O. Troian

National University “Lviv Polytechnic”

Department of Information Technology Publishing Affair

IDENTIFICATION OF THE LATENT ELEMENTS IN THE PRINTED AND ELECTRONIC DOCUMENTS

Проаналізовано методи захисту друкованих документів та показано, що латентні зображення залишаються перспективними у захисті. Визначено основні загрози друкованих та електронних видань та 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.

Ключові слова: спосіб захисту, цінні папери, захисні елементи, зображення.

The methods of protection of printed documents are analyzed and it is demonstrated that latent images stay very promising in protection. The main threats of the print and electronic media and types of fraud are determined. The basic principles of protection which ensure the reliability and integrity of the document containing latent element are created. A study in the work of the scanned images is conducted, and it was found that the main document does not correspond to the copy.

Key words: method of protection, securities, security elements

Introduction

Protection of printed and electronic documents at this stage of the technological process development requires special features of creation of security elements to minimize the possibility of fraud. This relates to the documents of state importance, the documents of individuals, banknotes, forms, coupons, and documents of electronic data bases. In a rather fast pace of information technology development, printed documents will need high-quality protection for many generations. Thus, the following types of printing products particularly badly need the protection from the fraud. Using these objects of printing design, the protection from falsification of the printed production is carried out.

The issue of protection of printing registration arose particularly acute in connection with the development of reproduction and digital technology that allows easily enough recreating and forging the document if it has no protection. Unlike traditional objects, the application of protection products have certain limitations – security elements should be visually inconspicuous and not to attract attention. These restrictions primarily relate to the value of the protected production, its semantics, character of design, and materials used.

Given the restrictions imposed on the means of documents protection, the applicability of most of them as well as economic efficiency is small. The effectiveness of protection of the majority of existing methods should be cost-effective.

Problem

Since the beginning of the printed and electronic documents and financial documents which have financial or economic importance for the state or individual it is necessary to protect them from fraud. Currently, the need to combat counterfeiting has become more acute. Current urgency of the issue is largely due to the development of printing technology, including digital, and its wide distribution. No matter how complex and effective the protection against fraud is there will soon be the way to recreate it. Therefore, the effectiveness of the protection depends on innovation methods, which defines a constant need for new means and technologies of protection [2].

All currently used methods of technical and technological methods of protection of printed products can be divided into five major groups: the defense at the stage of design, protection through special printing technologies, protection through the use of special printed base, protection through the use of a special paint, protection by processing the products. Of all these, graphical means of protection, based on the use of methods of processing and forming the image, minimally affect the price of the final product.

The necessary characteristics of the created means of protection are determined:

1. the possibility of introducing the latent image into the protected main image, which has no significant restrictions on semantics;

2. the invisibility of the latent image when visually assessed;

3. the ability of implementing on standard equipment without substantial changes in technology and the use of special materials;

4. the ability to determine the authenticity of the protected element without the use of special equipment;

5. the inability to recreate the original image when discovering the presence of latent content.

The main part

With all the variety of available graphic means of protection there is a gap in the protection of the inexpensive widespread products - forms, transportation vouchers, certificates [1]. Virtually there are no funds with high protective properties which are implemented using standard equipment which allows labeling the security elements without changing their visual characteristics.

The high degree of protection of printed products is determined by three components:

- complexity of technological processes
- limited access to the materials and equipment
- novelty and closeness of the methods used.

The development and application of the complex technologies such as metallographic, gravure printing, the use of special paints and coatings, protective laminates, holograms are not always appropriate from the economic point of view. The use of the materials with special chemical, physical properties creates the need for the use of special equipment to determine the authenticity of the product.

The easiest, the most convenient and economically feasible are means of protection implemented in the pre-press stage. Their use does not require special equipment and materials. There remains the possibility of their use for the creation of combined methods of protection. Development of the new and improvement of the existing methods of protection of printed documents is important for the safety and protection of the printed documents.

A method of forming the latent image which is implemented by using the methods of fine graphics that create structures close to the sub-elements size, but different in structural properties [5].

A method of visualization of the latent image which is implemented by the use of the software and equipment in use and equipment that can detect the images implemented and, thus, ensures inability to allocate this image for the use as an original source for fraud.

The process of creating the latent image consists of directly forming the latent image and a platform to identify latent content. The formation of the latent image consists of the following stages:

- Selection of the structures of fine graphics and formation of the filter to identify the latent image;
- Selection and preparation of latent images;
- Formation of the latent image;
- Printing of the image.

These technical recommendations were referred based on the implementation of the method of forming the latent image and the mode of its detection using the Photoshop program.

This method shows the difference between the figure 1a and 1b, during the comparison we can estimate not the number of uniform items that will not match when using the algorithm of the comparison of raster dots.

Selecting raster structures is the key moment in the process of the latent image creation. To create the latent image, stochastic raster structures are used, which are created by those available in the algorithm of rastering. It is necessary to conduct structural analysis to determine the possibility of their use. The

analysis is conducted based on the samples of raster structures obtained by rastering of a gradual transition or optical wedges [4].

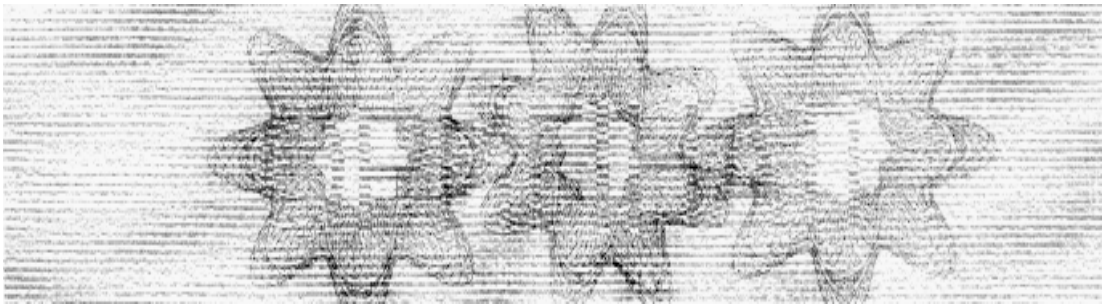

Fig. 1a. Original security image with visible latent image

Fig. 1b. A copy of the image with visible latent image

To form the latent image it is necessary to find structures that have the same visual characteristics and also have structural differences. Structural differences should allow the allotment of the latent image. To test this possibility when selecting the structures one must perform the projection of the security element and the verification of its efficiency. To test the effectiveness one should use the model of the printed latent image.

In order for the security structures to be visually imperceptible it requires the adherence of two conditions: the proximity of frequency parameters of raster structures and sub-elements size less than 50 microns. Frequency parameters are largely determined by the size of the dot given while rastering. In some cases, the size set by the rastering not accurately determines the size of the sub-elements which form the image. In this case, it is necessary to compare the visual samples of structures at high zooming. Original electronic images are used as samples. Forming the security elements should be the same. Determining the size of the raster dot should be made in the areas of tone 50–10 %. With this infill there is no contact of the raster dots. As useful software tools program Photoshop may be used. When displaying the images program does not use on-screen anti-aliasing.

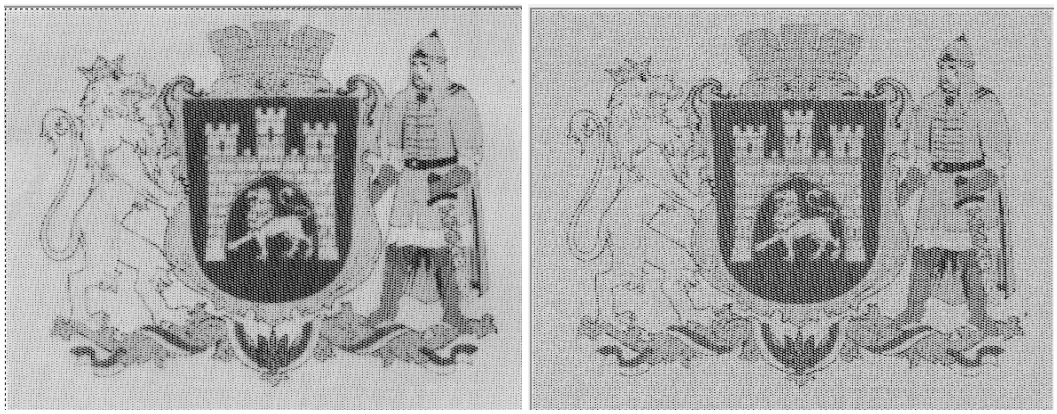

Fig. 2. Security image of the map of Ukraine by the method of color infill

Applying of the selected raster structures is possible only after building the filter which detects latent image. To check the ability of the filter can be done by comparing the results of the processing of model images formed by using the selected raster structures. Using the model allows us to predict the result of the impact of the filter on the printed latent image which reduces both material and time expenditures.

To obtain the model it is necessary to rasterize the plot image or gradient transition. When rastering, the image is recorded as a file in either PS or TIFF format. Most of the raster processors support the recording of the rasterized image in these formats.

In order to process in Photoshop, the Image inscribed in PostScript format, it is necessary to convert it lossless into the TIFF format. As practice shows, you need to only change the file extension.

The images in TIFF format may be open in Photoshop. The two compared images are placed into one document as layers. Then, the merge of the layers occur. The result is a document inside which the images are located next to the rasterized image using raster structures studied. To imitate the distortion occurring during the printing / scanning the image blurring is performed using Gaussian Blur filter. The parameter of the filter – Radius – is selected by the experienced way. For the glossy enamel paper this parameter equals 0.7.

To calculate the non-zero optical density of paper, the reduction of the upper output of the initial levels is carried out by using the instruction Levels.

To form the filter one must use the function Filter, Custom. Formation of the filter is done by the method of selection. As the source sharpening filter (2) should be used where n is a positive number that determines the degree of sharpening.

Then, it is necessary to change the filter coefficients of sharpening so that the direction of the coefficients change would be consistent with the direction of clusters of raster structure of the processed image (2).

Formation of protection based on the guilloche elements

A method of protecting the electronic and paper documents by creating the security grid is provided. The developed software allows selecting the type of lines created from a database created and to build graphic compositions in vector format which provides high-quality printing of the document protected. Selecting the parameters allows getting different types of graphs that allows personalizing of each document. Protected information is written in PostScript file which can be used by any image. It may contain plot information, pattern or picture of the symbols. Introduction of the image may occur around the whole field of the main image as well as at the small area of it. In order to avoid the excess loss of the details of the latent image during the identification, it is necessary for the size of details of the latent image was not less than 1 mm.

During the implementation the image must be in the form of one-bit. The sequence of operations is performed to prepare the image to the introduction.

The command Image - Adjustments – Threshold is used to binarize the image. This command allows you to set the threshold of binarization. As a rule, the plot image contains sufficient number of small details. After binarization of some images, small parts may look as separate light or dark dots of the image because of the presence of extreme overfalls of brightness in these fields. To remove this, it is necessary to conduct the low-frequency filtering of the image.

The specific value of the parameters is chosen depending on the characteristics of the original image and the required size of the details after processing. With blurring of the image, a transition from dark gray to light gray appears on the border of the sharp details. Part of dark pixels belonging to detail is getting brighter and some part of the pixels relating to the surrounding white area is getting darker. Then, the size of the details is determined by changing the binarization threshold. In some cases it is necessary to reduce the size of some parts and others – to increase, or change in one direction the sizes of the light as well as the dark details. In this case, a gradual correction should be used before binarization, and only then – binarization.

Thus, to create the right balance of large and small details it is necessary to apply a combination of low filtration techniques and gradual correction. After all preparatory operations are done, the image

conversion into the one-bit sequence is generated with the help of commands Image – Mode – Bitmap. If you convert input and output images they should coincide, the binarization method – 50 % Threshold. After this operation, the implemented image is ready to use.

If there is a possibility of choice of the main image, it is better to avoid images with large solid areas of uniform tone. The distribution of brightness of the image by pixels affects the degree of detection of the latent image. For more seamlessness of the latent image by visual analysis and the increase of the degree of detection of the latent image is preferably uniform distribution of brightness in the center part of the histogram.

With the implementation of the latent image into the color image, the introducing is performed into one of the CMYK color channels [6]. Accordingly, if the printing uses larger number of inks, the implementation can occur in any channel of color-separated image. In determining the channel for the introduction of the latent image it is necessary to analyze medium brightness of the channel. It should not be too dark and too bright (the analysis is made by percentage filling). The paints brightness of primary colors and their overlapping should be taken into account.

The analysis of the structure of PostScript-files enabled to offer information technology for the protection of documents. The PostScript programming language and building the required elements into the appropriate PostScript-files is used to create security elements. Thus, we can not build only security elements, but also encrypt or hide the required information.

The following stages to build the secure model of publications are offered:

1. Analysis of the file structure;
2. Search of the scenario change;
3. Generating the necessary PostScript code scenario;
4. Adding the code of protection into the places found;
5. Generation of the document model with protection.

Thus, the operation of protection based on the Ateb-functions before the operation of writing the file in PostScript or PDF format is added into the standard information technology of pre-press preparation (see. Fig. 3).

The model can be made in the standard software or in a developed information technology. If the model is done in the developed information technology, the sequences of the actions of a protected model of the edition are:

- Creation of the model of edition in the developed information technology;
- Adding the security elements into the model;
- Generating the PostScript or PDF file.

One of the degrees of document protection is the presence of the complex types of graphic elements. They are divided into: guilloche grids, protective grids of any types including those with irregular structure of graphic elements, special types of rasters, etc. Background grids are complex elements that intertwine and constitute an obstacle to imitate them using digital copiers. Fine lines that make up the background grids constantly change the direction and curvature, so they cannot be truly copied. The grids are performed with the use of unsaturated paints, and if they are to be copied with the use of the office equipment they will “break” into separate dots when using printers. The method offered was applied during the stage of pre-press preparation of the document. The scheme of the method is presented in Fig. 3.

We will describe the algorithm of the method, the scheme of which is shown in Fig. 3. We choose the document generated in any software. For text documents it may be MS Word. For the model of package the source file can be the layout presented in any software for printing publications. Block 2 suggests the presence of pre-calculated values of Ateb-functions of the single graphic element. Block 3 implements the construction of the form of protective grid. The choice of the repetition of lines algorithm is conducted. When building the protective grid one can change the color, thickness and type of lines. The graphic element is multiplied by parallel displacement, rotation, compression or tension, copying, combining different combinations and so on for the protective grid formation. In the Block 4 we conduct the forming of the code in PostScript language which will implement the chosen design of the protective

grid. In Block 5 the combination of single file of the protective grid and output document is performed. At this stage, the forming of the protected document is complete. But if necessary, the file can be converted into PDF format in block 6.

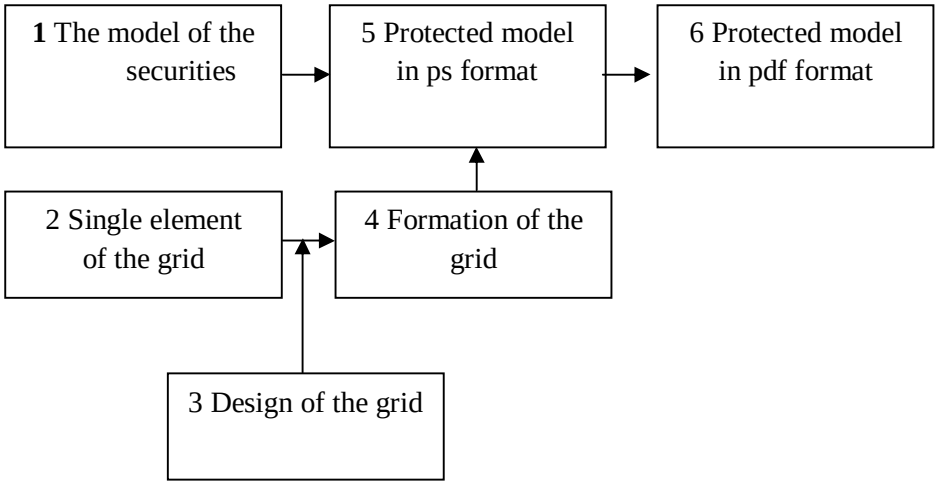

Fig. 3. Diagram method of constructing the protective grid [7]

The methods and, based on them, information technology and software for building the documents of vector format which are protected from unauthorized access by imposition of protective grids of unique structure, are developed.

To build the protective grids superimposed on the document, a technology based on precise mathematical formulae is developed. Graphics primitives, based on the offered method of protection using the PostScript technology, are built according to these formulae. The method is designed, and based on it, the software which helps building the security elements, elements of the small graphics are geometrical basis for the figures of which. This information technology can be used not only to protect the printed production, but also to protect the documents for general public use on the Internet.

Protection using fine graphics is based on the difficulty of reconstruction and reproduction of fine graphic elements: guilloches, grids, rosettes, vignettes, latent elements and micrographics. Printing protection is considered effective if the document area is covered at least in 70 % with fine graphics. Difficulty of reproduction is connected with complex geometry structure and minimum possible thickness of the lines of the fine graphics elements.

Special software is developed for printing information protection that makes it possible to build fine graphics in vector format that provides the highest quality of output printed production.

The file built using this method is ready for viewing by any user, pritected and suitable for printing replication.

Forming protection based on traps

One of the ways to protect the documents is to create the graphic traps in which the infringement of the existing image or text document is performed. Creation of the graphic traps is done through deliberate distortion of lines. Various tricks are used in the construction of graphical trap: subtle breaks in graphic ornaments; intentional violation of local symmetry when reconstructing one of the multiple repetitive elements of the ornament; in the text details – the use of single characters which are different from others in size, type or tilt, etc. In addition, you can insert some secret ornaments and other complex drawings, fragments of repeated strokes of the given thickness and period (Fig. 4).

This method creates a neutral background that will be printed on the original one. When copying the original, the latent image becomes visible and also the background grid is created which includes a unique pattern that appears when copying. Background grid is based on the construction of lines of varying thickness. This helps to distinguish the authenticity at the level of expertise and distinguish the original from the fake. Generation of the unique code ensures the reliability even if the same software will be used.

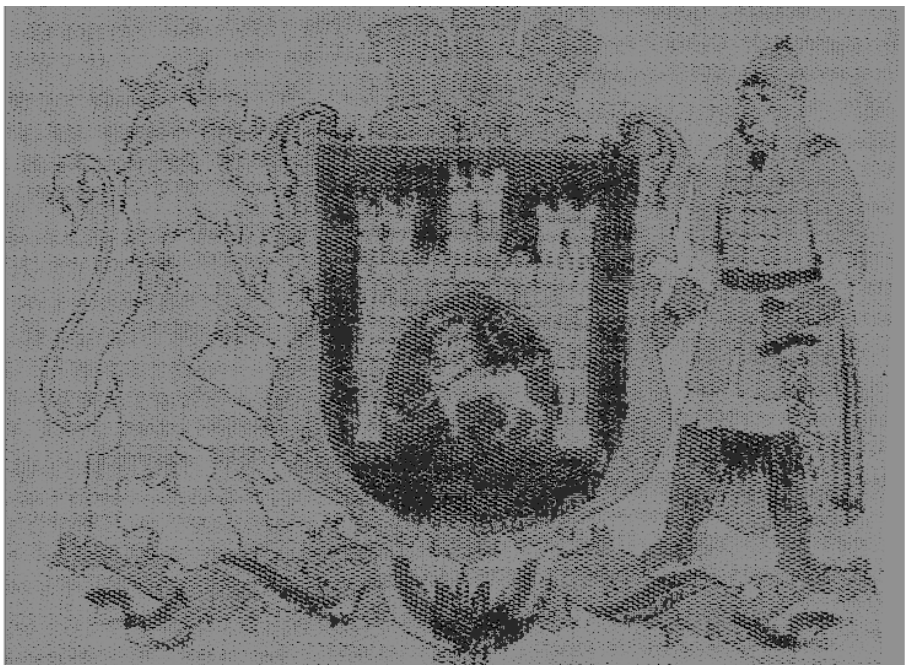

Fig. 4. Image formation based on lines perturbation

The developed protection of the document includes such graphic (dashed) security elements: background guilloche protective grids, with the size of positive lines of 40-80 microns according to the state requirements [3] and negative ones – of 60–100 microns, and micro text. The main element of the raster image is a dot (the point). The size of the dot of raster image depends on the technique used and the parameters of the rasterization of the original image. During the rasterization, lines grid, cells of which form the raster element, is superimposed onto the original. Raster grid frequency is measured by the number of lines per inch (lpi – lines per inch) and is called the raster frequency. Rastering depends on the optical density since all objects are described in the coordinate grid of a certain size. Many printing machines print the image with maximum raster frequency of 120–160 lines per inch. In order to reliably protect the document it is needed to create such small touches of micro text which will be well printed on the offset printing machine. So, the minimum number of reproducibility of the dashes and micro text with offset printing, raster frequency of the text of 150 lpi in which the image is blurred for the observer, and raster frequency of 200 lpi where only a small number of printing machines can print high-quality images, are defined. [10] That's why during the copy or reprinting of the document after scanning, the frequency and the number of rasters is changing, and using the program we get a result of the document forgery.

Conclusions

Special software was developed for printing information protection, which makes it possible to build fine graphics in vector format, which provides the highest quality of the output printed production. The file, which was built using this method, is ready for viewing by any user, secure and suitable for printing replication. As a result of the development of the method for protecting the printed products, methodology and criteria for selection of raster structures to form the latent image was developed. Used raster structures should have almost unnoticeable visual characteristics and different structural and / or frequency characteristics. The following raster structures were selected and analyzed. The method of their choice on the basis of spectral and structural analysis is designed. The method of forming the latent images using raster structures that meets the specified criteria is designed. The method is implemented using industrially applicable hardware and software. The method does not limit the image into which the latent image was introduced, which enables the use of the method for protecting a wide range of products. Formed printed latent image is characterized by the seamlessness of the inserted image during the visual assessment. A study of the protective properties of the latent image was made, which showed that the exact allotment of

the latent image is necessary to form the falsified latent image, is almost impossible. Falsified image contains obvious signs of fraud expressed in the visible latent image distortion. The work is illustrated by examples.

1. Maria Nazarkevych Analysis of Software Protection and Development of Methods of Latency in Printed Documents / Maria Nazarkevych, Oksana Troyan // In Proc. of the VIIIth International Scientific and Technical Conference CSIT 2013, 16–18 November, Lviv 2013, p.120–121. 2. Medykovskyy Mykola Methods of protection document formed from latent element located by fractals / Mykola Medykovskyy, Piotr Lipinski, Oksana Troyan, Mariya Nazarkevych // In Proc. of the X International Scientific and Technical Conference CSIT 2015, 14–17 September, Lviv 2015, p. 70–73. 3. Dronyuk I. Development of a method of protection of securities in the prepress stage / Dronyuk I., M. Nazarkevych, A. Myronyuk // Proceedings of the National University "Lviv Polytechnic". COMPUTER science and information technology. – 2011. – № 694. – P. 352–358. 4. Nazarkevych M. Analysis of modern methods and software items with graphical protection of printed documents / Maria Nazarkevych Oksana Trojan // Technical missing. – 2013. № 1 (37). – S. 42–44. 5. Nazarkevych M. Development of a method of document protection latent elements based on fractals / Nazarkevych M., I. Dronyuk, A. Troyan, T. Tomaschuk // Information Security. – 2015. – № 1. – P. 81–85. 6. Nazarkevych MA The method of document protection from moiré effect / MA Nazarkevych, OA Trojan // Scientific Herald NLTU Ukraine. – 2015. – Vol. 25.8. – C. 337–346. 7. Nazarkevych M. Mathematical model of document security with the formation of moiré based on multiple periodic lattices // MA Nazarkevych, O. A. Troyan // Computer Technology Printing: Coll. Science. works. – Lviv: UAH works, 2015. – № 30. – P. 164–170.