An Optical/Digital Identification/Verification System based on Digital Watermarking Technology

A. Herrigel[a], S. Voloshynovskiy[b], Z. Hrytskiv[c]
[a]Digital Copyright Technologies, Stauffacher-Strasse 149, CH-8004, Zurich, Switzerland
[b]University of Geneva, Department of Computer Sciences, 24 rue Général Dufour, 1211 Geneva 4, Switzerland
[c]Lviv Polytechnic State University, Department of Radio Engineering, S. Bandery str. 12, 290060, Lviv, Ukraine

ABSTRACT

This paper presents a new approach for the secure integrity verification of driver licenses, passports or other analogue identification documents. The system embeds (detects) the reference number of the identification document with the DCT watermark technology in (from) the owner photo of the identification document holder. Since the watermark technology is resistant against many image distortions such as affine transformations, lossy compression, quantization, dithering and other common image processing operations, the owner photo my even be damaged without any performance decrease in the detection process. During verification the reference number is extracted and compared with the reference number printed in the in the identification document. The approach combines optical and digital image processing techniques. The detection system must be able to scan an analogue driver license or passport, convert the image of this document into a digital representation and then apply the watermark verification algorithm to check the payload of the embedded watermark. If the payload of the watermark is identical with the printed visual reference number of the issuer, the verification was successful and the passport or driver license has not been modified.
This approach constitutes a new class of application for the watermark technology, which was originally targeted for the copyright protection of digital multimedia data.
The presented approach substantially increases the security of the analogue identification documents applied in many European countries.
Keywords: document protection, document owner identification, digital watermarking.

1. INTRODUCTION

Everybody of us has experienced that the community in we are working and living gets more and more mobile. This means that many business or research contacts are no longer only locally based and there is quite a number of contacts we have which are concerned with project partners from different countries. Within the European Community, the European Commission has issued several years ago a new passport systems which provides a unique document structure for the different countries. Along with this mobility comes the need for fast a verification of the identification documents at the custom of some country borders, since more and more people move between different countries for business, research or private purposes. In addition, the mobility is also exploited by unlawful people who are living in one country but violating the law in other countries. These unlawful people exploit the weaknesses of the current passport or other identification systems, since it is not hard for professionals to replace images in stolen passports with new images to get for a period of time a new personal profile which is exploited for unlawful actions.
The schemes for a secure analogue identification system vary from country to country. Many of them are either based on holograms, random phase mask encoding, special high-resolution modulation patterns, and specific techniques exploiting the material physical properties of the identification document paper structure. Although these approaches have provided a specific level of security in the current applications, they can be penetrated by unlawful people. Another problem is that the production process based on this different approaches has to be applied in very confidential environments, since knowing the details of the technology enables always to counterfeight the protection. Finally, the applied approaches do not provide any means to check the integrity of the identification document. If some parts of the document are modified to execute criminal actions with the profile of a lawful person, there is no possibility today to detect these modifications.
The approach presented is based on a new exploitation of the digital watermark technology, which is today applied by different companies for the copyright protection of multimedia data. The system embeds (detects) the reference number of the identification document with the DCT watermark technology in (from) the owner photo of the identification document holder. Since the watermark technology is resistant against many image distortions such as affine transformations, lossy compression, quantization, dithering and other common image processing operations, the owner photo my even be damaged

without any performance decrease in the detection process. During verification the reference number is extracted and compared with the reference number printed in the in the identification document. The approach combines optical and digital image processing techniques. The detection system must be able to scan an analogue driver license or passport, convert the image of this document into a digital representation and then apply the watermark verification algorithm to check the payload of the embedded watermark. If the payload of the watermark is identical with the printed visual reference number of the issuer, the verification was successful and the passport or driver license has not been modified.
The paper first describes the specific features of the watermarking technology for digital still pictures. Then the visual and hidden data verification scheme is presented. The sections concerning the image acquisition system of the document verification device and the image processing system for watermarking describe the essential details of the systems. Due to limited scope of the paper we will present references to recently published research results of a unified approach to address the particularities of human visual system (HVS) during the embedding and detection process.

2. DIGITAL WATERMARKING

Copyright infringements of digital multimedia data can be detected by digital watermarks, embedded by special software programs. Visible and invisible watermarks may be applied for copyright protection. Visible watermarks direct the observer to the fact that the image is copyright protected. The practical usage of this approach is, however, quite limited. The quality of still pictures is substantially changed and the applied protection procedure is not robust, because the visible watermark can be removed by image processing programs such as PhotoShop. In addition, with respect to the target application, a new digital image can be chosen and the text embedded.
The invisible watermark utilizes the inability of the human vision system to perceive small differences in optical data. These slight differences are exploited by special software programs for embedding copyright information directly into the still pictures. Invisible watermarks have the advantage that they can not been easily identified and destroyed.

The Watermarking Process
The copyright protection of a multimedia data set is considered as the process of proving the intellectual property rights with digital evidence data to a court of law against unauthorized reproduction, processing, transformation, or broadcasting. This process is based on a watermarking process WP. We use the expression Cover-Data and Stego-Data. The specific Cover- or Stego-data is a specific type digital multimedia data. The WP embeds or extracts owner authentication data in or out of the multimedia data set. The owner authentication data is embedded such that the commercial usability of the multimedia data set is not affected. For this purpose, a cryptographic key is applied to embed encoded owner authentication data, called the watermark, into the Cover-Data I, resulting in a Stego-Data I*. The watermark data can then be extracted from the stego-data if the correct key is used. The embedding and verification process is illustrated in Fig. 1.
We assume that the WP applied for the embedding is a one-way function [1-3], collision resistant [1-3] and robust, i.e. it is for an unauthorized third party not possible to overwrite or delete this watermark without the cryptographic keying information. WP is based on a symmetric cryptographic system, such as a perceptually adaptive spread spectrum technique.

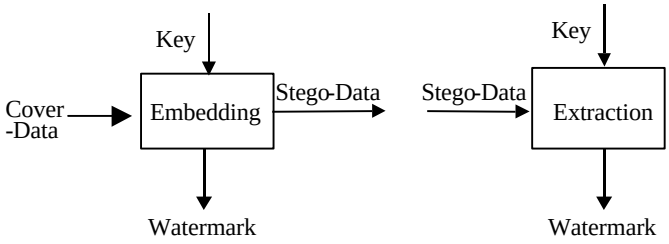

Figure 1. The watermark embedding and verification process.

To embed or extract a watermark, it is necessary to know the exact values of the seed used for the generation of pseudo random sequences used to encode the watermark. Depending on the seed applied for the embedding and verification, we distinguish between a private and a detection watermark. A private watermark is defined as encoded owner authentication data embedded with a cryptographic signature as the seed. A detection watermark is defined as encoded owner authentication data embedded with a cryptographic secret key as the seed.
Digital watermarks in connection with digital copyrights prevent copyright infringements; it can be proven that the picture's use was not authorized.

3. THE VISUAL AND HIDDEN DATA VERIFICATION SCHEME

The proposed document identification/verification system consists of the two principal units (Figure 2), an image aquasition system and image processing system. The input document has two types of data that will be used for the decision making about the content integrity of the examined document. Underlying data is related with the personal identification number (ID) that is assigned to the owner by the corresponding service. The first part of data is visual ID that is directly printed on the document surface and could be detected without special technical means and the second one is the hidden perceptually invisible ID that coincides with the visual ID. In the case of authentic document these IDs should be identical and when the attempt to counterfeight document was done, the document content integrity is damaged that is indicated on the device screen.

The image aquasition system is to convert the analogue color image to the digital form that then will be used for the visual and hidden personal ID extraction in the following image processing system. Based on the comparison of the visual and hidden IDs system will make automatically conclusion about the identity of the given document that is performed in the final unit of the system. The enhanced level of the security in the proposed solution is based on the fact that most of the existed technologies of document protections against counterfeight assume that the unauthorized reproduction of the document requires the knowledge of the used unique technology that is protected by know-how. In the proposed system such an assumption is not more chosen as the basic protection principal because of the high efficiency of the modern copying or printing apparatus or hologram reproduction techniques. The key idea of the watermarking document identification consists in the embedding of the perceptually invisible noise-like signal with high robustness properties against different sort of distortions including compression, addition of the noise or another watermark, quantization, dithering, removal of the part of image, and geometrical transformations such as rotation, scaling, change of aspect ratio,

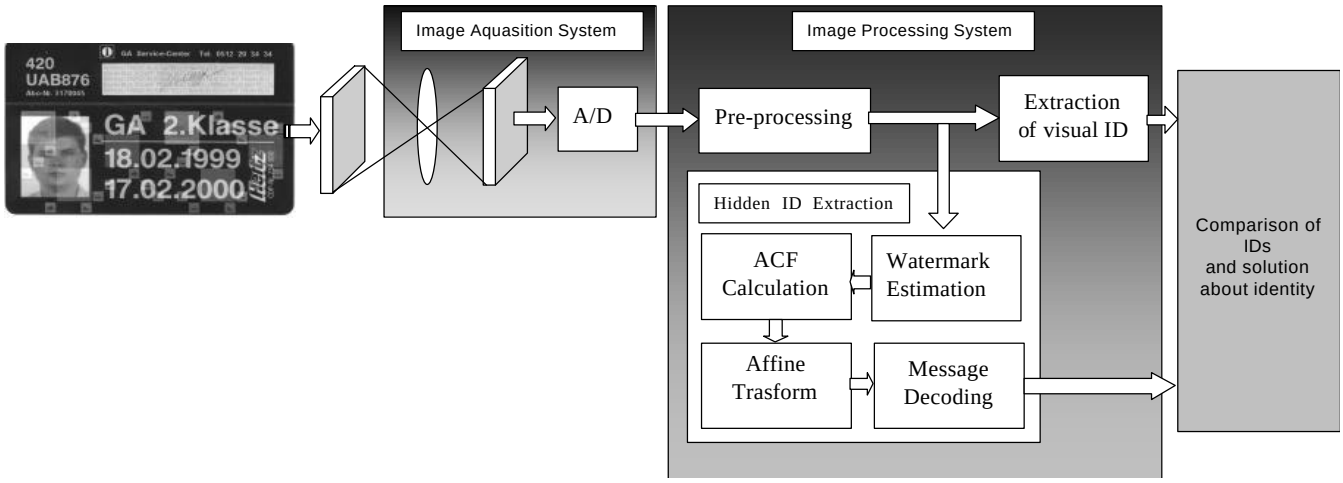

Figure 2. The main components of the optical/digital identification/verification system

shearing and their combinations. It is even assumed that the unauthorized reproduction party exactly knows the method of watermark embedding and detection and can reproduce it on the software or hardware level. However, such a reproduction will not lead to the success in the counterfeight because to embed and extract the watermark the unique key is required that is only known for the document production service and is supplied with the control device. Therefore, the document content integrity is guarantied by the secret key.

4. IMAGE AQUASITION SYSTEM OF DOCUMENT VERIFICATION DEVICE

The task of the image acquisition system is to convert analogue image to the digital form (this procedure is also known as digitization). Two main parts are distinguished in the system - scanning unit, which transforms 2D image of document to 1D analogue electrical signal, and analog-to-digital converter. The scanning unit consists of lighting unit, optical part and light-

to-analog signal converter. General requirements for the acquisition system impose some limitations. Some special problems are discussed below.

It is evident that artificial light should be used in the scanner - this is the condition of the lighting stability of the document and as result the pre-condition of the system robustness independently of internal lighting terms. In the case of use such light-to-signal converter as CCD matrix, a source of light has to illuminate all surface of working zone of the document. This is a classical television scheme. Another scheme is known as flying-spot one. In this case the source of light is the lighting spot with sufficiently small dimensions which moves in the surface of document. Such spot is usually generated by the scanning cathode ray tube (CRT) or by light or laser diode. In the last case a mechanical scanning has to be applied. The first solution has a low scanning speed. The flying-spot scheme simplifies a structure of light-to-signal converter because the task of image-on-elements decomposition is performed by flying spot, not by light-to-signal converter as in the classical television scheme.

The light spectrum is an important property of the light source for the color of document watermark pixels: there is the expedience to print watermark pixels (and calibration points, see following section) in color which is little visible for eye (both with the naked eye and with lenses). It is desirable to have an intensity of this component in spectrum as large as possible. There is no necessity to be worry in regard to efficient detection of printed in the document ID because the last is usually printed in black color on light background.

The optical part is essentially different in the case of CCD or CRT schemes and in the case of moving spot generated by light (or laser) diode. In the first case a lens should create working zone as large as document dimensions (or part of document has to be scanned). As result the optical part has also comparatively large dimensions, which imposes additional constraints for the mobile handling of the device. In the second case only small-size spot should be projected on surface of document that means that the lens dimensions may be also small. This solution can only be realized by a mechanical scanning unit. The amount of transmitted light, the spectral properties and the spatial resolution (resolving power) are relevant for all cases.

The main requirement to scanning unit is the spatial resolution. It has to be such high that a successful watermark detection and retrieval is supported. This implies that it must be higher than the resolution with which message was embedded. To simplify the problem of spatial resolution there is a sense to restrict the scanning zones of the document by those where, for example, photo of the owner and ID are placed on the document.

Scanning procedure in CCD is determined by its structure and standard schemes for CCD control. Spatial resolution of CRT variant of scanning unit is determined by CRT resolution, precisely speaking, by the light spot diameter. The last is not the parameter of the CRT itself. The properties of deflection yoke are of great importance. Special means are sometimes necessary for good spatial resolution ensuring [4]. They permit to correct deflection yoke aberrations, such as considerable aberration as astigmatism. In many cases deflection yoke determines also a distortion of scanning. As it is pointed out in section 4, because of special measure used in image processing system, the CRT distortion does not create obstacles on the way of action of the device. It should be noted that the CRT variant of the scanning unit, as an analogue equipment, is sensitive to the precision of electronic schemes fulfillment which control CRT action.

We do not discuss the mechanical scanning unit in this paper because of it essential peculiarities. However if decreasing of the time of scanning is not very important, this version of scanning unit performance may be attractive.

The analog-to-digital converter is the last part of image acquisition system. A lot of types of such devices are produced by many manufacturers. Their parameters cover wide range of the values in capacity (binary digits), bit rate, output voltage, price etc. That is why the choice of corresponding converter is not the problem. This choice is based on parameters of converter matching with the properties of input and output circuits, and with requirements to identification/verification system in general.

5. IMAGE PROCESSING SYSTEM

Image processing systems consists of the pre-processing unit, and blocks of visual and hidden ID extraction. The digitized image from the image aquasition system could have some blurring, distortions, aberrations and noise due to the unperfected optical system elements. The pre-processing unit aims to compensate them using denoising and deblurring operations. The

calibrations points and zones on the document are predetermined to measure the level of distortions. For examples, 3 calibrations delta-pulses are used to measure blurring in different part of the document assuming that the distortions were shift-variant. The predetermined flat part of the document makes possible to estimate the introduced noise. Also image is divided on the segment in the pre-processing unit that will be used for the extraction of the visual and hidden IDs.

Extraction of the visual ID is performed from the above established corresponding segment of the document using character recognition. The style of the character printing in the document is fixed and has the same size, orientation and spacing between characters for all documents of the interest. Therefore the simple character recognition algorithm could be used to perform this task. As far as, the a lot of attention was paid to the problem of the printed and hand written character recognition , we will concentrate our consideration on the extraction of the hidden data from the digitized images.

The most complicated part of the image processing system is the hidden ID extraction block. The invisible ID number is inserted in the part of the document that represents some unique personal features of the owner. For example, it could be owner's photo or fingerprint, or even the record of the voice. The main idea to perform insertion of the hidden data in this part of the document is to protect the documents against the attempt to counterfeight it using the standard document of another owner (that was lost, stolen etc) and deleting from there the personal features of the original owner and inserting the photo or fingerprint of new unauthorized person. However, such an operation will not lead to the success even if it is performed on the very high professional level. The content integrity of the document will be destroyed that will be immediately detected in the proposed device. The hidden ID corresponds to the visible ID and is called message according to the established digital watermarking and steganography terminology. The owner personal features used for message embedding are called cover image in our case. The marked in this way image is called stego image.
To produce perceptually invisible watermark the embedding system should take into account the particularities of human visual system (HVS), i.e. it should be content adaptive. A lot of empirical models are developed to incorporate the HVS in the structure of watermarking technology [5-8]. A unified stochastic approach to solve this problem is proposed in [9] where it is shown that some known empirical models are the particular cases of the developed approach. To demonstrate the main features of the above mentioned content adaptive watermark embedding in the owner's photo the computer simulation was performed. The cover image is shown in Figure 3a, and the computed function that reflects noise visibility on the cover image using stationary Generalized Gaussian stochastic model of the image is shown in Figure 3b. The resulted stego image with the inserted watermark that has strength equals 12 is depicted in Figure 3c. The direct embedding of the watermark with so high strength could lead to the significant artifacts on the image and especially in the flat regions. Due to the content adaptive features of the proposed method watermark is perceptually invisible and the cover and stego images are undistinguishable that makes possible to preserve the quality of the cover image and perform the identification of the owner from his/her photo. The elements of holograms are visible on the photo and their quality is preserved as well.

a **b** **c**

Figure 3. Example of invisible watermark embedding in the owner photo: (a) cover image; (b) noise visibility function calculated from the cover image; (c) stego image.

Unlike the classic digital image watermarking of still images or video, where the watermark should be extracted after many attacks to prove that the examined image belongs to the corresponding owner, the task of watermarking in the structure of the described system is just to check out the content integrity of the document. It means that assuming that document is original and no attacks were applied to remove watermark (oppositely to classical watermarking where attacker tries to

remove watermark, here he should care to preserve watermark to have unique detection results that will coincide with the visual ID) the requirements to the watermarking algorithm could be essentially reduced.

In particular, the watermark extraction unit consists of the watermark estimation, the block of geometrical transformation compensation that includes the calculation of autocovariance function and the block of affine transform and finally the detection and decoding module which performs the extraction of the hidden message. The task of the watermark estimation is to perform the estimation of watermark based on the stego image using *maximum a posteriori probability* (MAP) method. The different models of the cover image and watermark could be used for this aim. In particular, assuming non-stationary Gaussian model for the image and stationary Gaussian for watermark one receives the classical adaptive Wiener or Lee filter, and assuming stationary Generalized Gaussian model of the image with the same watermark model one receives shrinkage solution similar to wavelet domain [9]. The main idea of this operation is to separate the cover image from the watermark to receive oblivious scheme for message decoding, i.e. the scheme that does not require the knowledge of the original cover image to extract watermark. The second argument for performing the separation is to reduce the crosscorrelation term between image and watermark in the autocovariance calculation and in the decoding module that considerably increases the performance of the scheme. The autocovariance function of the watermark is used to compensate the possibly introduced geometrical distortions during image formation that could destroy the synchronization of the scheme as it was proposed in [10]. Another example of geometrical transformation detection and compensation could be Fourier domain based methods that use the predefined templates for this aim [11]. Final message decoding is performed in the decoding module which first accumulates the all bits of the message according to the spatial spreading rule used for the embedding or equivalently performs the function of the matched filter for the used M- or Gold-sequences. Based on the received integrated peak decision about its sign is made that assigns –1 or +1 to the corresponding values after matched filter.

The decoded hidden message is compared with the visual ID and the conclusion about document identity is made in the final device of the system.

6. CONCLUSIONS

We have presented in this paper a new approach for the generation and verification of analogue identification documents. In contrast to previous approaches, the approach verifies not only the authenticity of the document but also the integrity of important information elements within the document. In addition, the scheme presented my not be penetrated if the approach is known in the public, since the security of the system depends on cryptographic keys. This means that the security requirements and associated costs for a future production process are substantially decreased. We have also shown in the paper that the watermark technology can be very effectively exploited for the target application and is not limited to the copyright protection of digital multimedia data only.

Stirmark Benchmark Results, Version 3.0, accumulated results from previous tests		
Position	Company	Stirmark Ratio (1 is maximum)
1	DCT (AMT)	0.828
2	Digimarc	0.780
3	DCT/CUI (FFT Approach)	0.700
3	Signum Technologies	0.700
4	Blue Spike/Dice	0.230
5	Alpha Tec	0.290
6	MediaSec	0.220
7	IP2	No Show
7	Signafy	No Show
7	Kodak	No Show

The DCT watermark technology has been proven to be very robust against different image transformations which enable the use of the detection devices for identification documents which have been substantially damaged. This was also verified applying the Stirmark benchmark system, known to be the most advanced tool today to check the robustness of a watermarking technology (see table above).
We will extend the DCT technology with respect to a modified color model, M-arrays, and a better luminance estimation

The integration of elliptic curves for the cryptographic key, and a more robust detector are also investigated.

7. REFERENCES

1. Alexander Herrigel, Adrian Perrig, and Joseph J. K. Ó Ruanaidh, "A Copyright Protection Environment for Digital Still pictures", Gesellschaft für Informatik e.V., Fachgruppe 2.5.3 "Verläßliche IT-Systeme", Institut für Informatik und Gesellschaft, Universität Freiburg, "Verläßliche IT-Systeme: Zwischen Key Escrow und Elektronischem Geld", VIS'97.
2. Alexander Herrigel, "Copyright Protection for Multimedia-Data based on Asymmetric Cryptographic Techniques", EUROPTO'98, Electronic Image Capture and Publishing, Hotel Mövenpick, Zurich, Switzerland, May 18-20, 1998.
3. Alexander Herrigel, Joseph Ó Ruanaidh, Holger Petersen, Shelby Pereira, and Thierry Pun, "Secure Copyright Protection Techniques for Digital Still pictures", Workshop on Information Hiding'98, April 1998, Portland, USA, Springer.
4. Z. Hrytskiv, High-Definition Television Methods and Means in Applied Problems. Proc of papers of 3rd Int. Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Services, Vol. 2, pp 568-577, Yugoslavia, 1997.
5. M. Kankanhalli and R. Ramakrishnan, "Content based watermarking of images", ACM Mulimedia98, Bristol, UK, 1998, pp. 61-70.
6. F. Bartolini, M. Barni, V. Cappelini, A. Piva, "Mask bilding for perceptually hiding frequency embedded watermarks", Proc. of 5th IEEE International Conference on Image Processing ICIP98, Chicago, Illinois, USA, October 4-7, 1998, Vol.1, pp. 450-454.
7. C.Podilchuk, W. Zeng, "Image adaptive watermarking using visual models", IEEE Journal on Selected Arias in Communications, May 1998, Vol. 16, No4, pp. 525-539.
8. J. Huang and Y.Shi, "Adaptive image watermarking scheme based on visual masking", Electronic Letters, April 1998, Vol. 34, No8, pp. 748-750.
9. S. Voloshynovskiy, A. Herrigel, N. Baumgartner, T. Pun, Stochastic approach to content adaptive digital image watermarking, Workshop on Information Hiding, Dresden, Germany, Sept. 29-Oct. 1, 1999.
10. M. Kutter, "Watermring resisting to translation, rotation, and scaling", Proc. of SPIE, Boston, USA, November 1998.
11. Shelby Pereira and Thierry Pun, Fast robust template matching for affine resistant image watermarking, In *International Workshop on Information Hiding*, Dresden, Germany, Sep. 29 – Oct. 1, 1999.