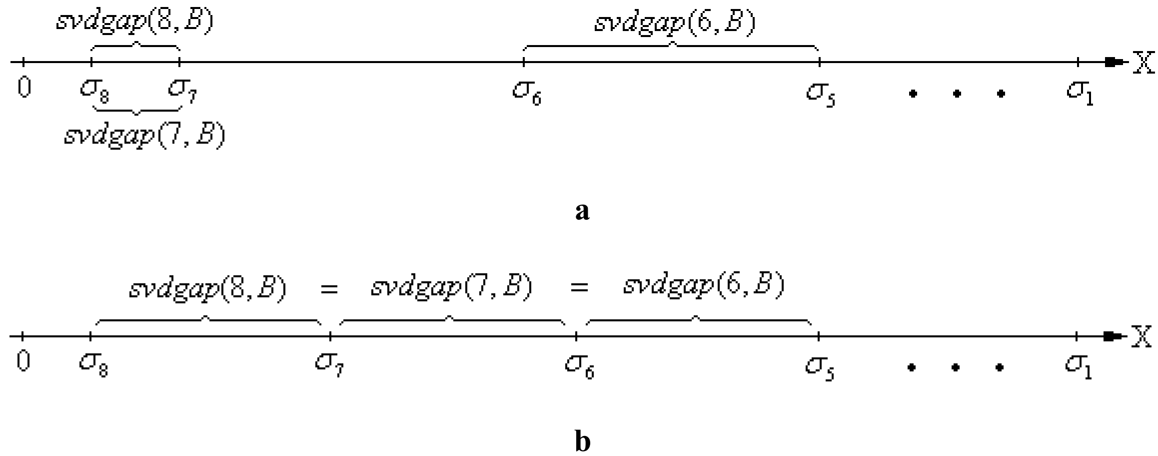


Fig. 1. Possible results of SVD operation: a – SNVL of the block of original digital image; b – SNVL of this block after performance of the SVD operation

In the original digital image, generally, SNVLs of practically all the blocks are non-zero (i.e, positive), and of the smallest separateness are σ_7, σ_8 (Table 1). Given this, to avoid the situation presented in Fig.1, we propose to perform the SVD operation in one of the two following ways.

1. For convenience, we shall denote post-SVD SNVLs of the block by $\bar{\sigma}_i, \overline{svdgap(i,B)}$, $i = \overline{1,8}$. In an arbitrary case, the increase in the separateness of all SNVLs

will be ensured only by increasing the distance between each two SNVLs with consecutive indices. This may be made as per the following formula:

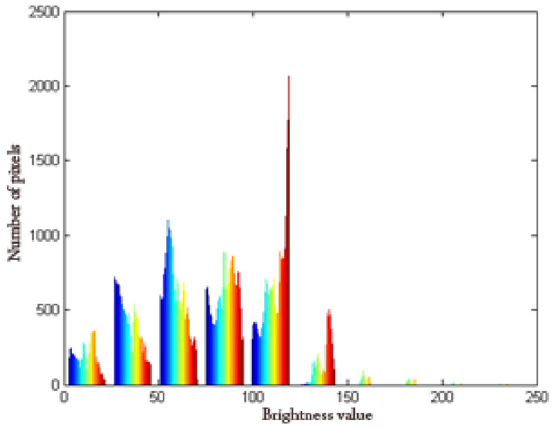
$$\overline{\sigma_i} = \sigma_i + (8-i)h,\ \ i = \overline{1,8}. \qquad (2)$$

Table 1.
Mean values of separatenesses belonging to blocks singular values, received as a result of computing experiment with 200 DI

Mean value $svdgap(i,B)$							
$i=1$	$i=2$	$i=3$	$i=4$	$i=5$	$i=6$	$i=7$	$i=8$
712.4564	23.1111	7.9843	3.0004	1.4232	0.7125	0.4667	0.5781

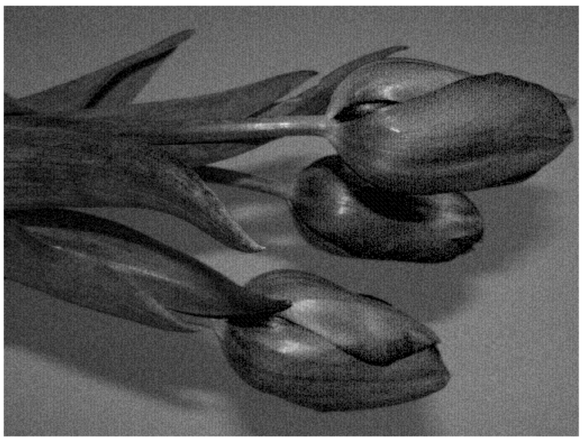
Relationship (2) makes it possible to increase the distance between each two SNVLs σ_i, σ_{i+1} by h, while h must be selected given the requirement for reliability of the perception of post-SVD image. The significant increase in efficiency of decoding with $A2$ stego algorithm occurs when h is comparable with 10; however, in this case, the amount of increase in SNVL value will result in the increase in energy of the image, and, consequently, may result in lightening (Fig. 2c) and even the development of evident artifacts (Fig. 2d).

a



b

c



d

Fig. 2. SVD result showing steadily increase in separateness of every SNVL. a – initial image; b – histogram of DI pixels brightness values; c, d – SVD results

As the computational experiment shows, such situation often occurs in shaded digital images with the pixel brightness histograms similar to that shown in Fig. 2b. Therefore, in practice, we propose to use $h \approx 2$.

2. Considering possible violation of reliability of perception of the DI at SVD when using method 1, in order to enhance efficiency of $A2$ it is proposed to provide SVD via nullification of σ_8, without changing the position of other SNVL (Figure 3a and Figure 3b respectively). This will ensure the increase of $svdgap(8, B)$ without attenuation in separatenesses of all other SNVL, although $svdgap(7, B)$ may not experience changes (Figure 3c and Figure 3d respectively). Method 2 guarantees reliability of perception of the image, although it is much less optimal from the point of $A2$ efficiency enhancing (Table 2).

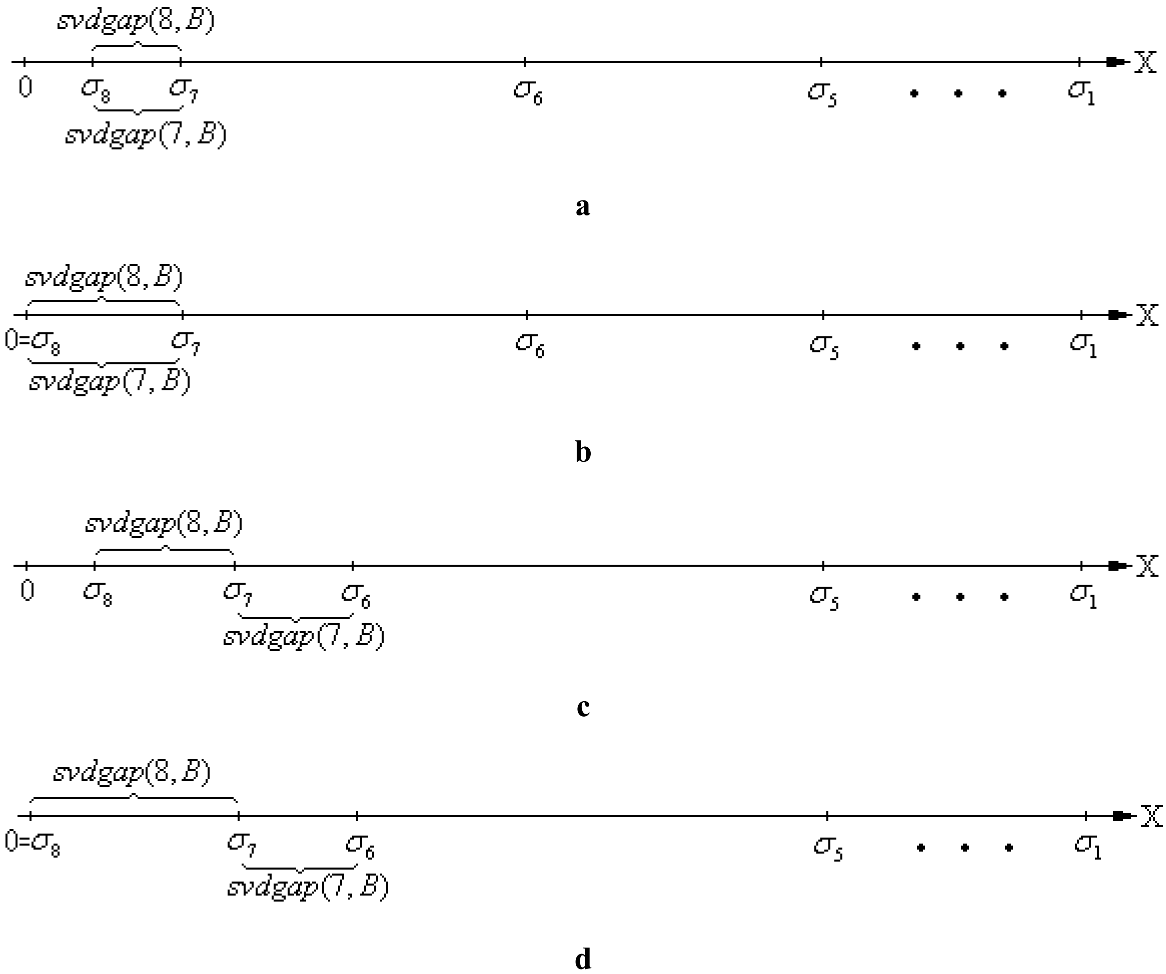


Fig. 3. Result of carrying out SVD using method 1: a, c – SV state in the initial block B; b, d – SNVL state after SVD when using method 1

Results of the computing experiment, involving 300 digital images, shown in Table 2, testify the decoding efficiency increase at the cost of SVD in $A2$, that was evaluated regularly according to correlation coefficient (NC), defined in accordance with [6]: $NC = \frac{\sum_{i=1}^{t} p_i' \times \overline{p}_i'}{t}$, where $p_1, p_2, ..., p_t$, и $\overline{p}_1, \overline{p}_2, ..., \overline{p}_t$, $p_i, \overline{p}_i \in \{0,1\}$, $i = \overline{1,t}$, — correspondingly, secret message inserted in the container and decoded from steganography message, $p_i' = 1, \overline{p}_i' = 1$, if $p_i = 1, \overline{p}_i = 1$, and $p_i' = -1, \overline{p}_i' = -1$, if $p_i = 0, \overline{p}_i = 0$. Therefore, the value $p_i' \times \overline{p}_i' \in \{1, -1\}$ is received.

Table 2.

Results of AI decoding using the $A2$ steganography algorithm

SM format		TIF	JPEG			
			$QF = 80$	$QF = 30$	$QF = 20$	$QF = 10$
Mean value NC	Without SVD	0.9603	0.9577	0.9498	0.9454	0.9359
	SVD with method 1 $h = 10$	0.9801	0.9767	0.9634	0.9484	0.9409
	SVD with method 1 $h = 2$	0.9706	0.9617	0.9569	0.9465	0.9386
	SVD with method 2	0.9621	0.9587	0.9507	0.9453	0.9375

Conclusions

In the present paper, a technique for singular value decomposition of blocks of a cover matrix was improved considering requirements for reliability of perception of the image received as a result. The efficiency of decoding the auxiliary information was improved by a "robust to compression attacks" steganographic algorithm $A2$ due to decrease in sensitivity of the formed stego message to computational error.

References

1. Мельник, М.А. Sign-нечувствительность сингулярных векторов матрицы изображения как основа стеганоалгоритма, устойчивого к сжатию / М.А.Мельник // Інформатика та математичні методи в моделюванні. – 2013. – Т.3, №2. – С.116-126.
2. Гонсалес, Р. Цифровая обработка изображений / Р. Гонсалес, Р. Вудс; пер. с англ. П.А. Чочиа. — М.: Техносфера, 2006. — 1070 с.
3. Кобозева, А.А. Стеганографический алгоритм, основанный на sign-нечувствительности сингулярных векторов матрицы изображения / А.А.Кобозева, М.А. Мельник // Системи обробки інформації. – 2013. – Вип. 3(110), том 2. – С.90-94.
4. Кобозева, А.А. Нечувствительность стеганосообщения к сжатию и формальные достаточные условия ее обеспечения / А.А.Кобозева, М.А.Мельник // Збірник наукових праць Військового інституту Київського нац-го ун-ту ім.Т.Шевченка. – 2012. Вип.38. – С.193-203.
5. Деммель, Д. Вычислительная линейная алгебра [Текст] : теория и приложения / Д. Деммель; Пер. с англ. Х.Д. Икрамова. — М. : Мир, 2001. — 430 с.
6. Lin, W.-H. A blind watermarking method using maximum wavelet coefficient quantization / W.-H. Lin et al. // Expert Systems with Applications. — 2009. — Vol. 36, Iss. 9. — PP. 11509–11516.

РОЗПОДІЛ СИНГУЛЯРНИХ ЧИСЕЛ ЯК ІНСТРУМЕНТ, ЩО ПІДВИЩУЄ ЕФЕКТИВНІСТЬ СТЕГАНОГРАФІЧНОГО АЛГОРИТМУ

М.О. Мельник

Одеський національний політехнічний університет,
просп. Шевченко, 1, Одеса, 65044, Україна, e-mail: ritochek@yandex.ua

У роботі шляхом удосконалення способу розподілу сингулярних чисел блоків матриці цифрового зображення-контейнера підвищена ефективність декодування додаткової інформації розробленого автором раніше стійкого до атаки стиском стеганографічного алгоритму. Запропонована розробка забезпечує дотримання надійності сприйняття зображення. Наведені результати обчислювального експерименту, що підтверджують зменшення чутливості зформованого стеганоповідомлення до обчислювальної похибки.

Ключові слова: стеганографічний алгоритм, розподіл сингулярних чисел, обчислювальна похибка, стійкість до атаки стиском, матриця.

РАЗДЕЛЕНИЕ СИНГУЛЯРНЫХ ЧИСЕЛ КАК ИНСТРУМЕНТ, ПОВЫШАЮЩИЙ ЭФФЕКТИВНОСТЬ СТЕГАНОГРАФИЧЕСКОГО АЛГОРИТМА

М.А. Мельник

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: ritochek@yandex.ua

В работе путем усовершенствования способа разделения сингулярных чисел блоков матрицы цифрового изображения-контейнера повышена эффективность декодирования дополнительной информации разработанного автором ранее устойчивого к атаке сжатием стеганографического алгоритма. Предложенная разработка обеспечивает соблюдение надежности восприятия изображения. Приведены результаты вычислительного эксперимента, подтверждающие уменьшение чувствительности формируемого стеганосообщения к вычислительной погрешности.

Ключевые слова: стеганографический алгоритм, разделение сингулярных чисел, вычислительная погрешность, устойчивость к атаке сжатием, матрица.