MED. INFORM. (1993), VOL. 18, NO. 3, 271–278

Optical memory card applicability for implementing a portable medical record

H. GUIBERT† and A. GAMACHE‡

† Service d'Etudes communes de la Poste et France Télécom, BP 6243, 14066 Caen, Cedex, France

‡ Laboratoire d'informatique en gestion, Département d'informatique, Université Laval, Québec, G1K 7P4, Québec, Canada

(*Received January 1993*)

Abstract. The implementation of portable record based on laser card technology is discussed in terms of data structures for quick access and software tools to reinforce security and confidentiality as required by medical data. Experimental results from a field test with a laser card technology are reviewed with regard to implementation in a large-scale and public information system. An efficient data structure is described for storage purposes, and some proposals are put forward to secure stored data.

Keywords: Portable medical record; Optical card memory; Data security; Storage reliability.

1. Introduction

Sharing information is becoming an issue in the quest of containing costs in health-care systems. It has been acknowledged that communication paradigm [1] is central to improve quality, performance, efficiency and reliability in delivering services to people, and in particular in the health-care fields [2]. Doctors, pharmacists and nursing staff have for a long time recognized the prime importance of sharing medical knowledge to provide their patients with the best care and therapy available. On the other hand, sharing data on a patient's health has not brought the same level of attention; it is still mostly managed the way it was a few decades ago, with almost no data mobility and with restrictive access rights related to security and confidentiality issues.

Cumulating sound facts on one's health is of great value to instantiate a doctor's or a pharmacist's knowledge and getting a better diagnosis, eventually with some support from an intelligent system. Hopefully, these historical data should lead to the most appropriate course of action. This idea has been rejuvenated in recent years following computerization of hospital information systems and emerging expert systems in medicine, and has gained even greater value with the concept of the portable medical record (PMR). By integrating bearers of a secure set of personal medical data in a loosely connected network system, it is possible to implement a virtual link between points of services based on flow of data carried by each patient. No centralized mission-oriented agency is needed to manage medical records; therefore there is no immediate pressure, from a system point of view, to debate privacy and ownership issues of medical data. The system architecture we propose has a built-in feature that puts data to work with reinforced confidentiality, whereas the issue of ownership is being kept pending and does not have a direct and

0307–7640/93 $10·00

immediate influence on the operation of the system. Operating costs of such a system are expected to be lower for equivalent services provided by central or distributed architecture, partly because of low capital investment in hardware and communication network.

The portable record (PR) has great potentialities in system integration either in medical fields or in such areas as electronic banking, distributed manufacturing of maintainable goods and consumer services. Implementation of a portable record is linked to an appropriate technology for storing sensitive information in a card format medium, and to comply with constraints [3] pertaining to large-scale public information systems:

(1) adequate storage capacity for pocket-size format media;
(2) reliability and durability of memory contents;
(3) security, confidentiality and persistency mechanisms for stored data;
(4) fast access to data and technology-independent;
(5) low cost for mass distribution.

2. Optical memory card technology

Many pilots and systems based on smart card technology carried out in many countries have been reported in the literature [4, 5]. Advantages and limits have been scrutinized from various points of views, and most of the time the smart card technology is highly rated with respect to flexibility, security and reliability for storing data on a long-term basis [2]. However, limited storage capacity available, added to a costly microprocessor, appears as a serious drawback to its integration in a decentralized, virtually connected medical information system [6]. Furthermore, new memories such as flash technology memory,high-density magnetic card memory and optical media such as the laser card, have larger storage capacity and are becoming available as a substitute technology for implementing future PR in large-scale public information systems [7, 8].

In this article we address three issues—data structure for quick access, reliability and security of data—in the perspective of a public medical information system based on a PMR implemented with an optical memory. We will also mention some new opportunities offered by laser card technology for system development and integration.

3. OMC memory and formats

Optical memory card (OMC) technology is very similar to WORM (write once read many) optical disc technology. A focused laser beam is used to burn holes into a sensitive layer during writing, while the same laser at a lower power is used for reading, by measuring differences in reflected light. The information is physically grouped in linear tracks, each one is soft sectored during writing. The physical sector is the smallest unit of information that can be written onto the card. To gain more flexibility, several formats corresponding to different sizes of sector per track can be used.

Beside proprietary formats, the *de-facto* standard DELA format is available from most card manufacturers. Work on this format is in progress by an ISO working group, created in 1990 (JTC1/SC17/WG9) to propose an international standard for OMC. Depending on the type of sector used, the memory storage capacity goes from 500 Kbyte to 3·4 Mbyte with error correction code (ECC).

Data organization and management

An OMC's portable record can be designed, as a floppy disk, on a file-based organization with a file directory and a file allocation table containing lists of sectors included in each file. Updating a file is then being done in a non-obvious manner by logically cancelling updated sectors and then writing back and indexing new sectors. An optimal use of optical memory space implements two stacks, one for data and a second for indexes located at the opposite end of the memory, growing towards each other.

In fact, such a file system can be memory- and time-consuming when processing a medical record which is basically transaction-oriented. When looking at the frequency and average amount of data written into a PMR, it seems more convenient to see transactions at a logical level to be mapped to physical records. The records are collected together in physical zones depending on their meaning and access rights. A typical PMR such as the one being tested in the Quebec pilot comprises the following physical zones: ID data, emergency, diagnoses, medication, vaccines, laboratory results.

With a PMR, updating medical records may be mandatory in two non-frequent cases: when a system failure occurs while writing in a physical zone and when a patient wants to delete a transaction. In the first case a special mechanism deals with the atomicity of logical transactions in order to preserve data integrity. The second case is related to a recognized patient's right to discard sensitive information from his PMR. The transaction's records containing the data are physically deleted by overwriting the sector, and new updated records are created using new sectors.

Due to the sectoring of OMC the system always reclaims a sector whose size is just larger than the size of the record, thus avoiding costly internal record-keeping for managing record segmentation. In the special case of an image record it is rather considered as a file, and is then stored in a set of tracks with the first one being pointed to by an entry in the index stack.

With the current technology reading speed is still slower (160 Kbit/s including ECC bits); compare to the speed to which we are accustomed with floppy disks. To bypass this bottleneck we designed an efficient index mechanism to meet the requirements of health professionals who expect a quick access to the most recent records in each physical zone.

We now describe a PMR prototype using an optical memory card. The memory structure is based, as already mentioned, on two physical stacks growing in opposite directions. The data space is dynamically allocated with units made of blocks of homogeneous tracks with the same format and belonging to a physical zone.

Each block entry is stored in the index stack using the shortest sector available. An index block entry contains the physical zone number, the first track address of the block, block size and its format. The block size is a function of the physical zone number and the formats available, and is specified according to statistical results, given that block size for ID records should be smaller than those for diagnoses records.

A PMR physical zone is then composed of scattered blocks of tracks of different formats, allowing an efficient mapping between records and sector sizes. The records are also indexed by a transaction number field, which is the last data written in a special zone when the system commits a transaction. A complete transaction can later be rebuilt by software only if its unique transaction number occurs in this

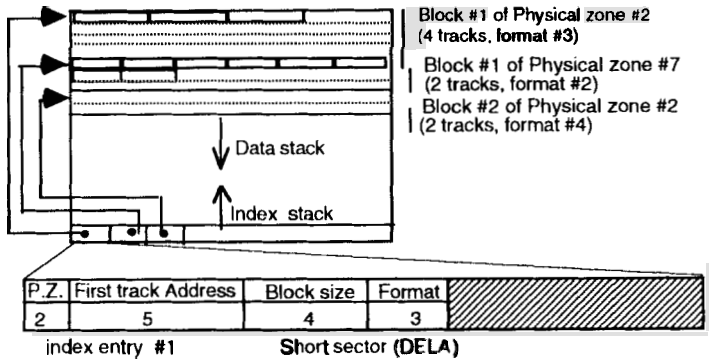

Figure 1. Physical memory layout.

special zone. Otherwise, a transaction is partial and cannot be validated for any purpose (figure 1).

To access a record in a given physical zone, the index stack should be looked up followed by a search in the transaction zone to obtain related transaction numbers before reading the records from the blocks of the given physical zone. If a professional wants to access the most recent records ignoring past records, a logarithmic search can process tracks in a given block.

5. Reliability tests

These tests are designed to evaluate the reliability of the optical card as it may be integrated in a large public scale system. The idea was to organize a field test on a short period, and to simulate intensive use of the card by a representative group of nine volunteers. Our intent was also to evaluate how important is the protective cover delivered with the card on reliability. The cards were distributed as follows:

(1) five professional workers with two carrying protected cards in their wallet or bag and three others without cover, used with no special directives and exposed to physical contact with embossed plastic cards;
(2) two clerical workers: cards without protective cover and carried in bags with individual plastic cases for each one;
(3) two technicians: a card used with the same conditions as for the clerical worker.

The cards were requested every week for testing: the procedure consists of writing 50 tracks composed of all available formats filled with a repetitive pattern of bits. The writings are scattered in order to test the entire card surface. Then all tracks written since the beginning of the test were read back and a file containing reading errors was systematically created. The field test lasted 4 months and the results are summarized in the following paragraphs.

We give some examples of evolution of different errors rates: a clerical card in figure 2 and a professional card in figure 3. We can notice the positive effect of ECC with protected cards whereas the same correcting code is no longer effective with unprotected ones. Secretarys' and technicians' cards have very few scratches and generate low error rates; $< 1\%$ errors for tracks with error-correcting code (ECC) and a 5% bit-error rate for tracks without ECC (figure 2). Professional cards with protective cover show no scratches and no reading errors (figure 3). Furthermore,

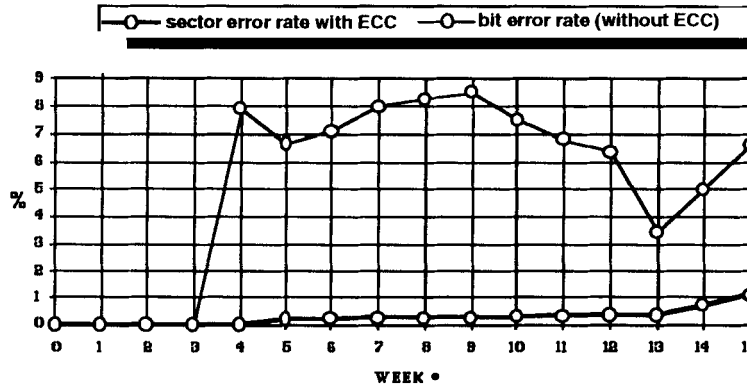

Figure 2. Evolution of error rates for a secretary's card.

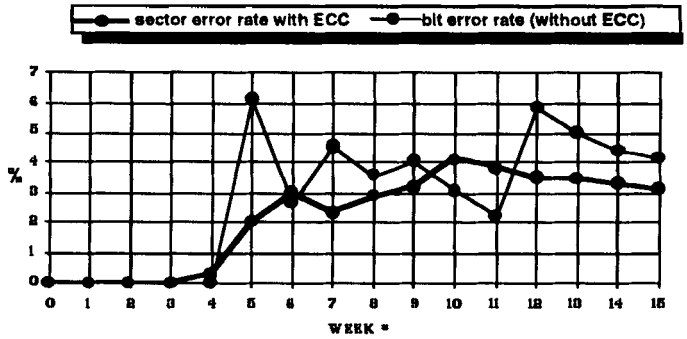

Figure 3 Evolution of error rates for a professional's card.

those without protective cover have many scratches and holes, generating high error rates from 3 to 8% with ECC, and up to 15% without it.

To complete the tests, and to obtain a better understanding of these results, we have made some measurements on holes and scratches responsible for software errors. We have done many profilometer readings to obtain details of width and depth of surface holes from professional cards. For scratches the width goes from 0·05 to 0·1 mm and the depth can go up to 10 μm; for spot holes the width is between 0·1 and 0·5 mm, with a mean depth around 2 μm. In the later case the physical damage was so severe that the ECC code was almost ineffective.

6. Security features for a PMR based on optical memory card

A well-recognized feature of a portable medical record is its ability to provide specific access rights to each medical zone depending on each group of health professionals [5]. Another important point is to ensure the confidentiality of the medical data. Compared to the smart card, the optical card is a rather passive medium. The physical confidentiality of data cannot be implemented by built-in mechanisms; the WORM nature of the media can only guarantee that a stored record has not been modified since its first writing. Confidential mechanisms should be added to the basic card facilities.

7. The health care professional card

The solution, commonly used for magnetic supports, is to cipher confidential data. The work can be done by software or, better, by a tamper-resistant module that can keep the key's secret in its memory. The smart card is a very good piece of firmware to achieve this goal, and will then be used as the healthcare professional (HCP) card. The professional authentication can be realized by a PIN built-in checking procedure.

8. Privacy of medical transactions

The access right to a physical zone is related to the professional group authorized to gain access, and is given by the encipherment/decipherment key hidden in each HCP's card. As the use of a secret key algorithm does not give sufficient information to differentiate between writing (encipherment) and reading (decipherment) operations, extra confidential data should be provided by the HCP card for gaining access to each zone. These access rights are transferred to the medical application software which manages the professional's logical access rights.

The Data Encryption Standard [8] is used because of its good computing performance (3000 bit/s) and its latest implementation in new smart card products. As the DES algorithm works with 64-bit blocks, longer records are split into such blocks, and the use of the cipher block chaining mode is being recommended to avoid identical ciphered blocks.

In order to minimize possible discovery of one of the primary encryption keys, the health professional card uses secondary keys specific to each patient card to cipher its data. Those secondary keys K_i' should be generated in each HCP card by a one-way function f using the primary key K_i of the physical zone i and the ID number of the patient card PMR_Id:

$$K_i' = f(K_i, \text{PMR\_Id})$$

9. Integrity of medical transactions

Another important aspect of data quality concerns the integrity of medical transactions. Each transaction must be stamped with the originator's ID, and a digital signature is computed from the data in the transaction by an internal public key algorithm stored in the control program area. Such a digital signature prevents unauthorized replications of transactions or a possible repudiation of the transaction by its originator. This last issue may become a critical point in some legal dispute.

The RSA algorithm [9] is recommended because it is widely used and is now hardware-implemented, taking an average of 2 s to compute a 512-bit signature. Each HCP card is provided with a secret RSA key pair (d,n) for signing while its public key pair (e,n) is used for verification. This information is made available from a well-disseminated public directory containing all health professional ID numbers and their public key [10].

A digital signature S is first processed by computing a digest $\mathcal{J}$ of the transaction T with a hash-function H, then by the RSA algorithm itself: $S = \mathcal{J}^d \bmod n$. A verification procedure consists in computing $\mathcal{J} = H(T)$, then with the originator's public key (e,n) to compute $\mathcal{J}' = S^e \bmod n$; if $\mathcal{J} = \mathcal{J}'$ then the transaction integrity is verified.

10. PMR authentication

In the same way the authenticity of the PMR can be guaranteed by a digital signature of the card ID computed by the card issuer (e.g. with RSA). To prevent possible forgery of a PMR using optical cards, they must be manufactured with a unique serial number in the card identity field as proposed by the DELA standard. PMR authenticity can be verified by the HCP card using the issuer's public key.

11. Conclusion

The optical memory card is a candidate technology for implementing a portable medical record. Its large amount of memory allows an expected longer life before saturation occurs. However, in the context of wide public use the PMR medium should comply with very strong standards regarding reliability. Results show that the OMC tested would be suitable, if and only if it provides system integrators with the guarantee that the protective cover will always be used by all bearers. Furthermore, using a DELA format gives each application software more technology independence and makes them less sensitive to short-term obsolescence. Otherwise, the driver should be enhanced with capabilities of recognizing proprietary formats and runs an appropriate set of commands. The feasibility of this approach has been shown to be workable by the successful development of a super-driver for smart card technologies in the Quebec PMR.

The security of medical data can be reinforced only by using smart cards with cryptographic facilities on board. The use of the DES and the new proposed DSS or well-known RSA algorithms is mandatory to achieve the two important requirements in this field: privacy and integrity of medical records.

Acknowledgements

This study was supported by a research grant from the Régie de l'Assurance-Maladie du Québec. The authors wish to thank Professor Michel Guillot from the Mechanical Engineering Department for profilometer readings, Pierre Durant from the Computer Science Department for fruitful discussions, and Mohamed Achemlal from SEPT for sharing data on OMC technology.

References

1. Moor, G. J. E. (1992) Telestroika in health care informatics: a challenge for standardization in Europe. *Medical Informatics*, **17** (2), 133–140.
2. Klein, G. (1992) Security principles for patient card systems. In *Proceedings of the Eighth Annual International Symposium on Computerization of Medical Records, New Orleans*, March, pp. 111–118.
3. Schieske, C. (1992) Long term strategic directions in health care communications. In *Proceedings of the Eighth Annual International Symposium on Computerization of Medical Records, New Orleans*, March, pp. 210–214.
4. Berubé, J. Fortin, J.-P., Boudreau, C., Lavoie G., and Kirouac, S. (1992) Expérience d'une carte santé à Rimouski. *Le médecin du Québec*, February, pp. 67–69.
5. Spencer, K. R. (1991) The encounter card project in Ontario. In *Proceedings of CardTech, Washington*, pp. 77–80.
6. Gamache, A., and Dan-Karami, H. (1992) Simulation de l'exploitation de la carte santé du Québec; cycle de vie de l'aide-mémoire médical portable. *Rapport de Recherche DIUL-RR-9203*. Université Laval, Québec, Canada G1K 7P4.
7. Brown, J. H. U., Vallbona, C., and Shoda, J. (1991) Evaluation of a new patient record system using the optical card. In *Proceedings of Thirteenth Annual Symposium on Computer Applications in Medicare*, pp. 714–717.
8. *Data Encryption Standard* (1977) National Bureau of Standards, Federal Information Processing Standards, Publication no. 46.

9. RIVEST, R., SHAMIR, A., and ADELMAN, L. (1978) A method for obtaining digital signatures and public-key cryptosystems. *Comm. ACM*, February, **21** (2), 120–126.
10. GUIBERT, H. (1993) Etude de faisabilité du dossier médical portable sur carte à mémoire optique. *Rapport de recherche, DIUL-RR-9301, 1993.* Dép. d'informatique, Université Laval, Québec, Canada G1K 7P4.