electronics

MDPI

Article

An Approach towards the Protection for Printed Documents by Means of Latent Elements with Fractal Grids and Electronic Determination of Its Authenticity

Mariya Nazarkevych [1], Ivan Izonin [1,*], Michal Gregus ml. [2] and Nataliia Lotoshynska [1]

[1] Department of Publishing Information Technologies, Lviv Polytechnic National University, 12 Bandera str., 79000 Lviv, Ukraine; mariia.a.nazarkevych@lpnu.ua (M.N.); natlot@ukr.net (N.L.)

[2] Department of Information Systems, Comenius University in Bratislava, Odbojárov 10, 82005 Bratislava, Slovak Republic; michal.gregusml@fm.uniba.sk

* Correspondence: ivan.v.izonin@lpnu.ua; Tel.: +38-(098)-888-96-87

Received: 7 March 2020; Accepted: 16 April 2020; Published: 20 April 2020

Abstract: An electronic method of protection for printed documents based on which latent elements are formed in a printed way has been developed. The development of security features has been done electronically. Protection using latent elements has been improved by overlapping fractal grids, which allows creation of graphics traps. The printing of designed security elements has been investigated on 15 paper samples. The security elements were printed on an offset printing machine. Prints were copied and compared with originals using the electronic method of pixel-by-pixel comparison based on a peak signal-to-noise ratio (PSNR). The comparison results between originals and their copies are presented in this paper.

Keywords: security element; electronic determination; latent image; printing technique; documents authenticity

1. Introduction

One of the challenges of the digital age is efficient processing of a vast amount of information in the digital form [1,2]. Despite that, there is a need to produce, store and present a large number of printed documents [3].

Under present conditions of business, its environment creates and consumes thousands of printed documents, based on which certain business decisions are made [4]. In such a large flow of information exchange [5], including one with individuals, protection of documents, as well as their effective authentication, practically constitutes a security requirement for a company, regardless of its size or ownership [6]. The veracity of information provided in the form of a printed document is critical for various sectors of the economy, especially in cases where it is the only basis for an important business decision to be made on. Compromised data integrity of a printed document caused by removing some information, falsifying the document, or by an error of an expert authenticating the protected document manually are only a part of problems that both business environment and state-owned enterprises encounter [7]. The false information used to make a respective decision leads to various consequences e.g., loss of reputation or huge losses to a company [8].

Volume and variety of printed documents, significant differences in types of paper on which they are printed, as well as printing equipment, lead to complex management and control issues. The development of a security policy for a company's printed documents can help solve this problem [9]. The policy should be based primarily on automation of the procedures mentioned. Methods of protecting printed documents, and especially the electronic ones of their authentication, in particular, allow significant release of time, human and financial resources of a company.

The analysis of modern document protection tools shows that the most promising technologies in terms of practical implementation of graphic security facilities are those of latent elements, which are electronically based [10]. This method implies forming latent elements at a document pre-press stage. The graphic elements created contain hidden information that can be reproduced only by specialized software a developer is familiar with.

Latent images are a large group of images that have one common property: change in visibility of image elements in the event of changes in observation conditions. They are formed by applying a variety of sophisticated and precise processes, including creation of some elements in latent images. Depending on an angle of light, one can see different ornamental patterns, colors, and images. A complex structure and infinite possibilities of using latent elements form reliable protection against forgery. Latent images can be formed in various ways: by means of holography, using the phenomenon of polarization, special inks, and coverings. There exists a method of creating latent elements at the pre-press stage while forming graphical protection. Forming the latent images based on the selection of high line resolution is one of the graphical ways of printed document protection.

2. State-of-the-Art

The term "latent image" [11] denotes a developed printing technique based on the features of offset printing from engraved plates, on the basis of which it is possible to create "hidden" and "transient" images, and the optical principles based on which they work.

In [12], new information technologies that build a presentation of an original image in a new ICaS color space are proposed. The paper suggests equation solutions for color image synthesis, which have optimized the use of latent images. Specialized software for latent image processing has been developed. The software is based on a new color separation information model.

Printed documents, including certificates, forms, diplomas, and important letters, are currently in circulation. Therefore, there remains a need to protect this type of documents from forgery. In [13], an application in Python determines whether a document is original or fake. Based on the test results, it has been concluded that this application meets all the requirements and designs, and the application has predicted true physical documents that protect against fake attacks.

In [14], it is proposed to construct hidden images by printing them on opaque materials in visible light, i.e., inkjet printing with transparent paints or epoxy, without dimming brightness. This increases the rigidity of the system.

In [15], it is suggested to print prints on matte-coated paper and a measured contact angle, solid ink density, color strength, and print gloss. The color characteristics (ΔEab *) of ink have been calculated with regard to standard inks and an influence of the transparent and opaque white on the rheological and printing properties of ink. The perfect color ratio of the clear and opaque white to ink has been proven in terms of printing quality. Recommendations for their application are provided.

It is well-known that processing a printed document with special substances for the construction of hidden prints can effectively protect printed documents [16]. This study has been initiated to determine an impact of hidden prints on printed documents. Four different variables were manipulated and evaluated during the testing process. The results can be necessary for better protection for hidden printing.

Anti-counterfeiting technology is widely used in many fields, especially in the printing industry for protection for banknotes and security documents. In [17], a method of counterfeiting by constructing a different angle of screening is presented and an implementation procedure is described. Thus, a document that is printed is offset by the ordered halftone method with a 0° and 45° angle, respectively. A binary image that contains hidden information is generated using a mask. Finally, a hidden image is generated by combining two halftone images with different shielding angles. The experimental result shows that the proposed method can generate the desired hidden image better.

The purpose of this article is to develop a method of establishing originality of printed documents and their counterfeiting. Printed documents were printed offset and the counterfeits were made on a

photocopier. To enhance security, the latent elements changing their characteristics when copying are applied to a document. To improve the reliability of the proposed method, the latent security elements were printed on standard, commonly used, paper samples for printing documents. The research method is based on an electronic pixel comparison between the original and the fakes.

The main contributions of this paper can be summarized as follows:

(1) a method of protection for printed documents by applying latent elements and fractal grids has been developed;
(2) the effective procedure of document electronic identification based on the authors' investigation of the significant difference between the peak signal-to-noise ratio (PSNR) values of the original and the copy has been developed;
(3) a new method for the formation of protective latent elements based on the construction of fine lines which can be printed with high quality by an offset printing machine, cannot be reproduced, or are reproduced with great deviation has been developed;
(4) an experimental study of reproducing latent elements on 15 different paper samples, as well as on their copies, has been performed.

3. Materials and Methods

3.1. Mathematical Foundations for the Construction of Thin Security Elements in the Printed Manner

An analysis of minimum line thickness that can be reproduced by traditional offset printing and office equipment of electrophotography printing that prints copies has been conducted. The quality of printing is evaluated by optical density, image sharpness, uniformity of ink distribution on a print, and feathering, which can be determined using a spectrophotometer. The optical density D [18] is determined by the logarithm of the inverse value of reflection and is expressed as follows:

$$D = \log_{10} \frac{1}{R}, \tag{1}$$

where R stands for the reflection determined by the ratio of a luminous flux reflected by a surface to a luminous flux reflected by a white clean surface.

When ink is transferred from a printing machine onto a sheet of paper, the ink feathers, i.e., the area of typographical elements increases, which is calculated by the Sheberstov-Murray-Davis formula [19]:

$$\Delta S = \frac{1 - 10^{-D_p}}{1 - 10^{-D_{pl}}}, \tag{2}$$

where D_p is the optical density of a raster field; D_{pl} is the optical density of a printing surface; and ΔS is an area of typographical element.

However, when measuring a relative size of a raster dot on some materials, it is necessary to consider optical light feathering, therefore, the Yule-Nielsen correction coefficient is introduced into the Sheberstov-Murray-Davis formula [20]:

$$\Delta S = \frac{1 - 10^{-D_p}}{1 - 10^{-D_{pl}}} - \frac{1 - 10^{-D_{p/N}}}{1 - 10^{-D_{pl/N}}}, \tag{3}$$

where N is Yule-Nielsen's light scattering coefficient which changes from 1 to 4.

The Yule-Nielsen formula shows that the higher paper quality is, the less ink penetrates inside, and consequently, the lower the degree of ink feathering is. However, the larger raster lines are, the closer lines and the greater blur are.

D_p and S are obtained as a result of spectrophotometric measurements, and the relative size of a raster dot is presented in Table 1.

Table 1. The results of densitometry measurements.

№	Paper Sample	Optical Density of a Raster Field, D_p	Feathering of Printed Elements, S	Relative Size of a Raster Dot
1	CANSON tracing paper	0.77	88	80
2	4CC silk fiber paper	0.71	60	96
3	4CC calandered paper	0.74	30	90
4	Sirio Pearl Oyster Shell	0.6	14	84
5	Optima Self-adhesive Standard	0.8	25	99
6	Optima Self-adhesive	0.1	29	102
7	Folia Fotokarton, 300 g/m^2.	0.2	100	82
8	Embossed card paper (Russia)	0.2	33	98
9	Canson tracing paper	0.16	100	99
10	Fedrigoni Constellation Jade Riccio	0.32	47	87
11	Constellation Ivory	0.25	100	91.9
12	Art-Tech Gold, two-side coated paper	0.3	90	96
13	Stardream peridot	0.2	88	98
14	Canon Plus Glossy II PP-201	0.16	88	95
15	Star Dream Moon Stoo	0.15	77	100

3.2. Comparison of the Quality of Thin Lines Printed by Offset and Electrophotography

Let us consider how an image is formed on copies using office equipment, in particular printers and copiers [21]. To obtain a copy, charged particles of toner are transferred onto a sheet of paper. An image formed by toner is transferred onto a sheet of paper and fixed as a result of the toner sticking to paper under heating [22].

The toner consists of fine elementary particles with an average radius of 0.1–0.2 μm. The thickness of the finest lines, which can be created based on electrophotography, is 40 μm [23] (see Figure 1, curve 1). Nonetheless, when analyzing the formation of wider lines, we observe an edge effect on the copy obtained, which is shown in Figure 1. (curve 2). In this Figure, we can see that there are no gaps between the lines, as opposed to the thin lines, but there is a valley of a curve as shown in the shaded area.

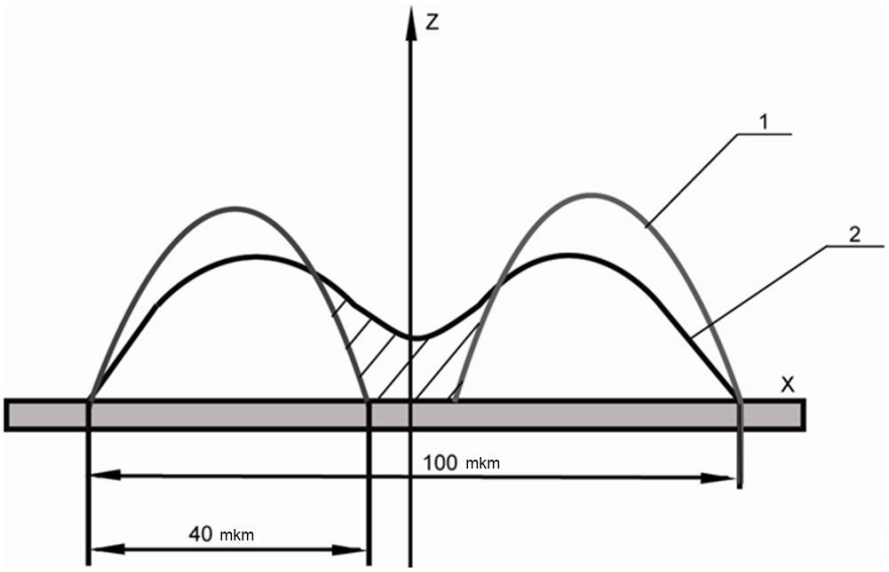

Figure 1. Distribution of toner's particles in making a copy on a copy machine, where Z represents the number of toner's particles, X stands for (current value) thickness of the line.

The designed method of protection will be based on the creation of fine lines, which are well printed by an offset printing machine and cannot be reproduced or can be reproduced with some deviations by a copy machine, in Figure 1 (curve 2), a 100-µm edge-effect line is represented. Consequently, toner is accumulated in the middle of the line and the line splitting is not observed. Therefore, latent elements can hardly be reproduced using a copy machine, since a slight thickness of lines and a permanent change in the curvature of each line pose obstacles to their reproduction.

From the analysis conducted it can be inferred that for a latent element to be protected effectively, line thickness should be ranged between 40 and 90 µm. If the line thickness exceeds 90 µm, a copy machine reproduces latent elements without defects, and without providing the protection needed. If a line is thinner than 40 micrometers, an offset machine reproduces lines on the selected samples of paper.

After comparing the values of minimum lines reproducibility, let us move on to the development of a method of protection for the latent elements used for printing.

3.3. A Method of Protecting Printed Documents Based on the Construction of Latent Elements and Fractal Nets

The suggested technology of forming a latent element is effective by using high lines per inch (lpi) that are greater than 200 lpi, and printing a document with a 3000–4000-dpi resolution [24]. In this case, this method ensures reliable protection of the document against being copied. During an attempt of duplicating, a raster original structure will not be reproduced with high quality. Besides, with a template being overlaid, a hidden image will not be reproduced and a moire effect will be observed [22].

By means of the developed software, the information needed is combined with security features, and an electronic file in PDF format with protected information is created, which allows printing with the maximum quality that this output device has. Thus, it is possible to realize printing the protected information with a resolution of 3000 dpi and above. The limitation of printing resolution is created only by capabilities of an output device for printing [25]. The flowchart of the information technology for protection for printed documents is presented in Figure 2.

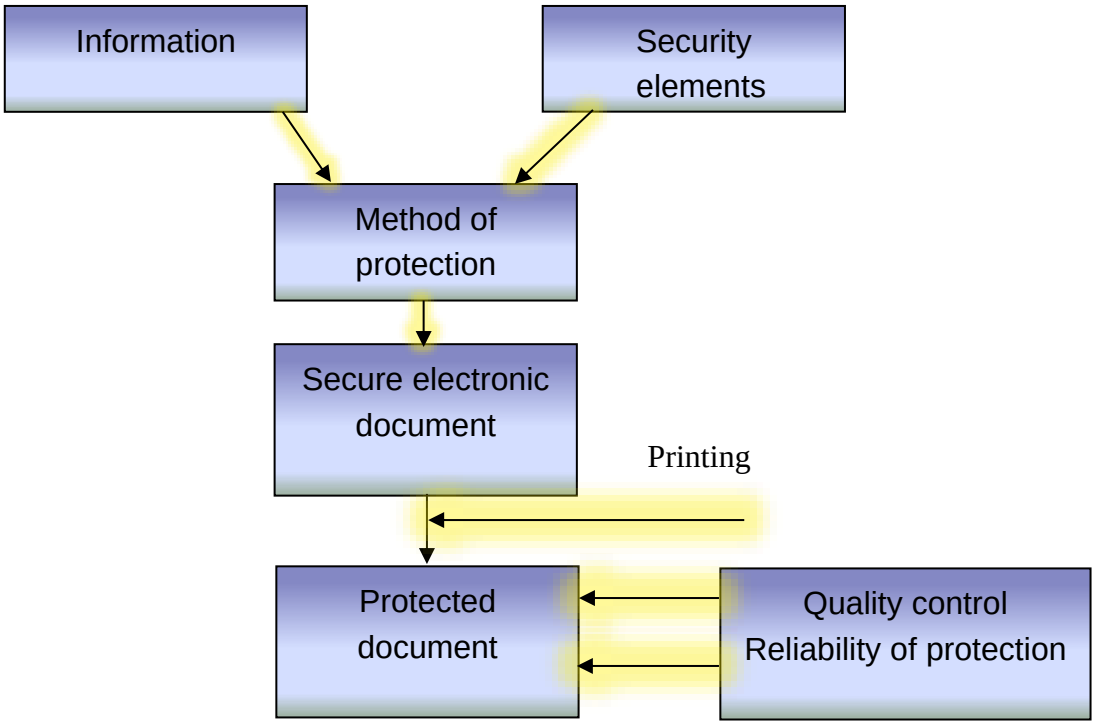

Figure 2. Flowchart of information technology for protection for printed documents.

The method of creating latent elements consists in the following steps. A raster field with parameters of 60–70% of the maximum shades of gray is created. The raster field is created in the vector format in the way that the vector field of a grey level at 60–70% of the maximum is set, as well as a transparent one of the same thickness near it. A necessary inscription is created, e.g., "ORIGINAL", which is shifted to a transparent field. A new raster field being the grey level at 15–20% of the maximum is created. Similarly to the previous raster field, dark and transparent fields, and an inscription are created. The fields are overlapped afterward, displacing the width of one field in a way that prevents any empty space. The latency of the inscription will be observed due to a light inscription being against the dark background and vice versa. If such a design is printed offset, it has very good readability.

For protection to be increased, fractal grids are overlapped between the margins which are built with the finest lines that an original printing machine can reproduce, which represents the way latent security features are created. When copying, the properties of the layers are violated because of being overlapped, and the overlapped fractal grids much more impair the quality of the document. A flowchart of the latent element construction method is shown in Figure 3.

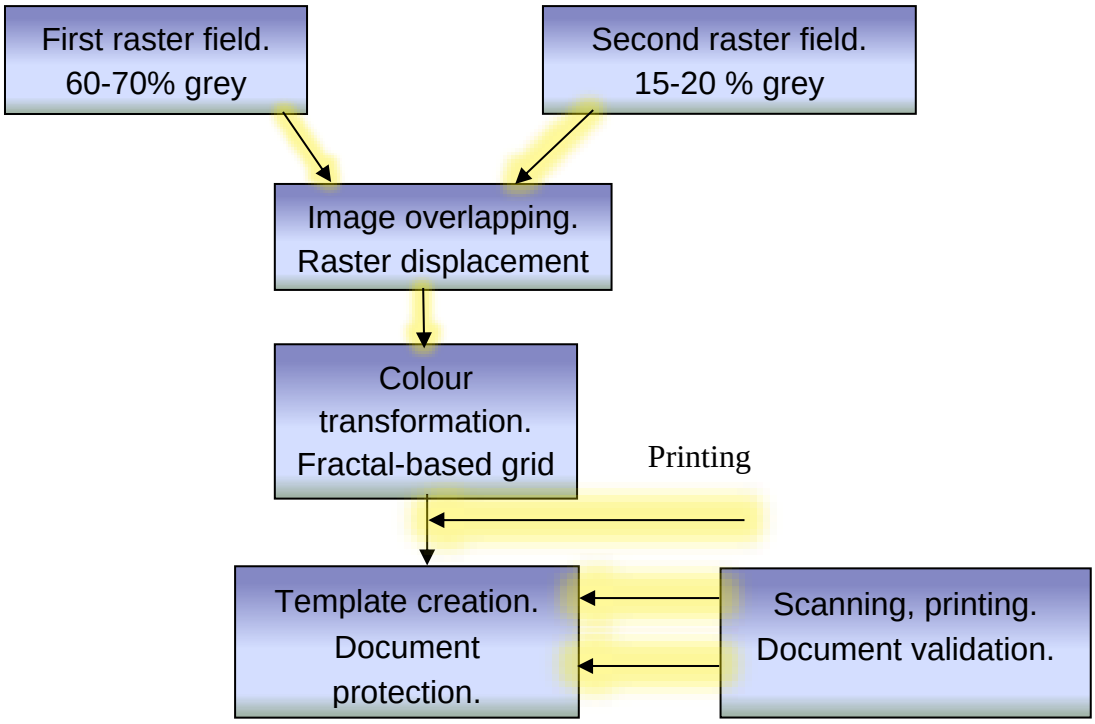

Figure 3. Flowchart of a method of constructing latent elements.

The main idea of the protection method is that for a security element, the displacement of a part of lines is half of the raster line step value [26].

To increase the security effect, a security element is laid on by a grid of geometrical fractals [27].

The class of geometrical fractals is formed as a sequence of specific geometric operations. The realization of such fractals starts with two shapes—an initiator and a generator. The latter is an oriented polygonal line consisting of N equal segments with a length, r. Let the geometrical fractal named as the Minkovskyi fractal be a basis for a security element [28]:

$$D = \frac{\log N}{\log(1/r)}, \tag{4}$$

where D is the dimension of the fractal; $1/r$ is the similarity ratio; and N is the number of iterations.

The method of protection lies in that graphical elements of a protection gird are formed in the vector format. Further, they are copied. Then, by means of a recursive procedure, we form a

fractal-based grid. Fractals are formed by a recursive procedure, where every single graphical element is a generator, which sets the value of a security element, which should be as minimal as possible to be reproduced in the printed form. Then, an initiator fills the grid surface.

The formation of the grid starts with setting of fractal parameters. Based on the fractal formed, we can create a large number of fractal girds variants changing a scale, rotation, and increasing or decreasing the number of iterations. The fractal background grids are difficult to reproduce because it is necessary to use an algorithm for constructing the selected type of fractal. A document to be protected can contain text, graphics or tabular information that is placed onto the upper level. At the lower level, the fractal background grid is generated with certain controlled parameters, i.e., the fragmentation degree of security element values.

Any graphical filling of a document consists of single graphical elements, the values of which are set by fractal parameters. The thickness of single graphical elements is set with minimum parameters, which are difficult to be reproduced by office copying equipment. The color of single graphical elements is set in a light tonal range or with adding special inks in the percentage ratio to the basic ink, which provides the reliability and effectiveness of protection. The method of document protection involves the vector technology of grid formation with the use of the software code, which is completely adapted to the information output on printing equipment that makes it possible to increase the effectiveness of protection and generates files in a pdf file.

4. Modeling and Discussion

The suggested technology of forming a latent element uses high lines per inch that are greater than 200 lpi and a printed document with a 3000–4000-dpi resolution. The developed method has been implemented with the line thickness of 40–90 μm which is well-printed by offset printing. The first raster field for creating latent elements used a grey level at 60–70% of the maximum. The second raster field used the grey level at 15–20% of the maximum.

The Minkowski fractal parameters (4) are the following: the dimension of a fractal is 1.5; the similarity ratio is $\frac{1}{4}$; the number of iterations is 8.

New paper samples with different characteristics appear on the market annually. The authors have used 15 typical paper samples and their characteristics based on the densitometry measurements described in the next section. The original was printed offset and the copy was made on a Xerox machine. Other widespread samples can be simply evaluated using the proposed methodology.

4.1. Experimental Investigations of the Characteristics of Different Paper Samples

In our investigation we used 15 different paper samples:

1. **CANSON tracing paper, 90 g/m^2, France.** Translucent tracing paper is based on cellulose and synthetic resins. It is recommended for the use in laser printers to print out document layouts and in polygraphy for offset, varnishing, embossing, and lamination.
2. **4CC silk fiber paper.** High-grade paper for digital document printing produced by the Finnish company Stora Enso. This brand of paper is presented in the following types: calendered, uncoated, high-glossy, artistic, and silk matte paper. The weights of all types of paper are ranged from 90 to 270 g/m^2. 4CC paper is distinguished by its smooth surface.
3. **4CC calendered paper.** High-glossy two-side coated paper is specially designed for printing highly artistic images. In terms of parameters, the paper features an optimal combination of high porosity, opacity, and smoothness that is achieved by using a particular technology of paper manufacturing and chalking. This also ensures the exceptional stability of characteristics for this type of paper.
4. **Sirio Pearl Oyster Shell.** Sirio Pearl paper is suitable for all major printing methods: letterpress, offset, thermal and screen printing.

5. **Optima Adhesive Standard.** Optima Self-adhesive is rough 70 g/m^2 paper for inkjet and laser printers and copiers. A special heat-resistant glue and base paper ensures correct and uninterrupted passage through different printers.
6. **Optima Adhesive.** Self-adhesive optima label is rough 100 g/m^2 paper for inkjet and laser printers.
7. **Folia Fotokarton.** Design paper Fotokarton (TM "Folia", Germany) is high-quality two-side coated, smooth, matte, full-color, and full dense, 300 g/m^2 cardboard.
8. **Embossed aquarelle card paper, 200 g/m^2 (Russia).** Embossed card paper is used for offset, screen printing, colorless embossing, and foil stamping. This type of paper is suitable for cutting, folding, gluing and is distinguished by high whiteness.
9. **Canson tracing paper, 200 g/m^2.** This is a type of transparent calendered paper for copying drawings with Indian inks and obtaining blueprints. The effect of transparency is achieved by using finely ground cellulose and various resins. The matte tracing paper for electrographic devices is used for laser printers to print out layouts, which are then copied to produce printing forms.
10. **Fedrigoni Constellation Jade Riccio.** White uncoated paper and cardboard with a variety of one- and two-side embossing patterns, and high strength. This paper can be used for offset, laser and inkjet printing.
11. **Constellation Ivory/Snow.** Manufacturer: Fedrigoni. Hoarfrost. White and beige uncoated paper with a variety of one- and two-side embossing patterns and high strength is made from bleached pulp.
12. **Two-side coated paper. Art-Tech—Gold East Paper (China).** The Art-Tech matte coated paper produced by Gold East Paper (Jiangsu) features a blue-white shade with a high degree of whiteness. Despite the paper being matte, a gloss of the surface does not exceed 35%. It is distinguished by high strength, and excellent printing performance, low content of carbon, and recyclability.
13. **Stardream Peridot.** Stardream peridot is design 120–285g/m^2 cardboard that gives a grey-green shimmer and features by a smooth metalized texture.
14. **Canon Plus Glossy II PP-201.** Superior glossy photo paper is a perfect choice for high-quality output with a glossy finish. The advantages of this brand of paper are an exceptional glossy surface, superior quality photo printing, real photo look with saturated blacks and live colors.
15. **Stardream Moon Stoo.** Tinted paper with a pearlescent and metallic coating. The paperweight of 285 g/m^2 perfectly suited for leaflets, folders, covers, bags, and another packaging.

For these paper samples, we have measured the densitometric parameters of the optical density of the raster field, D_p is the percentage of raster dot feathering, the relative size of a raster dot, S. The results are shown in Table 1.

When analyzing the data presented in Table 1, we can see that the highest degree of the printed elements feathering was observed in paper samples № 7, 9, 11, while paper samples № 2, 5, 6, 8, 9, 12, 13 and 15 demonstrated the largest relative size of a raster dot. The data also show that the paper sample № 9 was not recommended for using since the values of feathering of printed elements and relative size of a raster dot were very high. This suggests that the copy on this paper sample will be reproduced with the same wide lines as on the original, which reduces the likelihood of correct identification of the original and the copy. The most appropriate paper samples were № 1, 3, 4, and 10 with the minimum level of printed element feathering, S, and the minimum relative size of a raster dot. Formulas (2) and (3) can be used to calculate an optical density of the raster field and thus obtain reliable data for the security elements formation.

4.2. Simulation of Security Latent Elements on Printed Documents

A security element (Figure 4) was based on two uniform raster fields formed by a linear raster with similar lines per inch and relative area of raster elements. Approximately grey level at 60–70% of the maximum for the raster lines in the first raster field and grey level at 15–20% of the maximum in

the second raster field coincided, by size, with a basic guilloche element depicting dark areas in the first raster field and light areas in the second one (Figure 5).

Figure 4. Hidden inscription "ОРИГІНАЛ" formed by the displacement of raster lines in the first field.

Figure 5. Hidden inscription "ОРИГІНАЛ" formed by the displacement of raster lines in the second raster field.

An image of a future security element was placed onto the raster fields formed in this manner. This element was cut out, and the space formed was filled with the same raster displaced by a half step of the raster lines. The basic element was recolored afterward to form a fractal mask. This required white elements to remain white and dark elements to remain transparent. A fractal mask for hiding information was formed over the second raster field. The hidden information could be checked using an original template of a pellicle-detector which provided the possibility of document validation.

To form a security element, images of hidden information, e.g., the inscription "ОРИГІНАЛ", are placed on the first and second raster fields (Figures 4 and 5).

To verify the authenticity of the document for observation of the latent element regarding security features, a template was used (Figure 6) containing a grid with a linear raster whose frequency was equal to raster lines per inch of the latent image with the relative area of raster elements amounting to grey level at 40–45% of the maximum.

Figure 6. Template with the relative area of raster elements of 40–45%.

The created latent element is shown in Figure 7, and its enlarged fragment is given in Figure 8. Comparison between the document and its copy shows a difference in the raster lines per inch, therefore, the template overlapping led to strong visible moire and to poor readability of the latent image (up to illegibility with strong differences of lines per inch).

Figure 7. Creating a security element.

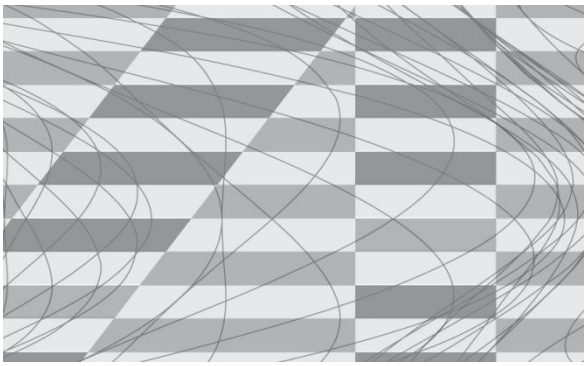

Figure 8. Enlarged fragment of a security element.

Figure 9 demonstrates a forged security element, where the original was copied using electrophotography. The examination of the document detected a moire effect.

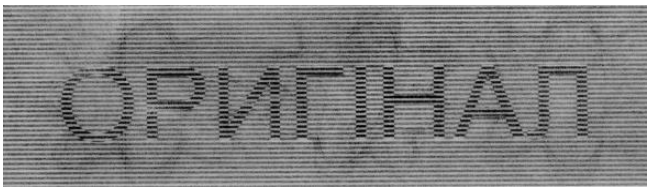

Figure 9. Indicators of forgery, strong moire.

This method of security element formation makes it possible to examine the document authenticity as follows: a template printed on a transparent film, as shown in Figure 5, was laid on a security element, which is shown in Figure 6. With the template being shifted by a half step, the inscription "ОРИГІНАЛ" was seen in a light tone, and with the template being shifted downwards, the inscription changed into a dark tone. Moreover, it can be seen that the tone changed sharply. If an authentic document was duplicated, narrow gaps between the lines lost their sharp contours (see Figure 4) because they were filled with toner powder. Thus, it was impossible to see the inscription in light-dark tones. This is demonstrated in Figure 9. This way of protection refers to visual and does not require devices to detect a forgery. It is advisable that line thickness be selected from the calculated values of printing elements feathering and the relative size of a raster point.

4.3. Electronic Authenticity of Printed Documents Protected According to the Developed Method

The methodology of detecting a computer forgery by means of computer facilities developed by the authors is based on a complete pixel-by-pixel comparison between original images and their copies [29]. To implement the electronic method of authentication of printed documents, it is necessary to calculate PSNR's values for both the original-to-original comparison and the original-to-copy comparison. This allows one to set certain PSNR's value limits for detecting the original and the copy electronically.

All further results of the experimental study have been obtained with the values of fixed parameters of the paper samples, which are described in Section 4.1.

The experiment was carried out in the following way. A security element of the image was developed using the method of thin graphics. This element was printed out by an offset printing machine. Then, the prints obtained from the films were printed on 15 paper samples, densitometric characteristics of which are shown in Table 1. The original prints were copied on 80 g/m^2 printing paper and called a forgery.

The originals and their copies were digitalized. The authenticity was determined by the PSNR coefficient value. The greater value of the coefficient was obtained, the more pixel coincidences were

found; and the less value of the coefficient was obtained, the more differences between the two pixels were observed. The authenticity of printed documents was established using the method of complete pixel-by-pixel comparison between originals (original-to-original comparison) and their copies (original-to-copy comparison) based on the software developed by the authors. It has been done to determine the upper and lower PSNR's values of the original and its copy for electronic authentication procedures of printed documents. The results of this experiment are presented in Table 2.

Table 2. The results of using the method of a complete pixel-by-pixel comparison between the security element of the original-to-original and original-to-copy, printed on offset machine.

Number of Paper Sample	Original-to-Original PSNR	Original-to-Copy PSNR
1	217.95	14.92
2	210.45	13.48
3	220.57	14.92
4	213.48	13.45
5	218.54	12.45
6	217.53	14.04
7	215.23	13.61
8	218.78	14.04
9	219.36	16.63
10	218.45	12.45
11	217.22	13.68
12	219.28	13.06
13	217.13	13.62
14	215.53	13.06
15	218.53	12.51

In Table 2, the difference in PSNR values between originals (original-to-original comparison) and copies (original-to-copy comparison) for all 15 paper samples being investigated is clearly shown. It is obvious that printing on different paper samples differed particularly because of the different paper structure described in Section 4.1. In addition, it was influenced by other characteristics such as the smoothness and thickness of the ink reproduction by the offset printing machine, changing the humidity, temperature, speed of the offset printing machine, changing the pressure, etc. Therefore, the PSNR values varied within a certain range. However, as can be seen from Table 2, the PSNR values within each of the two experiments (original-to-original comparison and original-to-copy comparison) differed slightly, while the values between the two experiments differed much more fundamentally (columns 2 and 3 of Table 2).

In particular, PSNR values for originals ranged from 213.48 to 220.57 dB, and for copies from 12.45 to 16.63 dB, respectively. This very difference being highly significant made it possible to distinguish the original from the copy electronically, since it was difficult to implement this under visual observation. In this case, the outcome of the proposed method for electronic authentication of printed documents is obvious.

In practice, there may arise a situation where the original printed document is lost and its duplicate is required. It can be printed on a different type of paper. Since different paper samples have different whiteness, weight, whitewash, smoothness, texture and are printed with different degrees of ink layer fixation, the problem of its authentication by the proposed method is likely to occur.

To achieve this, an experiment to compare the original document with its duplicate (original-to-duplicate) printed on a different type of paper by offset printing has been performed. In Table 3, all possible comparison variants for the 15 paper samples being investigated are presented.

The outcome of the experiment to compare the original document with its duplicate (original-to-duplicate) printed on different paper samples suggests slightly different results. In Table 3, the results of a pixel-by-pixel comparison between the original and the duplicate are shown to range

from 12.32 to 20.49 dB. In the vast majority of samples, in comparing the original with the duplicate (see Table 3) and the original with the copy (see Table 2), the PSNR values in the latter case were lower. Therefore, printing companies should take the printing and the interchangeability of different paper samples into account.

Table 3. The results of using the method of a complete pixel-by-pixel comparison between the original and duplicate, printed on offset machine on different paper samples.

Original-to-Duplicate Comparison №→№	Comparison Result, dB	Original-to-Duplicate Comparison №→№	Comparison Result, dB	Original-to-Duplicate Comparison №→№	Comparison Result, dB
1→2	18.11	3→12	14,27	7→9	17.50
1→3	17.93	3→13	15.26	7→10	12.76
1→4	18.52	3→14	14.69	7→11	14.90
1→5	18.92	3→15	18.25	7→12	14.67
1→6	19.69	4→5	17.89	7→13	14.75
1→7	16.97	4→6	18.09	7→14	15.37
1→8	16.98	4→7	16.98	7→15	17.40
1→9	16.84	4→8	17.20	8→9	16.88
1→10	13.74	4→9	15.54	8→10	14.62
1→11	15.63	4→10	12.92	8→11	15.81
1→12	17.32	4→11	14.95	8→12	16.48
1→13	17.23	4→12	14.83	8→13	14.72
1→14	16.46	4→13	14.38	8→14	15.18
1→15	18.21	4→14	13.71	8→15	18.61
2→3	20.21	4→15	19.96	9→10	14.03
2→4	18.65	5→6	20.49	9→11	16.50
2→5	18.50	5→7	18.17	9→12	16.43
2→6	18.09	5→8	18.61	9→13	15.54
2→7	19.56	5→9	15.54	9→14	15.58
2→8	18.09	5→10	12.89	9→15	16.43
2→9	18.61	5→11	15.62	10→11	12.55
2→10	12.50	5→12	14,99	10→12	12,43
2→11	14.95	5→13	15.85	10→13	19.56
2→12	14,57	5→14	14.99	10→14	12.32
2→13	12.48	5→15	16.97	10→15	15.99
2→14	14.45	6→7	18.17	11→12	15.27
2→15	17.39	6→8	18.61	11→13	19.75
3→4	19.85	6→9	15.54	11→14	14.86
3→5	16.88	6→10	12.87	11→15	14.74
3→6	19.65	6→11	15.58	12→13	18.71
3→7	19.65	6→12	14.99	12→14	14.96
3→8	17.89	6→13	14.91	12→15	15.62
3→9	14.83	6→14	15.28	13→14	15.01
3→10	12.38	6→15	17.98	13→15	15.85
3→11	14.31	7→8	17.53	14→15	14.61

5. Conclusions

The latent elements have been created on the printed documents produced by offset and by a copy machine (Xerox). The influence of the optical density of a raster field, printed element feathering, the relative size of a raster dot on the quality of printing obtained by offset and by electrography methods has been investigated. The quality indicators of the latent security elements printed by offset and of their copies on 15 paper samples of the famous brands currently popular on the market have been investigated.

The authors have developed a method for determining the authenticity of a printed document based on a pixel-by-pixel comparison of an original printed document and its copy. The peak signal-to-noise ratio coefficient (PSNR) has been chosen as a criterion for the comparison.

The outcome of the developed method of electronic authentication of documents printed on one type of paper suggests very good results. Considered a comparison between originals and copies printed on different types of paper under equal terms, those paper samples for printing that ensure the highest PSNR values are recommended for selection.

The main advantage of the developed method is the possibility of conducting an electronic rapid assessment for the authentication of printed documents. In case a more detailed analysis is required, e.g., one for the authentication of a duplicate printed offset on non-original paper samples, the printing parameters based on densitometric measurements using specialized equipment will be investigated.

Author Contributions: Conceptualization, M.N.; methodology, M.N.; software, I.I.; validation, I.I., N.L. and M.G.m.; formal analysis, N.L. and M.G.m.; investigation, M.M.; writing—original draft preparation, M.N.; writing—review and editing, I.I.; supervision, M.G.m. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Acknowledgments: The authors thank the reviewers for the relevant comments that helped to present the paper better.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Lim, K.; Islam, T.; Kim, H.; Joung, J. A Sybil Attack Detection Scheme based on ADAS Sensors for Vehicular Networks. In Proceedings of the 2020 17th IEEE Annual Consumer Communications Networking Conference (CCNC), Las Vegas, NV, USA, 10–13 January 2020; pp. 1–4.
2. Lim, K.; Tuladhar, K.M.; Kim, H. Detecting Location Spoofing using ADAS sensors in VANETs. In Proceedings of the 2019 16th IEEE Annual Consumer Communications Networking Conference (CCNC), Las Vegas, NV, USA, 11–14 January 2019; pp. 1–4.
3. Huang, K.; Tian, X.; Yu, H.; Yu, M.; Yin, A. A High Capacity Watermarking Technique for the Printed Document. *Electronics* **2019**, *8*, 1403. [CrossRef]
4. Kaczor, S.; Kryvinska, N. It is all about services-fundamentals, drivers, and business models. *J. Serv. Sci. Res.* **2013**, *5*, 125–154. [CrossRef]
5. De Angelis, F.L.; Di Marzo Serugendo, G. SmartContent—Self-Protected Context-Aware Active Documents for Mobile Environments. *Electronics* **2017**, *6*, 17. [CrossRef]
6. Kryvinska, N. Building consistent formal specification for the service enterprise agility foundation. *J. Serv. Sci. Res.* **2012**, *4*, 235–269. [CrossRef]
7. Shang, S.; Memon, N.; Kong, X. Detecting documents forged by printing and copying. *EURASIP J. Adv. Signal Process.* **2014**, *2014*, 140. [CrossRef]
8. Zaby, S.; Pohl, M. The Management of Reputational Risks in Banks: Findings from Germany and Switzerland. *SAGE Open* **2019**, *9*. [CrossRef]
9. Vacca, J.R. *Computer and Information Security Handbook*; Morgan Kaufmann: Burlington, MA, USA, 2017; ISBN 978-0-12-803929-8.
10. Fedoseev, V.; Mishkina, E. Selection of Relevant Filter Responses for Extraction of Latent Images from Protected Documents. In *Computer Vision and Graphics*; Springer: Berlin/Heidelberg, Germany, 2016; pp. 523–531.
11. Huber, R.A. The Latent Image and its Role in Document Security. *Can. Soc. Forensic Sci. J.* **1977**, *10*, 127–134. [CrossRef]
12. Shovheniuk, M.; Kovalskiy, B.; Semeniv, M.; Semeniv, V.; Zanko, N. Information Technology of Digital Images Processing with Saving of Material Resources. In Proceedings of the ICTERI, Kherson, Ukraine, 12–15 June 2019.

13. Wibowo Putro, P.A.; Luthfi, M. An Authentic and Secure Printed Document from Forgery Attack by Combining Perceptual Hash and Optical Character Recognition. In Proceedings of the 2019 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS), Jakarta, Indonesia, 14–15 October 2019; pp. 157–162.
14. Blumenthal, T.; Meruga, J.; Stanley May, P.; Kellar, J.; Cross, W.; Ankireddy, K.; Vunnam, S.; Luu, Q.N. Patterned direct-write and screen-printing of NIR-to-visible upconverting inks for security applications. *Nanotechnology* **2012**, *23*, 185305. [CrossRef] [PubMed]
15. Aydemir, C.; Yenidoğan, S.; Karademir, A.; Arman, E. Effects of color mixing components on offset ink and printing process. *Mater. Manuf. Process.* **2017**, *32*, 1310–1315. [CrossRef]
16. Moore, D.S. The Electrostatic Detection Apparatus (ESDA) and Its Effects on Latent Prints on Paper. *J. Forensic Sci.* **1988**, *33*, 357–377. [CrossRef]
17. Duan, J.; Zhang, E. An anti-counterfeiting method for printed image by digital halftoning method. In Proceedings of the 2012 5th International Congress on Image and Signal Processing, Chongqing, China, 16–18 October 2012; pp. 562–566.
18. Johnston, J.; Fauber, T.L. *Essentials of Radiographic Physics and Imaging*, 3rd ed.; Elsevier: Amsterdam, The Netherlands, 2015; ISBN 978-0-323-56668-1. Available online: https://www.elsevierhealth.com.au/essentials-of-radiographic-physics-and-imaging-9780323566681.html (accessed on 16 February 2020).
19. Serafini, F.; Clausen, J. Typography as Semiotic Resource. *J. Vis. Lit.* **2012**, *31*, 1–16. [CrossRef]
20. Kibirkstis, E.; Havenko, S.; Gegeckienė, L.; Khadzhynova, S.; Kadyliak, M. Influence of Structure and Physical-Mechanical Characteristics of Threads on the Strength of Binding the Books. *Mechanics* **2019**, *25*, 313–319. [CrossRef]
21. Amidror, I. New print-based security strategy for the protection of valuable documents and products using moire intensity profiles. In *Optical Security and Counterfeit Deterrence Techniques IV*; International Society for Optics and Photonics: Washington, DC, USA, 2002; Volume 4677, pp. 89–100.
22. Medykovskyy, M.; Lipinski, P.; Troyan, O.; Nazarkevych, M. Methods of protection document formed from latent element located by fractals. In Proceedings of the 2015 Xth International Scientific and Technical Conference "Computer Sciences and Information Technologies" (CSIT), Lviv, Ukraine, 14–17 September 2015; pp. 70–72.
23. Dronyuk, I.; Nazarkevych, M. Development of printed packaging protection technology by means of background nets. In Proceedings of the 2009 10th International Conference—The Experience of Designing and Application of CAD Systems in Microelectronics, Lviv-Polyana, Ukraine, 24–28 February 2009.
24. Kipphan, H. Print Media and Electronic Media. In *Handbook of Print Media: Technologies and Production Methods*; Kipphan, H., Ed.; Springer: Berlin/Heidelberg, Germany, 2001; pp. 1005–1026. ISBN 978-3-540-29900-4.
25. Rashkevych, Y.; Peleshko, D.; Vynokurova, O.; Izonin, I.; Lotoshynska, N. Single-frame image super-resolution based on singular square matrix operator. In Proceedings of the 2017 IEEE First Ukraine Conference on Electrical and Computer Engineering (UKRCON), Kiev, Ukraine, 29 May–2 June 2017; pp. 944–948.
26. Jindal, S.; Sivia, J.S.; Bindra, H.S. Defected Ground Based Fractal Antenna for S and C Band Applications. *Wirel. Pers. Commun.* **2020**, *110*, 109–124. [CrossRef]
27. Nazarkevych, M.A.; Dronyuk, I.M.; Troian, O.A. Method of electronic and printed documents protection on the basis of moire effect. *Актуальні ПроблемиЕкономіки* **2016**, *5*, 382–394.
28. Cao, T.N.; Krzysztofik, W.J. Hybrid Minkowski fractal island antenna operating in two bands of GPS satellite system. In Proceedings of the 2016 IEEE International Symposium on Antennas and Propagation (APSURSI), Fajardo, Puerto Rico, 26 June–1 July 2016; pp. 211–212.
29. Ichigaya, A.; Kurozumi, M.; Hara, N.; Nishida, Y.; Nakasu, E. A method of estimating coding PSNR using quantized DCT coefficients. *IEEE Trans. Circuits Syst. Video Technol.* **2006**, *16*, 251–259. [CrossRef]