ELSEVIER

Dyes and Pigments 43 (1999) 147–151

DYES and PIGMENTS

Application of luminescent materials to encoding in authorized access systems

Yuri A. Gurkalenko [a], Vitali B. Distanov [a], Vera F. Berdanova [a], Alexandr N. Seryakov [a], Nikolaj V. Yakobchuk, Victor V. Prezhdo [a, b,*]

[a] *Department of Organic Chemistry, Kharkov State Politechnical University, 21 Frunze St., 310002 Kharkov, Ukraine*
[b] *Institute of Chemistry, Pedagogical University, 5 Checinska St., 25-020 Kielce, Poland*

Received 5 February 1999; accepted 29 April 1999

Abstract

Based on the analysis of existing means of encoding, storage and protection of information, it is argued that optical encoding has a great potential for applications. The use of luminophors for the development of information encoding systems is discussed. An optical encoding system for access differentiation is developed and recommendations for its use are given.

Keywords: Organic luminophores; Luminescent materials; Encoding systems; Photo-electric reading of information

1. Introduction

Systems that allow supervision of access to specific objects and which provide information protection have a profound impact on modern information technologies. There exist systems of automated identification of people, systems that ensure automatic differentiation of access to specific objects, automated credit systems etc.

Existing systems have drawbacks that cause considerable financial losses. Of prime importance is the problem of information protection. It is estimated that an average damage from a single information crime reaches 450 thousand dollars in the advanced countries. Annual losses due to unauthorized information access, such as breakins to bank computer networks, falsification of credit services, etc., amount to 100 billion dollars in USA and 35 billion dollars in Western Europe [1].

At present, information in such systems is recorded on magnetic carriers. Credit, identification and other types of cards have a special strip containing a ferromagnetic layer with encoded information [2]. These products are inexpensive. They allow for protection of information from visual access and can be rewritten many times. The carrier and identification blocks are simple to manufacture in these products. At the same time, a low degree of protection of the information carrier from falsification, as well as receptivity to action of electrical and magnetic fields often results in information loss. Protection of magnetic cards is largely improved by use of an additional strip for a laser record [3].

Alongside cards based on magnetic carriers, electronic chip based cards, both requiring

* Corresponding author. Tel.: +48-81-361-4012; fax: +48-81-361-4942.
E-mail address: victor@top.pu.kielce.pl (V.V. Prezhdo)

0143-7208/99/$ - see front matter
PII: S0143-7208(99)00052-2

and not requiring electronic contact, are gaining acceptance. They are applied in credit services as substitutes for banknotes and account cards [4–6]. Some electronic information carriers are able to self-destroy automatically at the attempt of unauthorized reading [7]. In comparison with magnetic carriers, electronic carriers are characterized by a higher degree of protection of encoded information, larger storage capacity and better information rewriting capabilities. At the same time, cards requiring electronic contact are not very reliable, because contact groups wear out. Contactless cards are expensive. Electromagnetic and radiation fields that are applied for information readout can gradually destroy electronic cards.

Recently in the field of information encoding, optical methods for recording, storing and reading of information have drawn close attention. To a significant extent, attention has been drawn by the appearance on the market of compact devices, which allow writing of very high density information using optical carriers, and reading of information using laser modulated optical beams. Still, such devices are expensive and require high accuracy during the production process. They have not found wide applications in systems of authorized access. More simple systems, which use both optical and electronic means of information reading are being developed [8,9].

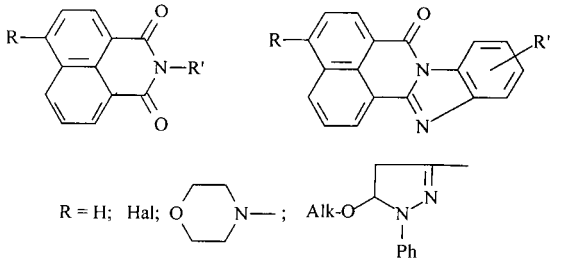
The problem of information encoding is directly related to the problem of information conservation. It is now being accepted that optical carriers of information could provide a more long-term conservation, because of the following advantages over the most widely distributed magnetic carriers [10]:

1. Optical carriers provide higher resolution. One square centimeter of magnetic coverage allows for up to 10^6 information bits, while optical carriers can store up to 10^8 bits within 1 cm^2.
2. Optical memory is more reliable than magnetic. Optical memory is more stable toward external influences and is much less affected by electrical, radiating and magnetic fields.
3. Optical carriers do not lose information with time. Magnetic carriers eventually de-magnetize, while optical memory can store analogue and digital information loss-free and essentially without time limit.

Thus, it is the optical means of information storage and photo-electric means of information reading that possess the greatest potential for the development and production of long-term coding systems.

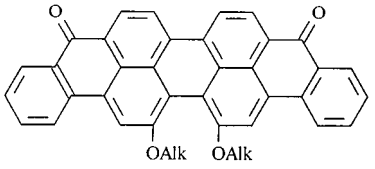
Luminescence properties of chemical compounds can be used for the protection and encoding of information. In order to apply luminescent compounds in optical encoding systems, spectral characteristics and physical-chemical properties of organic luminophors such as area and intensity of luminescence, light resistance, solubility in organic solvents and polymer materials can be exploited.

Judicious use of spectral characteristics of organic luminophors provides ways to move from the currently widespread amplitude based information storage to frequency based storage, which is more reliable in protecting encoded information. Choice of appropriate spectral characteristics of luminophors such as type (**I**) permits coordination with parameters of photo-electric receivers.



(I)

In recent years, information encoding based on luminescent materials has been used in tokens for subway counters. Proprietary organic luminofors such as type (**II**) synthesized in limited amounts are used for this purpose.



Alk = $-(CH_2)_n-CH_3$; n=0...8

(II)

Experience with the subway counters shows that luminescent dyes such as type (**I**) and (**II**) provide good efficiency and information protection. Use of luminescence for information encoding is not limited to subway tokens.

Widespread existence of high resolution duplication techniques makes visual inspection of documents unreliable. One would like to have an automated inspection system that can be used to check identification cards. At the moment, systems that employ magnetic coding do not provide sufficient efficiency and reliability due to the reasons discussed above. In our opinion, optical methods of information encoding and recognition, such as frequency based encoding by organic luminophors such as type (**I**) and (**II**) will allow the creation of a reliable and inexpensive means of access differentiation. These methods can be used to create long-lasting identification documents, transport tickets, certificates, monetary notes, etc.

2. Results and discussion

The purpose of the present work is the creation of an encoding system that uses the luminescent properties of organic compounds of type (**I**) and (**II**). The system is to form the basis of development of identification devices, automated means of travel payment, etc. This system should be simple and reliable in operation, should prohibit information access by visual means, and should possess high resistance to external influences. The system is to enable contactless information read-out by a photo-electric device.

A solution to the problem is provided by a coating that is applied over a card and which consists of a series of luminescent encoding labels located in a certain manner (Fig. 1). The coating prohibits visual recognition of the encoded information, but allows information read-out with the help of a photo-electric device.

In Fig. 1, synchronizing (2) and encoding (4) sequences that consist of synchronizing labels (3) and encoding fields (5) are deposited on the rigid substrate (1) of a card. Encoding labels (6) are placed within encoding fields according to a given encoding scheme. The synchronizing and encoding sequences can be deposited either on the same or on different sides of the card. In either case, the sequences must be appropriately coordinated.

Synchronizing sequences (2) are deposited on the rigid substrate by application of regularly alternating strips that absorb or luminesce in the visible or IR ranges. Deposition can be performed typographically or in other ways. Encoding sequences (4) are deposited by application of strips that alternate in a certain pattern and luminesce in the IR range. Fields that are not used for encoding (5) are covered with a non-luminescent material that has the same color. The synchronizing and encoding sequences are covered on top by a polymer filter (7) that protects encoded information from visual access.

In the above scheme, each encoding field carries one bit of information. The information is stored as a binary code and is inaccessible for visual reading.

The surface of the encoded card is laminated (8) in order to improve its mechanical reliability, protected against external influences, and increases durability in storage and operation. For these purposes the card can also be placed in a plastic case that will supply additional rigidity and stability against mechanical damage.

Identification of the encoded card is achieved with the help of a reception device, which is schematically depicted in Fig. 2. Modulator (1) controls radiation frequency of the optical synchronization pair (2) as well as the frequency of the code readout pair (3). As the encoded card (4)

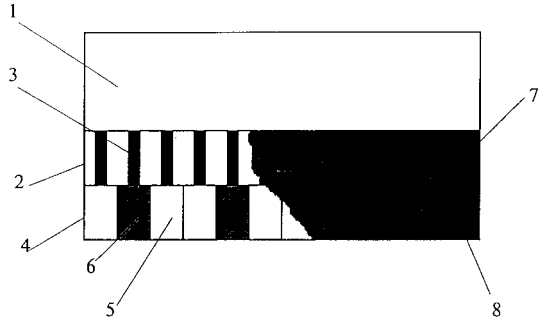


Fig. 1. Scheme of the encoded card: 1 — substrate; 2 — synchronizing sequence; 3 — synchronizing labels; 4 — coding sequence; 5 — encoding fields; 6 — encoding labels; 7 — polymer filter; 8 — lamination.

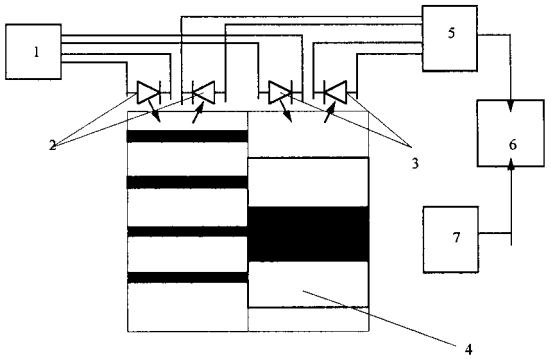


Fig. 2. Scheme of information reception: 1 — modulator; 2 — synchronization optical pair; 3 — code readout optical pair; 4 — encoded card; 5 — synchronous detector; 6 — digital analyzer; 7 — memory.

is scanned through the reception device, the optical pair 2 scans the synchronizing sequence, while the optical pair 3 scans the encoding sequence. Synchronous information readout from photoreceptors of the optical pairs 2 and 3 is provided by the synchronous detector 5. Binary information from the detector reaches the digital analyzer (6), which processes the information. If the information that has been scanned coincides with the information stored in memory (7), the digital analyzer (6) identifies the encoded card as "ours". If discrepancy between the scanned and stored information is found, the card is identified as "foreign".

The above scheme has been implemented in a final product, namely, electronic lock, which can be installed in industrial and household premises to provide authorized access.

Controller (the recognition device) for the card-key is installed on an outside door or other convenient place. It is mounted in a metal case, has a reception slot and an indicator of card recognition.

Power to the controller is provided through either an electrical network or a local block that guarantees an uninterrupted supply of power. Local power block is established in the protected premise and is connected to the network which carries an alternating current of 220 voltage and 50 Hz frequency. The local block contains a watertight accumulator, which can be recharged from the network and which ensures serviceability of the lock if power in the network fails.

The lock is installed in the door of the protected premise. It has a mechanical blocking mechanism and a door-open button. The plastic card-key is manufactured to provide no less than 210^5 door-open cycles. If needed, graphical information can be added to the card. The card-key is designed to be resistant to actions of light, heat and moisture. It withstands electromagnetic and nuclear radiation and works in the temperature range from $-20°C$ to $+50°C$. The encoded information is inaccessible to visual recognition and recognition by UV beams. The information cannot be extracted from the card, even if the card is physically taken apart. The encoding system used ensures no less than 2^{16} code combinations.

In order for the lock to open, the card-key is scanned through the reception slot of the controller. If necessary, an alarm system can be connected to the lock.

The developed device can be also used as part of an accounting system that monitors access to specified objects. For this purpose the device is connected to a computer through the RS-232 serial interface and is operated through the accounting system. When the scanned code coincides with the code of an employee, a sanction allowing passage through is issued and, simultaneously, arrival (or departure) time is recorded.

Devices based on the principles described in this work can be used in systems for access differentiation to objects, which exhibit undesirable properties, such as electromagnetic or nuclear radiation fields. The devices can be installed in industrial enterprises, exhibition halls, hotels, subways, etc.

References

[1] Development, manufacturing and installation of information protection devices. Brochure of enterprise. Kiev: Orekh, 1995.
[2] UK Patent 2091638. Int. Cl. B42D 15/02. Personalising identification cards. Gao Gesellschaft Fur Automation und Organisation MBH. 82.08.04, No. 4875.
[3] International patent No. 82/02968. Int. Cl. G06K 5/00. Banking card for automatic teller machines and the like. Drexler Techology Corporation (US). 82.09.02, No. 21.
[4] UK Patent 2094044. Int. Cl. G06K 1/00. Credit cart. Johnson Matthey Public Limited Company. 82.09.08, No. 4880.

[5] French Patent 2503902. Int. Cl. G06K 19/02. Carte d'identification avec composant a circuit integre. Gao Gesellschaft Fur Automation und Organisation MBH. 82.10.15, No. 41.
[6] French Patent 2503423. Int. Cl. G06K 19/00, 5/00, 7/00. Systeme de cartes a memoire electronique pouvant etre rechargees a des valeurs fiduciaives. Flonic SA. 82.10.08, No. 40.
[7] French Patent 2503424. Int. Cl. G06K 19/06. Support d'information secretes autodestructif. Thomson–CSF. 82.10.08, No. 40.
[8] UK Patent 2108906. Int. Cl. G06K 19/06, B42D. Identification card with concealed coding and decoding module. ITR International Time Limited (GB). 83.05.25, No. 4917.
[9] USSR Patent 698024, Int. Cl.G07C 9/02; A44C 21/00. The Counter for Checking and Running Point, Leningrad's Metro, 15.11.79. Byul. Izobr. No. 42, 20.11.79 (in Russian).
[10] Vsevolodov NN. Biopigments — photoregistratores, Nauka, Moscow, 1988, 224 pp. (in Russian).