

**ANALYSIS AND MODIFICATION OF THE ALGORITHM FOR THE BLUR
DETECTION IN A DIGITAL IMAGE****V.V. Zorilo, O.Yu. Lebedieva, P.S. Safronov**

Odessa National Polytechnic University,
Shevchenko Avenue, 1, Odessa, 65044, Ukraine; e-mail: vikazorilo@gmail.com, o.y.lebedieva@opu.ua

The use of the digital images in modern society is very common, making it difficult to name an industry where digital images are not used. However, in certain situations, the digital images may be direct or indirect digital evidence, such as in court cases. Tampering or violating the integrity of the digital images is one of the important issues in the information protection. The issue of the digital signal authentication by cybersecurity experts is a pressing issue in the present days. Therefore, the development of methods and algorithms for detecting the integrity of digital signals in general, and digital images in particular, is a very crucial task. Among all the possible variations in the integrity violation of digital images can be distinguished a separate group, in which the digital images are processed by various filters editors, such as blurring, sharpening, etc. The blurring is often applied to images not only when they are tampered, but also as a steganographic attack. Blur detection indicates the inability to use a digital image as the evidence of anything. One of the most effective blur detection methods known from the open sources is a method based on the analysis of singular values of blocks of a digital image matrix. The aim of this paper is to increase the efficiency of the blur detection in a digital image by modifying an algorithm based on the analysis of singular values. Computational experiments are performed to determine the number of parameters to be verified. The results obtained allow modifying the algorithm of the method of the blur detection in a digital image. The modification makes it possible to detect tampered access to a digital image. The modified algorithm is no less effective than the original algorithm, and allows analyzing fewer parameters in a shorter time. The computational complexity of the algorithm is determined by the second order polynomial that is acceptable in terms of the practical application.

Keywords: digital image, blurring, integrity violations, singular values, digital evidences, digital forensics.

Introduction

At present, the digital content expertise is actively developing, the software methods for detecting the integrity violations of a digital image (DI), such as cloning, collage, scaling, brightness correction, blurring, are being created and improved. As practice shows, blurring is a very popular tool among graphic designers. The presence of blurring indicates the possible tampering with DI, or the use of a steganographic attack.

In [1], the blur detection method (BDM) based on a general approach, to the analysis of the state and technology of the functioning of the information system, is developed. Among the methods well-known from the open sources, the BDM is the most effective. It is capable of detecting a Gaussian blur of 1 pixel radius that is the most difficult case to detect (figure 1).

One of the advantages of this method is the ability to separate DIs blurred by graphic editors from those which are stored in low-quality lossy format and (or) have a shallow depth of field in the image space (figure 2).

To date, BDM has many modifications and adaptations to detect different types of blurring [2, 3]. The method is based on the analysis of the growth rate of singular values (SVs) of $n \times n$ -blocks of a digital image matrix (figure 3).



a



b

Fig. 1. Image processing: a – before blur; b – after blur



Fig. 2. Shallow depth of field in the image space

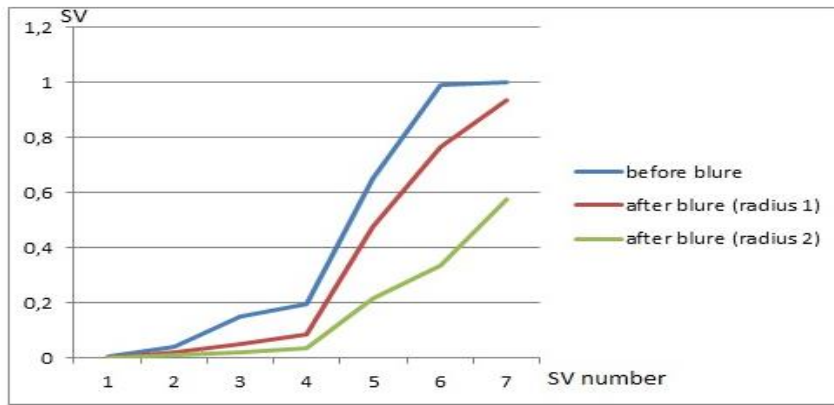


Fig. 3. Interpolating spline powers of one for SV set

According to [4], there is a correspondence between the singular spectrum and frequency spectrum of the digital signal, i.e. the largest singular values correspond mostly to low frequencies, the smallest ones correspond to high ones, with the decrease of the singular value, the contribution of low frequencies becomes smaller and the contribution of high frequencies becomes greater. Because blurring affects mainly the contour of a digital image, it reduces the growth rate of the smallest singular values. The authors of the method found that the analysis of at least five of the eight singular values makes it possible to detect the application of the specified filter. However, the question arises as to why only the five SVs/ are analyzed, since the higher the contribution of the higher frequencies, the smaller the singular value.

The basis of the modification performed is to verification the effect of the number of analyzed singular values on the effectiveness of the blur detection method in a digital image.

The aim of the paper

Is to improve the efficiency of the blur detection in the digital image by modifying an algorithm based on the analysis of singular values.

Main part

The visual result of the blurring is the contour smoothing, which will lead to a decrease in the high-frequency component of the signal. The basic steps of the blur detection method are as follows. The digital image matrix is divided into 8×8 -blocks in standard manner. For each block, the set of singular values is found. For the five smallest singular values in each block, the linear approximation is obtained, and for the approximating function, the derivative, whose value (constant) is the coefficient of the growth rate of the said singular values, is determined. If the maximum value of the coefficient of the growth rate (V_{max}) among all 8×8 -blocks does not exceed the threshold value, then the image is considered blurred.




If the average value of the coefficient of the growth rate (V_{av}) among all 8×8 -blocks exceeds the threshold value, then the image is not considered blurred. In other cases, the method requires additional verification. An additional verification is to have a deliberate blurring of the digital image by an expert, followed by a comparison of the analyzed parameters. If the expert blurring for the image is the first, the analyzed parameters are decreased more than twice (table 4).

With repeated blurring, the required parameters are decreased twice or less. This feature makes it possible to conclude whether the blurring by the expert is repeated for the image, or

it is applied for the first time. Increasing the blur radius only facilitates the blur detection in a digital image. However, the larger the blur radius, the lower the stability of visual perception. That is, an image blurred with a radius greater than one-pixel radius should be alarming, since it is most likely not original.

Table 1.

Influence of the expert blurring on the image analyzed parameters

	Digital image	Vav	Vmax
Original image		2,51	3,54
First blur		0,53	0,7
First blur		0,44	0,52

An experiment is conducted in which three, four, and six smallest singular values of eight ones in the blocks of a digital image matrix are analyzed for the blur detection. The images from the NRSC database recommended for the experimental DI is used for the experiment [6]. One-pixel radius Gaussian blur is performed using Adobe Photoshop. The experiments gave the following results.

In this case, the use of the three smallest singular values has led to a situation where it is almost impossible to distinguish a threshold value when it comes to a Gaussian blur with a radius of 1 pixel. Therefore, the given number of singular values for analysis is not successful in achieving the aim and solving the tasks of the paper. This fact indicates that it is inappropriate to use three SVs instead of the five SVs as in the original algorithm.

The use of the six SVs is resulted in a large number of type I errors, i.e. it led to a situation where the blur is applied, but it could not be detected. The results of the experiment are shown in table 2.

Table 2.

The effectiveness of blur detection with the analysis of the six SVs

Image format	Analysis of the six SVs	
	TIFF	JPEG
Type I errors	48	48
Type II errors	0,0	0,0

Instead, the use of the four singular values is comparable to the results obtained by the use of the five singular values.

The experimental data is partially presented in Table 3. To establish the fact of blurring, the coefficients is calculated using the ten blurred images as an example.

Table 3.

The coefficients of the average growth rate of the four SVs in the images before and after blurring

No	Coefficient of the average growth rate of SVs in the images before blurring	Coefficient of the average growth rate of SVs in the images after blurring
1.	5.3135	0.34524
2.	7.0841	0.73518
3.	5.3754	0.60165
4.	2.5972	0.2591
5.	2.2639	0.5707
6.	3.0558	0.43457
7.	1.9286	0.32922
8.	1.509	0.31949
9.	2.1537	1.439
10.	4.0608	0.6345

As we can see, including in Figure 5, the analyzed indices before blurring are significantly different from those after blurring. This allows to set a threshold value and indicates the possibility of using four singular values for analysis instead of five singular values.

The threshold value is set experimentally and equals to 1.75 when using the four smallest singular values of blocks of a digital image matrix.

Compare the efficiency of the said algorithm to the efficiency of the original algorithm (table 3).

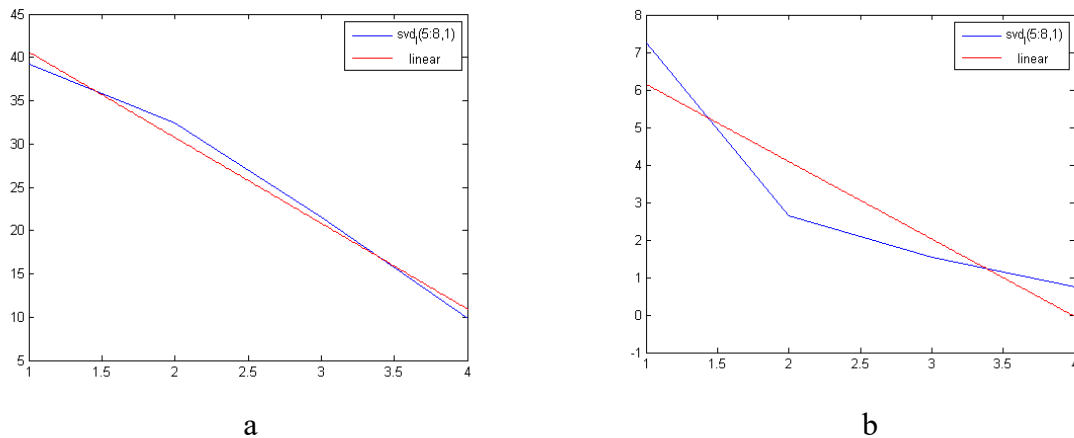


Fig. 5. First order interpolating spline for the 4 SVs (blue graph) and a linear approximation (red graph): a – before blurring; b – after blurring

As we can see, the number of type I errors when using four SVs for analysis is 0.5% higher than when using five SVs. However, the amount of time for the image verification by the software with analysis of the four singular values is 3.6% less than with using five SVs.

Based on the findings obtained, an algorithm of modified method for the blur detection in a digital image is developed.

Table 3.

Comparative analysis of the algorithm with the analysis of four SVs and five SVs

Image format	Analysis of the five SVs		Analysis of the four SVs	
	TIFF	JPEG	TIFF	JPEG
Type I errors	0.0	0.5	0.0	1
Type II errors	0.0	0.0	0.0	0.0

Let F is the $n \times m$ -matrix of the experimental DI.

Step 1. The matrix of the experimental digital image is divided into 8×8 blocks in standard manner:

$$F_{ij}, i = 1, 2, \dots, [n / 8], j = 1, 2, \dots, [m / 8].$$

Step 2. The matrix of singular values is composed: singular value decomposition is performed for each block F_{ij}

$$F_{ij} = U_{ij} \Sigma_{ij} V_{ij}^T,$$

where U_{ij}, V_{ij} are the orthogonal 8×8 -matrices of the left and right singular vectors F_{ij} respectively,

$$\Sigma_{ij} = \text{diag}(\sigma_1, \dots, \sigma_8)$$

is a matrix of singular values, $\sigma_1 \geq \dots \geq \sigma_8 \geq 0$.

Step 3. For $\sigma_l, l = 5, \dots, 8$ blocks F_{ij} a linear approximating function is obtained

$$y = ax + b (w_{ij} = a).$$

Step 4. The matrix of the growth rate W is composed.

Step 5. The average value of the matrix of the growth rate M_F is calculated. If $M_F > 1.75$, the image is not blurred, otherwise the image is blurred.

When obtaining a conclusion about the presence of a blurring, it is recommended to perform an additional verification with the blurring by expert.

Conclusion

The performed modification of the algorithm makes it possible to detect tampered access to the digital image. The modified algorithm is no less effective than the original one and allows fewer parameters to be analyzed in a shorter time. The computational complexity of the algorithm is determined by a second order polynomial that is acceptable in terms of the practical application.

References

1. Зоріло, В.В. Методи підвищення ефективності виявлення порушення цілостності цифрового зображення. / В.В. Зоріло // Інформаційна безпека. – 2013. – №1(7). – С. 34-41.
2. Зоріло, В.В. Вплив розмиття різного радіусу на властивості матриці цифрового зображення / В.В. Зоріло, Ю.С. Колісніченко // Матеріали міжнародної науково-практичної конференції «Інформаційні управляючі системи та технології». – Одеса, 2013. – С.7-9.
3. Зоріло, В.В. Аналіз параметрів цифрового зображення в умовах різних видів розмиття засобами графічного редактору Adobe Photoshop / В.В. Зоріло, К. Кейта // «Захист інформації і безпека інформаційних систем»: Матеріали V міжнародної науково-технічної конференції 02-03 червня 2016 р. – Львів: 2016 – С. 56-57.
4. Кобозева, А.А. Использование особенностей возмущения сингулярных чисел матрицы цифрового изображения для обнаружения его фальсификации / А.А. Кобозева // Искусственный интеллект. – 2008. – №1. – С.145-153.

АНАЛІЗ ТА МОДИФІКАЦІЯ АЛГОРИТМУ ВИЯВЛЕННЯ РОЗМИТТЯ ЦИФРОВОГО ЗОБРАЖЕННЯ

В.В. Зоріло, О.Ю. Лебедева, П.С. Сафронов

Одеський національний політехнічний університет
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: vikazorilo@gmail.com,
o.y.lebedieva@opu.ua

Використання цифрових зображень в сучасному суспільстві настільки поширене, що важко назвати галузь, де б їх не застосовували. Однак у певних ситуаціях цифрові зображення можуть бути прямими або непрямими цифровими доказами, наприклад, у судових справах. Підробка або порушення цілісності цифрових зображень – одна з важливих проблем захисту інформації. Перед фахівцями з кібербезпеки сьогодні гостро стоїть питання перевірки автентичності цифрових сигналів. Отже, розробка методів та алгоритмів виявлення порушень цілісності цифрових сигналів взагалі та цифрових зображень зокрема є дуже актуальною темою. Серед усіх можливих варіантів порушення цілісності цифрових зображень можна виділити окрему групу – застосування обробки різними фільтрами графічних редакторів, таких як розмиття, підвищення різкості тощо. Розмиття доволі часто застосовують до зображень не лише при їх фальсифікації, а й як стеганографічну атаку. Виявлення розмиття вказує на неможливість використання цифрового зображення в якості доказу будь-чого. Один з найефективніших методів виявлення розмиття, відомих з відкритого друку, це метод, заснований на аналізі сингулярних чисел блоків матриці цифрового зображення. Метою даної роботи є підвищення ефективності виявлення розмиття цифрового зображення шляхом модифікації алгоритму, заснованого на аналізі сингулярних чисел. В роботі проведено обчислювальні експерименти щодо встановлення кількості параметрів, що перевіряються. Отримані результати дозволяють модифікувати алгоритм методу виявлення розмиття цифрового зображення. Виконана модифікація дозволяє виявити наявність несанкціонованого доступу до цифрового зображення. Модифікований алгоритм є не менш ефективним в порівнянні з оригіналом і при цьому дозволяє аналізувати меншу кількість параметрів за коротший час. Обчислювальна складність алгоритму визначається поліномом другого степеня, що є прийнятним з точки зору його практичного застосування.

Ключові слова: цифрове зображення, розмиття, порушення цілісності, сингулярні числа, цифрові докази, цифрова криміналістика.

АНАЛИЗ И МОДИФИКАЦИЯ АЛГОРИТМА ВЫЯВЛЕНИЯ РАЗМЫТИЯ ЦИФРОВОГО ИЗОБРАЖЕНИЯ

В.В. Зорило, Е.Ю. Лебедева, П.С. Сафронов

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: vikazorilo@gmail.com,
o.y.lebedieva@opu.ua

Использование цифровых изображений в современном обществе настолько распространено, что трудно назвать отрасль, где бы их не применяли. Однако в определенных ситуациях цифровые изображения могут быть прямыми или косвенными цифровыми доказательствами, например, в судебных делах. Подделка или нарушение целостности цифровых изображений - одна из важных проблем защиты информации. Перед специалистами по кибербезопасности сегодня остро стоит вопрос проверки подлинности цифровых сигналов. Таким образом, разработка методов и алгоритмов выявления нарушений целостности цифровых сигналов вообще и цифровых изображений в частности является очень актуальной темой. Среди всех возможных вариантов нарушения целостности цифровых изображений можно выделить отдельную группу - применение обработки различными фильтрами графических редакторов, таких как размытие, повышение резкости и тому подобное. Размытие довольно часто применяют к изображениям не только при их фальсификации, но и как стеганографической атаке. Выявление размытия указывает на невозможность использования цифрового изображения в качестве доказательства чего-либо. Один из самых эффективных методов выявления размытия, известных из открытого печати, это метод, основанный на анализе сингулярных чисел блоков матрицы цифрового изображения. Целью данной работы является повышение эффективности выявления размытия цифрового изображения путем модификации алгоритма, основанного на анализе сингулярных чисел. В работе проведен вычислительные эксперименты по установлению количества параметров, проверяемых. Полученные результаты позволяют модифицировать алгоритм метода выявления размытия цифрового изображения. Выполненная модификация позволяет выявить наличие несанкционированного доступа к цифрового изображения. Модифицированный алгоритм не менее эффективным по сравнению с оригиналом и при этом позволяет анализировать меньшее количество параметров за более короткое время. Вычислительная сложность алгоритма определяется полиномом второй степени, что является приемлемым с точки зрения его практического применения.

Ключевые слова: цифровое изображение, размытие, нарушения целостности, сингулярные числа, цифровые доказательства, цифровая криминалистика.