Conclusion

The developed program, depending on the configuration of the genetic algorithm, in a short time finds a minimum degree of damage in the identified process of modeling of risks and can be used both in the development of methodological recommendations, as in assessing software risks at its manufacturers.

References

1. James McCaffrey, Analysis of Vulnerabilities and Project Risks Using PERIL. [Electronic Resource] - Access mode: http://msdn.microsoft.com/en-us/magazine/dd315417.aspx
2. I.Sutskever, J.Martens, G.Dahl, G.Hinton. On the importance of initialization and momentum in deep learning. J. Machine Learning Research, 2013, vol. 28, no. 3, p. 140.

UDC 681.215

MATHEMATICAL AND SOFTWARE IMPLEMENTATION FOR IMPROVING THE EFFICIENCY OF THE MOBILE DEVICE CONTENT PROTECTION

Lyudmyla Honchar [1], Sergii Kondyuk [2], Vitaliy Gritsiv [3], Bohdan Kostyk [4]

Ternopil National Economic University

[1]PhD., associate professor, [2)3)4)]Master's Degree Student

I. Statement for the task

In our time, the big problem is that some of the information in the field of economics, politics, as well as individual information can be widely available and have no protection against illegal tampering, copying, blocking or destroying. To solve this problem there are various ways and methods for improving the effectiveness of mobile device content protection [1].

II. The purpose of the work

The purpose of scientific research is the program implementation of the method of increasing the effectiveness of the content protection of mobile devices.

III. Kutter-Jordan-Bossen method for protecting the content of a mobile device

In addition to robustness, the Kutter-Jordan-Bossen algorithm is quite simple to implement: for embedding a digital watermark (DW), there is no need to perform bulky linear transformations of a digital image (DI), DW is built by manipulating color components.

Each image consists of pixels, each pixel represents an combination of three color matrices: red - R, green - G, blue - B, and matrices of transparency - A. The embedding is performed in the blue channel, as the system of human vision is the least sensitive to blue [2].

Let S_i be the bit we embed, container $I = \{R, G, B\}$, $p = (x, y)$, is a pseudo-random position in which the attachment is executed. The secret bit is embedded in the blue channel by modifying the brightness:

$$l(p) = 0{,}299r(p) + 0{,}587g(p) + 0{,}114b(p), \quad (1)$$

$$b(p) = \begin{cases} b(p) + ql(p), & if \quad S_i = 0 \\ b(p) - ql(p), & if \quad S_i = 1 \end{cases} \quad (2)$$

where q – coefficient, which specifies the energy of the data bit, which is built on (based on the functional purpose and the features of the steganosystem). Its value depends on the purpose of the scheme. The greater q, the higher the robustness of an attachment, but the stronger its visibility. Extracting a bits by the recipient is carried out without the presence of the original image, namely blindly. For this purpose, the prediction of the value of the output, unmodified pixel is base (p)d on the values of its neighbors. It is suggested to use the values of several pixels located in the same column and the same row for the pixel estimation. The method used a "cross" pixel size 7×7. The estimate b'' is calculated by the formula (3):

$$b(p) = \frac{1}{4c}\left(-2b(p)\sum_{i=-c}^{+c} b''(x+i, y) + \sum_{k=-c}^{+c} b''(x, y+k)\right), \quad (3)$$

where c – number of pixels from the top (bottom, left, right) from the estimated pixel.

Since in the process of embedding the DW each bit was repeated cr times, we will receive cr estimates of one bits of the DW. The secret bit is located after averaging the pixel estimation difference and its real value by the formula (4).

$$\delta = \frac{1}{cr}\sum_{i=1}^{cr} b_i(p) - b_i(p) \quad (4)$$

The sign of this difference determines the value of the built-in bit.

Since there is no original image on the receiving side, it is not guaranteed to know in which direction the brightness of the blue color has changed. Therefore, the brightness value of blue is predicted for data extraction.

The method has many advantages:

a) high bandwidth;

b) high resistance to unauthorized acquaintance;

c) high resistance to frequency detection;

g) high resistance to the destruction of the younger bits of the container;

e) resistance to compression attack.

Conclusion

Therefore, the proposed method has only one drawback - the detection process is probabilistic. To reduce the likelihood of an error using unrestricted encoding or increasing the number of pixels in the vivinity to accurately extract information from the modified image. That is, it is necessary to use not a square 5×5. With an angle of two pixels and a frame 7×7 or 9×9. The Kutter-Jordan-Bossen for Windows Phone is implemented programmatically.

References

1. Gonzalez R., Woods R., Digital Image Processing. Edition 3. Moscow: Technosphere, 2012, 1104 p
2. Fridrich J., Steganography in Digital Media. New York: Cambridge University Press, 2010, 448 p
3. Kutter M., Jordan F., Bossen F, Digital Signature of color image using amplitude modulation. Proc. of the SPIE Storage and Retrieval for Image and Video Databases, 1997, vol. 3022., pp. 518—526

УДК 004.4

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ДЛЯ РЕАЛІЗАЦІЇ АЛГОРИТМУ РОЗПІЗНАВАННЯ ДВОМОВНОГО ПОТОКУ ГОЛОСОВИХ ПОВІДОМЛЕНЬ В ТЕКСТОВИЙ ФОРМАТ

Марценюк Є.О.[1)], Вільчинський В.[2)]

Тернопільський національний економічний університет

[1)]к.т.н., доцент; [2)]магістрант

I. Вступ

Більшість розроблених програмних ресурсів з автоматичним розпізнаванням мови орієнтовані на правильне, нормативне одномовне мовлення . Однак, часто доводить мати справу з двомовною розмовою, коли чергуються відрізки слів на різних мовах, або змішана, коли в розмові появляються слова або вирази з іншої мови.

Тому створення програмного забезпечення для реалізації алгоритму розпізнавання двомовного потоку голосових повідомлень в текстовий формат, який забезпечує значну швидкодію є актуальною і важливою задачею з наукової і практичної точок зору.

II. Мета роботи

Метою даної праці є створення програмного забезпечення для реалізації алгоритму розпізнавання двомовного потоку голосових повідомлень в текстовий формат.

III. Постановка задачі

На основі аналізу існуючих алгоритмів для реалізації розпізнавання голосових повідомлень в текстовий формат було реалізовано алгоритм програми «Speech to Text», призначеного для обробки голосових повідомлень двома різними мовами (в даному випадку англійська і російська) в текстовий формат [1]. Спрощений алгоритм даної програми складається з наступних кроків :