Науковий вісник НЛТУ України
Scientific Bulletin of UNFU
http://nv.nltu.edu.ua
https://doi.org/10.15421/40290325
Article received 08.04.2019 p.
Article accepted 25.04.2019 p.
УДК 004.056.5:655.25

ISSN 1994-7836 (print)
ISSN 2519-2477 (online)

@ Correspondence author
O. A. Troyan
troyan.oxana@gmail.com

M. A. Nazarkevych, O. A. Troyan
Lviv Polytechnic National University, Lviv, Ukraine

IDENTIFICATION OF LATENT IMAGES IN PRINTED DOCUMENTS

The protection of printed documents plays an important role in the information security of the state. The problems of the development of graphic methods of document protection are analysed. The analysis showed that there is a certain gap in document protection and the control of originality, and also the need for effective protection of documents to prevent their falsification. The possibility to improve the protection result by using latency for the effectiveness of document security is considered. This method allows providing a high level security of information in printed form, leaving no room for possible falsifications even on modern copier devices. The technology of protection involves the creation of protective elements based on the release of latency when attempting to falsify documents. Information technology is developed at the stage of document preparation for printing. The method of protecting printed documents, showing which latent images remain promising in protection, is analysed. The main threats for printed and electronic publications and types of falsifications are determined. The basic principles of protection have been constructed, which ensure the reliability and integrity of the document containing a hidden element. The research of scanned images has revealed that the original document does not match its copy. The article describes the method of identifying means of their unique features. The methods of selecting multiple image keys are explored and they are compared with the corresponding keys of the reference images. The method can be applied in various ways, for example, to recognize graphic elements. The advantages of this method are simplicity of circuit design, increased speed, and accuracy of identification. The results of application of the elemental comparison method for recognition of latent images are proved, which confirms its efficiency. For the protection of documents, a fairly wide range of defence methods is used, each of which is characterized by a certain degree of reliability and has its own specificity, which consists in determining the assessment of threats to the documents, the conditions of their circulation and application. Moreover, it should be noted that any protection will only be effective if it is constantly improved and outpaces the technical and financial capabilities of the initiators of attacks.

Keywords: information technology; identification; latency; printing.

Introduction. Today's protection of information is gaining weight at the state level. The printed information requires more and more secure methods of falsification. At this stage of the development of information technology it is becoming easier to falsify any documentation. So in order to increase the level of protection, it is necessary to develop new methods, which require a lot of time and effort to reproduce. To be effective, he must meet the criteria for reliability and cost-effectiveness. The higher the degree of protection, the harder it is to counterfeit. Modern technologies allow literally to fake everything, but then the question arises whether falsification of the spent effort and money is worth it. The main purpose of the protection is to make counterfeiting unprofitable. It is clear that increasing the quality of document security leads to an increase in the value of fraud. Thus, having considered various cases of document protection, it can be concluded that the development of a protected document is necessary taking into account the maximum protection and profitability.

Analysis of recent research and publications. Interest in falsifications may be caused by documents with signs of par value, authenticity identifier, indirect cost characteristics. Lack of protection in these documents can cause significant damage. Therefore, the problem of protecting printing documents is and remains relevant. Depending on the requirements, there are a number of methods for protecting documents. As an integral indicator of protection in work (Nazarkevych & Troyan, 2013), the parameter is offered as a degree of reliability. In work (Nazarkevych & Troyan, 2014) the levels of reliability of individual methods and means of protection have been developed, which categorized certain types of protection. For the protection of securities and documents of strict accounting from falsification, a classifier of types of protection is proposed. Such a wide range of protective methods is primarily due to the availability of a wide range of potential unauthorized persons to forgery of documents. It is known that a protected document must have the following properties:

- *confidentiality* – to be protected from unauthorized acquaintance;
- *integrity* – to be protected from unauthorized distortion, destruction or destruction;
- *accessibility* – to be protected from unauthorized blocking (Konshyn, 1999).

The following threats may be made to the document:

Інформація про авторів:
Назаркевич Марія Андріївна, д-р техн. наук, доцент, кафедра інформаційних технологій видавничої справи. **Email:** nazarkevich@mail.ru
Троян Оксана Анатоліївна, асистент, кафедра автоматизовані системи управління. **Email:** troyan.oxana@gmail.com
Цитування за ДСТУ: Назаркевич М. А., Троян О. А. Identification of latent images in printed documents. Науковий вісник НЛТУ України. 2019, т. 29, № 3. С. 120–124.
Citation APA: Nazarkevych, M. A., & Troyan, O. A. (2019). Identification of latent images in printed documents. *Scientific Bulletin of UNFU, 29*(3), 120–124. https://doi.org/10.15421/40290325

falsification of a document; loss of some information; replacement of some information; copying of a paper carrier; data digitization; replacement of the document. Therefore, we can identify such threats: partial counterfeiting; full fake; falsification of a document; falsification of personalizing attributes and details of a document; theft.

Commonly accepted methods for managing threats: strategic management; tactical management. Depending on the degree of security, the document may be in: a controlled environment; uncontrolled environment; professional environment (Grechikhin & Shumskii, 2005; Shevchuk, 2004).

Recommendations for management, that is, we formulate a method for counteracting a certain set of threats and form a security policy document. Modern methods of protecting electronic and printed information provide for the use of various elements to protect against counterfeiting. There are four classes of security (Konshyn, 1999). If you can verify the authenticity of a document with a naked eye, then these types of protection belong to the first class of security. In order to check the reliability of the document for the second level of security, there are auxiliary means: a magnifying glass, magnifying glass, an ultraviolet lamp (Nazarkevych et al., 2015). Third-class security includes protection methods that allow you to explore the identity of a document only if you have special equipment or specialized laboratories (Droniuk, Nazarkevych & Opotiak, 2013). There is a fourth class of security where protection is known only to developers who release them. Copy protection aims to effectively recognize the original documents and reveal counterfeits, that is, unauthorized copies. The document provides such properties that are lost when reproduced on the copier equipment (Nazarkevych & Troyan, 2013). It is important that these properties do not change during the use of the document and could not be repeated by malicious people (Nazarkevych & Troyan, 2014). These tasks can be solved with the help of so-called algorithmic methods of document protection. The algorithmic methods are based on computational algorithms for image processing and cryptography. These methods differ from traditional methods of protection, which are based on the uniqueness of the printing process (Larionov & Skrypnikova, 2001). The object of the research is algorithmic methods of copy protection and methods for recognizing security marking on printed documents.

A well-known printing means of protection is a tool created on the basis of the application of flexible elements, which represent a thin graph in the form of colored lines that intersect and can take the form of ornaments, protective grids and other graphic images. The thickness of the lines of cellular elements is 50–90 and 40–70 μm (Kekin et al., 2003). For the formation of the geometries of the corresponding gill-lines, special software is used. The next effective remedy is polygraphic grids, special linear raster, stochastic rasterization (Romanov, Haleliuka & Klochan, 2010), which uses an image consisting of many randomly scattered microglasses of 15–30 microns in size. The images created with linear rasters represent grids of concentric circles or straight lines, and images are formed by changing the thickness of the lines. Micrographics and microtext are used to create documents protection tools (Kovalskyi et al., 2015; Kondratenko & Lernatovych, 2012). They are formed on the basis of the use of high resolution graphic thin lines. In this case, the lines under normal conditions are perceived as thin, consisting of characters, letters (DPI, 2008). Hidden, or latent images are equally widespread in the formation of remedies (Pysanchyn, Zanko & Shovheniuk, 2007). The effect of the latency of the image lies in the fact that when turning at a certain angle of a sheet of paper with such an image there are new elements in it. On these images, the foreground lines are more distinct than the rear (Lernatovych & Kondratenko, 2012; Pandit & Gupta, 2011). In the usual way, latent images have the form of common design elements, and only when the illumination is selected, the hidden part of the image becomes noticeable. The well-known print media "Void Pantograf" (Savchenko, 2011) creates the effect of displaying the signal insert hiding in the background grid of the printing product. At the first stage, the printing of the image of a grid makes for the protection of information, we develop software that would protect the electronic and documents at the preprint stage (Potapov et al., 2008; Honsales & Vuds, 2005).

Today, to protect the forms of securities and documents of strict accounting, the graphical system of Barco (Honsales & Vuds, 2005) is used, which allows to form elements of protection of documents built on certain geometric laws with high accuracy. Such elements include cellular elements, tangent nets, special linear raster, etc. Barco's system allows automating the processes of designing and manufacturing graphic security products and consists of the following software modules: creation and editing of special raster objects; preview on document screen; creation of lines with different and variable thickness; choice of colors for graphic protection means; creating lines of random thickness; creating lines with different gaps and angles.

For the protection of securities, the coding of images by linear periodic raster structures is also used (Shovheniuk & Didukh, 2006; Pavlov, 2006). This method consists in obtaining two images with coded symbols:

- the first – in the form of two interconnected linear rasters;
- the second (the key to it) – with one linear structure.

As a result of the overlay of two images, the coded image is visualized. A known method of encoding an image, where the symbols are dot periodic raster structures, are very sensitive to the boundaries of the contours of the coded image, which does not provide high-quality encoding. In addition, such structures can be easily decoded and tampered with.

The goal of the work – Develop information technology for latent image protection to identify the original document. *Objects of research* – printed documents (forms, certificates, documents requiring protection).

Results. One of the areas of protection that satisfy these conditions are the protection implemented at the prepress stage of manufacturing products. In particular, such means are latent images. However, the existing methods of forming latent images do not fully provide a due degree of protection against falsification, ease of use, and the possibility of using a halftone image as the basis. To eliminate these shortcomings, a method of forming latent images was developed, based on the use of various stochastic raster structures. In the framework of the study, the developed models allow the latent image to be formed by the proposed methods based on the original and concealed images.

We will simulate the formation of latent images by selected paths to the output and input images consistently for each pair of images (Figure 1), respectively, and retained received latent images. As seen in latent images, the plot structure of the original images is completely preserved;

there are no visible signs of the presence of a hidden image. The display of hidden elements in the image provides a high degree of protection. The formation of hidden images is the coded nature of the built-in information. Latent elements that are displayed by the effect of a hidden image on the imprint are the text printed in a font with a height of characters not more than 0.2 mm, practically not visible to the human eye. When using copying equipment, this effect makes it easy to distinguish the original from forgery. When copying the original, the hidden image becomes visible, as well as creates a background grid, which includes a unique pattern that appears when copying. It allows you to distinguish authenticity at the level of expertise and distinguish the original from forgery.

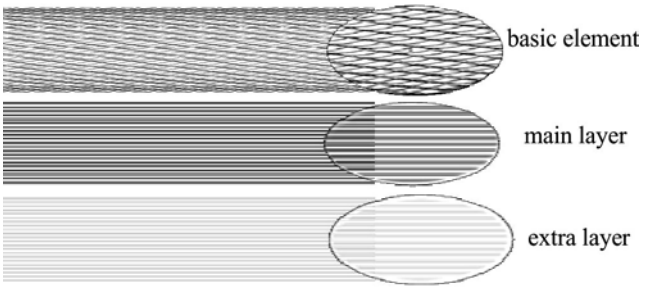

Figure 1. Formation of hidden image layers

The resulting latent images were analyzed by the detected detection method and the resulting hidden images were saved. Figure 1 shows pairs of concealed and detected images. As you can see, the discovered images completely preserved the structure of the hidden images and, in the case of text as a concealed image, fully visible and readable.

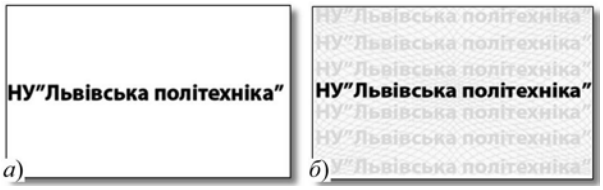

Figure 2. *a*) The appearance of the protected document; *b*) Scanned document with visible hidden elements

As can be seen from Figure 2, the images detected completely saved the structure of the hidden images, in the case of text as a concealable image, it is completely visible to the reader. The latent image is considered visually visible and falsifies. Thus, the developed methods of forming allowed to improve the quality of the formed latent image. A new type of graphic security element based on Hadamard orthogonal matrices is developed. The use of a two-dimensional matrix of binary cells of an ordered non-periodic structure based on Hadamard matrices provides high-resolution image encoding, greatly reduces the noise of a scanned image, and thus provides identification reliability and a high level of copy protection.

Thus, for the protection of printed documents, a fairly wide range of defense methods is used, each of which is characterized by a certain degree of reliability and has its own specificity, which is to determine the assessment of threats to documents, the conditions of their circulation and application. In addition, it should be noted that any protection will only be effective if it is constantly improving and outpacing the technical and financial capabilities of the initiators of attacks. The analysis of existing methods of document protection has shown that for today there are no universal means for this. The reliability of document security is ensured not by the perfection of a particular method, but by a balanced set of different types of it. Formation of the level of protection of documents should be made depending on the real needs for the protection of certain technological processes, served by the relevant documents. An important condition for this is the combination of high reliability and efficiency of security products with their maximum cost. Currently, the means of protection are complex in manufacturing technology, which causes their high cost. However, the approach to the creation of expensive and technologically complex means of protection is completely understandable. After all, there is a proper technique for forging documents, and at this stage, there are such means of protection that would meet the real danger. Most organizations that prepare and use documents of varying importance have systems for automated document circulation, which must ensure that the documents are not undermined not only within their borders, but also in other structures and areas where they will be applied. However, they do not perform these functions. In addition, the security measure of a document provided by such graphic means is determined predominantly by the identity of the respective images with some reference graphic samples. In this case, one of the important tasks of providing a certain level of protection is the determination or identification of the corresponding graphic image as conforming to the standard. The solution to this problem is mainly based on image recognition techniques, which, in turn, are based on comparisons of the standards with the images to be identified. This approach to document identification is extremely cumbersome and complex, since it requires a lot of memory to save all possible standards andcosts of computing resources required for the implementation of classical pattern recognition algorithms. Obviously, the document security system should provide for their operational identification at all stages of use. This requires the creation of low-cost protection technology using modern portable equipment, which would allow the operational identification of documents, because the visual does not provide reliable information about originality. In order to accomplish this task, which can be considered as a counteraction to attacks of forgery of documents, it is necessary to develop methods for the identification of graphic means of protection that would not require significant memory resources and large computational resources, as well as explore and solve a number of problems, in particular:

1) ensuring the identification of documents at all stages of use; creation of an automated document flow system that could respond to changes in the level of protection of printed documents;
2) creation of graphical means of protection in which it would be possible to change the level of protection without changing the technology of production, which would have key geometric parameters, which could be sufficiently accurate identification of the appropriate means of protection (the number of such parameters should be significantly smaller than the number of graphic points an image characterizing it as a whole);
3) development of methods for measuring the corresponding key geometric parameters of graphic images that would not require significant computing resources that would allow them to be implemented within the hardware-software of measurement and identification.

Identification of the latent image is necessary in order to be able to determine the authenticity of the latent image and, accordingly, the printing product that contains it. For ease of use, the method of detecting the hidden part should

be able to be implemented using standard, widely used hardware and software. Such a tool is digital filtering of the scanned image. To be able to use digital filtering, it is necessary to scan the latent image while preserving the raster structure. It was experimentally determined that for accurate reading of a stochastic raster structure with a printed dot size in highlights of 20 μm, the minimum resolution is 2400 dpi. Although the resolution of 2400 dpi and acceptable for reading the raster structure, it is desirable to use a resolution of 5000 dpi, which is quite easily achievable with the current level of technology.

To identify the latent image, it is possible to use various types of filtration: filtering using standard filters of Photoshop, filtering using mathematical programs, for example, Matlab in the spatial and frequency domain. The ability to apply all of these filters has been tested experimentally. Using the standard filters of Photoshop and their combinations turned out to be ineffective. More effectively, as practice has shown, is the use of frequency filters, the form of which corresponds to the distribution of the spectral amplitudes of one of the used raster structures. This is primarily due to the need to perform direct and inverse Fourier transforms before and after filtering, respectively. In addition, for frequency filtering it is necessary to use specialized software, which is not widely used in industry. This filtering method requires a small computational cost, the process of forming filters is quite simple and under certain conditions it is possible to implement filtering in Photoshop using the Custom function. The limitation of this function is the integer filter coefficients and the maximum filter size is 5×5. The formation of the filter was based on the analysis of the structural features of the raster structures, both in their samples and in their spectr.

To build the protective elements that are superimposed on the document, a technology based on the joint use of graphic elements and structural characteristics of latent images is developed. Based on this principle, graphic elements with irregular structure of hidden elements are constructed, which is a serious obstacle for imitation of their digital copiers. The developed technology assumes that each document that needs protection will be provided personification attributes depending on the level of security of the document.

The developed information technology provides documents of additional properties, distinguishes the levels of attributes of documents, provides integrity of data, which reduces the possibility of tampering documents.

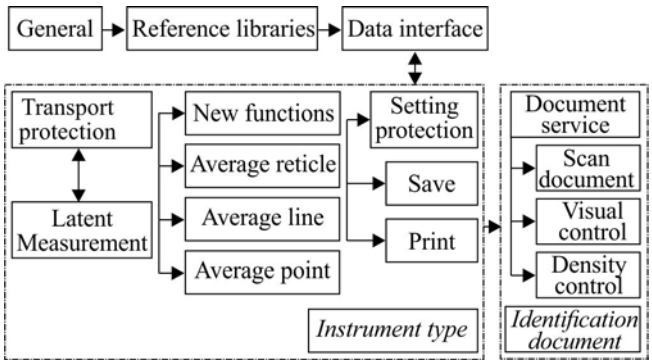

Figure 3. Information technology for the identification of latent images

The developed system of formation and control of latent images, on the basis of the offered methods allows to present processes from the moment of formation to determination of authenticity of the protected document, in contrast to the known, in the developed system the control of latent images is provided.

Information technology for analyzing and identifying documents using graphic elements is very simple and very convenient for programming. In addition, it does not require a large amount of output data, which means that the software implementation of this block diagram will have high performance.

Conclusions. The information technology of protection of printed documents is developed, which provides creation of protective elements on the basis of the formation of latent images. The technology is developed at the stage of preparation of documents for printing. For the first time a method of latent image creation was developed to ensure the authenticity of a document on the basis of the combined use of hidden elements and structural characteristics of images. This method is not complicated in the program implementation, which allows it to be applied on any document to verify originality. The proposed method of protection may be implemented by standard hardware and software. The method is economically feasible and reliable.

Перелік використаних джерел

DPI. (2008). Atiz Innovation, Inc. Making sense of DPI, PPI, Mega–pixels and Resolution / Atiz Innovation, Inc. *Atiz Innovation, Inc. Manual,* 1–4. Retrieved from: https://www.atiz.com/resources/DPI-PPI-Megapixels-and-Resolution.pdf. [In Ukrainian].

Droniuk, I., Nazarkevych, M., & Opotiak, Yu. (2013). Vyznachennia dostovirnosti drukovanykh dokumentiv metodom popikselnoho porivniannia. *Bezpeka informatsii*, *19*(1), 29–33. [In Ukrainian].

Grechikhin, L., & Shumskii, I. (2005). Sistema avtomaticheskoi identifikatcii izobrazhenii s avtokorreliatcionnoi i vzaimnokorreliatcionnoi obrabotkoi ne sviazannykh mezhdu soboi neironnykh setei. *Iskusstvennyi intellekt*, *3,* 381–387. Retrieved from: http://iai.dn.ua/public/JournalAI_2005_3/Razdel5/08_Grechikhin_Shumskiy.pdf. [In Ukrainian].

Honsales, R., & Vuds, R. (2005). Tsyfrovaia obrabotka yzobrazhenyi. *Tekhnosfera, 1072*. Retrieved from: https://www.twirpx.com/file/2344473/. [In Russian].

Kekin, A., Kovalov, A., Kovalov, D., Studinskii, A., Fedotov, A., & Khnykov, Iu. (2003). Apparaturnye sredstva kontrolia podlinnosti dokumentov na osnove opticheskogo metoda nerazrushaiushchego kontrolia. *Spetcialnaia tekhnika, 2*. Retrieved from: http://www.db.agepi.md/inventions/PdfHandler.ashx?id=a%202006%200168&linkPdf=Bib/a%202006%200168.pdf. [In Russian].

Kondratenko, Yu., & Lernatovych, O. (2012). Analiz robastnikh vlastivostei metodu elementnikh porivnian pri identifikatsii. *Iskusstvennyi intellekt. Intellektualnye sistemy: Materials of the international scientific and technical conference,* 2, (pp. 82–85). Donetsk: IPII "Science and education". Retrieved from: http://oaji.net/articles/2015/1872-1428761355.pdf. [In Ukrainian].

Konshyn, A. (1999). *Zashchyta polyhrafycheskoi produktsyy ot falsyfykatsyy "Synus"*, 157 p.

Kovalskyi, B., Zanko, N., Pysanchyn, N., & Shovheniuk, M. (2015). Doslidzhennia kolorymetrychnykh parametriv vidbytkiv za standartom ISO 12647-2:2013. *Science and Education a New Dimention: Natural and Technical Science, 3*(8), 111–115. Retrieved from: http://pvs.uad.lviv.ua/static/media/1-71/9.pdf. [In Ukrainian].

Larionov, V. G., & Skrypnikova, M. (2001). Kak zashchititsia ot poddelki? (Obzor tekhnologicheskikh sredstv zashchity tcennykh bumag, dokumentov i firmennykh tovarov ot falsifikatcii i poddelki). *Marketing v Rossii i za rubezhom, 3*(8). Retrieved from: https://www.cfin.ru/press/marketing/2001-3/07.shtml. [In Russian].

Lernatovych, D., & Kondratenko, Yu. (2012). Identyfikatsiia zobrazhen metodom elementnykh porivnian. *Iskusstvennyi intellekt, 4,* 204–212. Retrieved from: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/57734/20-Lernatovich.pdf? sequence=1. [In Ukrainian].

Nazarkevych, M., & Troyan, O. (2014). Rozroblennia prohramnoho produktu dlia zakhystu informatsii na osnovi plivok iz prykhovanym latentnym. (Ser. Computer Science and Information Technology). *Bulletin of the National University "Lviv Polytechnic", 806,* 187–194. Retrieved from: http://ena.lp.edu.ua:8080/handle/ntb/27223. [In Ukrainian].

Nazarkevych, M., & Troyan, O. (2013). Analiz suchasnykh metodiv ta prohramnykh uzhytkiv z hrafichnym zakhystom drukovanykh dokumentiv. *Tekhnichni visti, 1*(37), 42–44. Retrieved from: http://ena.lp.edu.ua:8080/bitstream/ntb/25913/1/10-61-65.pdf. [In Ukrainian].

Nazarkevych, M., Droniuk, I., Troyan, O., & Tomashchuk, T. (2015). Rozrobka metodu zakhystu dokumentiv latentnymy elementamy na osnovi fraktaliv. *Zakhyst informatsii, 1,* 81–85. Retrieved from: https://cyberleninka.ru/article/n/metod-zahistu-dokumentiv-na-osnovi-efektu-muaru.pdf. [In Ukrainian].

Pandit, M., & Gupta, M. (2011). Image Recognition With the Help of AutoAssociative Neural Network. *International Journal of Computer Science and Security, 5,* 54–63. Retrieved from: https://www.researchgate.net/publication/232708673_Image_Recognition_With_the_Help_of_Auto-Associative_Neural_Network

Pavlov, Y. (2006). Kontrol podlynnosty dokumentov, tsennykh bumah y denezhnykh znakov. *Tekhnosfera, 472*. Retrieved from: https://bigl.ua/p708528816-potapov-pavlov-kontrol. [In Russian].

Potapov, A., Guliaev, Iu., Nikitov, S., et al. (2008). *Noveishie metody obrabotki izobrazhenii.* Moscow: FIZ-MATLIT, 496 p. Retrieved from: http://fireras.su/biblio/wp-content/uploads/50999.pdf. [In Russian].

Pysanchyn, N., Zanko, N., & Shovheniuk, M. (2007). Modeliuvannia syntezu koloriv u rastrovomu protsesi. *Naukovi zapysky Ukrainska akademiia drukarstva, 1,* 23–40. Retrieved from: http://nz.uad.lviv.ua/static/media/1-11/6.pdf. [In Ukrainian].

Romanov, V., Haleliuka, I., & Klochan, P. (2010). Tekhnolohii autentyfikatsii osoby za biometrychnymy kharakterystykamy. *Computer zasoby, merezhi ta systemy, 9,* 54–61. Retrieved from: http://journals.khnu.km.ua/vestnik/pdf/tech/2012_1/47sin.pdf. [In Ukrainian].

Savchenko, A. (2011). Metod napravlennogo perebora dlia zadach klassifikatcii s bolshim kolichestvom alternative. *Raspoznavanie obrazov*, *1,* 30–40. Retrieved from: https://publications.hse.ru/books/82233163. [In Russian].

Shevchuk, A. (2004). Zakhyst blankiv tsinnykh paperiv ta dokumentiv suvoroho obliku za dopomohoiu hrafichnoi systemy Barko. *Drukarstvo, 2,* 12–16. [In Ukrainian].

Shovheniuk, M., & Didukh, L. (2006). Hrafichnyi element zakhystu tsinnykh paperiv. *Kompiuterni tekhnolohii drukarstva, 16,* 245–251. [In Ukrainian].

М. А. Назаркевич, О. А. Троян

Національний університет "Львівська політехніка", м. Львів, Україна

ІДЕНТИФІКАЦІЯ ЛАТЕНТНИХ ЗОБРАЖЕНЬ У ДРУКОВАНИХ ДОКУМЕНТАХ

В інформаційній безпеці держави важливу роль відіграє захист друкованих документів. Проаналізовано проблеми розвитку графічних методів захисту документів, які застосовують як у соціальній сфері, так і в сфері управління. За результатами аналізу з'ясовано, що існує певна прогалина в захисті документів та контролі оригінальності, а отже, потрібно запровадити ефективний захист документів для запобігання їх фальсифікації. Розроблено спеціальні графічні побудови, на основі яких створено латентні елементи, що підвищують ефективність та надійність захисту. Розглянуто можливість поліпшити результати захисту за допомогою використання латентності для підвищення ефективності захищеності документів. Цей метод зможе забезпечити високий рівень захисту інформації в друкованому вигляді, не залишаючи можливості фальсифікації навіть на сучасних копіювальних пристроях. Технологія захисту передбачає створення захисних елементів на основі виникнення латентності у разі спроби фальсифікації документу. Інформаційну технологію розроблено на етапі підготовки документів до друку. Проаналізовано методи захисту друкованих документів та показано, що латентні зображення залишаються перспективними у захисті. Визначено основні загрози друкованих та електронних видань і види фальсифікації. Побудовано основні принципи захисту, які забезпечують надійність та цілісність документа, що містить прихований елемент. Досліджено скановані зображення і виявлено, що основний документ не відповідає копії. Також описано метод ідентифікації зображень за їх унікальними особливостями. Суть методу полягає у виділенні множини ключів зображення та в їх порівнянні з відповідними ключами еталонних зображень. Метод можна застосовувати для різних прикладних задач, наприклад, для розпізнавання графічних елементів. Перевагами цього методу є простота схемотехнічної реалізації, підвищена швидкодія та точність ідентифікації. Наведено результати застосування методу елементних порівнянь для розпізнавання латентних зображень, що підтверджують його працездатність та ефективність. Для захисту документів використовують досить широкий спектр методів захисту, кожен з яких характеризується певним ступенем надійності і має свою специфіку, що полягає у визначенні оцінки загроз щодо документів, умов їх обігу і застосування. Окрім цього, треба зазначити, що будь-який захист буде ефективний тільки тоді, коли він постійно вдосконалюється й випереджає технічні і фінансові можливості ініціаторів атак.

Ключові слова: інформаційна технологія; ідентифікація; латентність; друк.