UDC 519.725.4 + 004.932.2

L.A. Kuznetsova, A.A. Iakovenko

*Odessa National Polytechnic University, Odessa*

# MEDICAL IMAGES VERIFICATION

*Medical image security can be enhanced by using watermark (WM), which is formed using an identifier of the image (ID). Identifier may consist of doctor's digital signature or personal number. We propose a reversible WM secret system consisting of modulo addition of the mark into a cover image (CI). This approach is only applicable to image storing formats, that utilize no transform domain compression techniques. There is also a restriction to the image format type, so that image compression should either be lossless or image should be compressed before the embedding. The referent pattern of WM is the secret key of the system, which can be generated randomly or evaluated from doctors' personal ID's. The use of modulo operations for WM embedding allows us to recover the exact original image. In order to avoid significant degradation of the WM detection efficiency, we propose an adaptive choice of WM detector and WM intensity combined with error-correcting codes. With this approach the watermarked images cannot be used as-is for medical applications because of visible distortion.*

***Keywords:*** *verification of images, convertible digital thread-marks, correctings codes, detector of digital thread-marks, invisibility.*

## 1. Introduction

In Medical Information Systems (MIS) the definition of information security relies on data means the integrity, authenticity, availability and confidentiality conditions. If we approach this subject using watermarking technology we face a number of restrictions [1 – 3]. The most important restriction is that image distortions resulting from the insertion process, should not interfere with the image interpretation. To overcome this issue, one possible solution is to use reversible watermarking, for which the extraction of a WM allows should restoring the pixels of the image to their original state. If we use a modulo addition approach to embed a WM, the restoration of the original image is possible by using a modulo subtraction operation. Once the watermark is removed the image is not protected any longer.

Another solution consists in simplifying the task by forming ID of the most important (from the medical point of view) area of image. The obtained WM is embedded in the remaining part of CI, in Regions of Non-Interest [1].

Working with arithmetic modulo may introduce a salt and paper noise in the image, but after the extraction of WM using arithmetic modulo subtraction method this noise disappears. The other known disadvantage of modulo addition algorithm is the efficiency degradation of WM extraction [4].

In this paper we analyze a combined watermarking method based on modulo addition of the mark with adaptation of the detector to the luminance probability distribution of the image luminance (histogram) of the image and using error-correcting codes to improve the overall efficiency of WM detection. In the Section II, among the usual correlation blind detectors, we discuss the selective and modulo detectors we propose for our application. The system is secret and the reference pattern of WM is used as a secret key. In Section III the results of the simulation are provided. Section IV contains some conclusions and discusses the problems which remain open.

## 2. Adaptive watermarking detection

Let us assume that the ID of the image contains *R* bits. If we use a binary systematic error correcting code

$$Z \in (m,\ L,\ d),$$

where $m$ – the block length; $L$ – the number of information bits; $d$ – the minimum code distance; $R_o = R / L$ code blocks are necessary to encode R bits. Since the CI consists N pixels there will be necessary

$$N_o = NL / Rm$$

pixels per code symbol at the identifier embedding.

The j-th code block can be embedded as

$$s(n) = \left( c(n) + \alpha(-1)^{b\left\lceil \frac{n}{n_o} \right\rceil + 1, j} w_r(n) \right) \bmod C_m,$$

$$n \in A_n,\ A_N = \{1, \ldots\ N\}, \qquad (1)$$

where $c(n) \in C$ is the original image; $\alpha$ is an integer, $w_r(n)\big|_{n \le N} \in W$, W is a reference pattern, $w_r(n)$ is an i.i.d. random sequence; $s(n) \in S$, S corresponds to the watermarked image; $b_{ij}$ is the *i*-th bit of the *j*-th block in the code, $i = 1, \ldots, m$, $j = 1, \ldots, 2^L$.

We assume that the blind WM detector knows the reference sequence and the parameter $\alpha$, but does not know the original image. Synchronization between the transmitted and received WM code blocks block is pro-

vided. To simplify the case and reduce the complexity of calculations here we take only grey scale 8-bit images, although those algorithms could be applied to color images as well.

For this algorithm, it is quite normal to use a correlation detector [6]. We take a decision about the embedding of the j-th code block if the correlation between the secret key and the marked image is in the max [6]:

$$\Lambda_j = \max_{0\le j\le 2^L} \sum_{n=1}^{\frac{NL}{R_0}} (s(n)-C_0)\alpha(-1)^{\left\lfloor \frac{n}{n_o} \right\rfloor + 1, j} w_r(n), \quad n \in A_n, \tag{2}$$

where $C_0 = E\{C\}$ is the expected value of the image.

We use the selected parts of the image, which allows us to assume that the data is distributed as a stationary process in the wide sense. The correlation detector is not optimal for model eq. (1), but we can estimate an error probability for any histograms of the image [6]. Taking into account Central Limit Theorem the probability of false decoding of code block is upper bonded as follows:

$$P_{fd} \le (2^L - 1) Q\left( \frac{\alpha}{\sigma_c} \sqrt{\frac{N}{R} Vd} \right), \tag{3}$$

where $\sigma_c^2$ is the variance of the image, $V = L/m$ is the code rate and

$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty \exp -(t^2/2)\, dt .$$

From eq. (3) we can also see that efficiency of the WM detection is determined by the product $Vd$ of the chosen code. If $R = 64$, $w_r(n)\big|_{n\le 10000}$ then for the trivial code $Z:\{m,m,1\}$ 64 code blocks will be used. Then $P_{fd} \le 1{,}56 \cdot 10^{-5}$ and signal-to-noise ratio after embedding of the WM $\eta_w = \sigma_c^2/\alpha^2 = 5{,}55$. Instead, for Golay code $Z:\{24,12,8\}$ and for fixed $P_{fd}$ we easily get a value $\eta_w = 160$, i.e. the image is better preserved.

The detection procedure eq. (2) is degraded by modulo addition in the general case and the calculation of the probability Pfd by eq. (3) is not precise. So here we have a contradiction, where we have to use the modulo addition approach for WM removal, but the same modulo decreases the efficiency of the detection. To diminish the modulo impact on performances of WM detection we propose using adaptation procedure consists in of selecting for each image of the most efficient detector and optimal WM intensity for each image. The choice is made upon the luminosity histogram of the image. In this work, two detectors are proposed; they take into account the use of arithmetic modulo. Let us consider for simplicity the comparison of the detectors without error correcting code. We will estimate probability of bit detection error in consideration of modulo embedding.

So, for the WM embedding stage, the idea of the selective detector (SD) is to use only those pixels which give the same results with modulo arithmetic and the usual one. We can describe such selective detector as follows:

$$\Lambda^{SD} = \sum_{n\in F_\alpha} (s(n)-C_0)w(n), \quad n \in A_N \Rightarrow$$

$$\Rightarrow \quad b = \begin{cases} 1, & \text{if } \Lambda^{SD} \ge 0, \\ 0, & \text{if } \Lambda^{SD} < 0, \end{cases} \tag{4}$$

where

$$F_a = \{ n \le N \,|\, (s(n)-\alpha) \bmod C_m \le 255-\alpha; \; (s(n)+\alpha) \bmod C_m \ge \alpha \}$$

is a set of selected pixels, $N_0 = |F_\alpha|$.

We have utilized the maximum livelihood criterion (MLC) for modulo detector analysis. MLC does not necessarily satisfy any optimality criterion, but it can almost always be computed, either through exact formulas or numerical techniques and it asymptotic optimality properties. According to the MLC we get the following optimal modulo detector for this model

$$\Lambda^{MD} = \sum_{n\le N} (((s(n)-\alpha w(n)) \bmod C_m) - C_0)^2 -$$

$$- \sum_{n\le N} (((s(n)+\alpha w)) \bmod C_m) - C_o)^2 \Rightarrow$$

$$\Rightarrow b = \begin{cases} 0, \text{if} \Lambda^{MD} < 0, \\ 1, \text{if} \Lambda^{MD} \ge 0. \end{cases} \tag{5}$$

The probability of bit detection error can be correctly calculated as

$$P_e = Q\left(\frac{E\{\Lambda\}}{\sqrt{Var\{\Lambda\}}}\right), \tag{6}$$

where $E\{\Lambda\}$, $Var\{\Lambda\}$ are respectively the conditional expectation and the conditional variance of the detection functional.

To use (6) we have to define

$E\{\Lambda_1\}$ and $Var\{\Lambda_1\}$ when $b = 1$;

and $E\{\Lambda_0\}$, $Var\{\Lambda_0\}$ when $b = 0$.

For all detectors

$$E\{\Lambda_1\} = -E\{\Lambda_0\}, \; Var\{\Lambda_0\} = Var\{\Lambda_1\}.$$

For correlation detector

$$E\left\{\Lambda_0^{CD}\right\} = N\left[\alpha - \frac{C_m}{2} P(C)\right];$$

$$Var\left\{\Lambda_0^{CD}\right\} = N\Big[\sigma_c^2 + C_{mo}^2 P(C) - \tag{7}$$

$$- C_m \left( \sum_{c(n)\in A_c} c'(n)\, f(C) - \sum_{c(n)\in D_c} c'(n)\, f(C) \right) - C_{mo}^2 P^2(C) \Big];$$

$$A_c = \{0,1,...,\alpha-1\};\ D_c = \{255-\alpha+1,...,255\};$$

$$c'(n) = c(n) - C_0;\ C_{mo} = 0,5\,C_m;\ f(C)$$

is the histogram of the image and

$$P(C) = \sum_{c(n)\in D_c} f(C) + \sum_{c(n)\in A_c} f(C).$$

In Table 1 we present the error probabilities for CD calculated by eq's. (6), (7) for the Second Image.

Table 1

WM detection error probability dependence from α, obtained by analytical analysis

| α | 3 | 4 | 5 | 6 | 10 | 20 | 30 |
|---|---|---|---|---|---|---|---|
| $P_e$ | 0,06 | 0,15 | 0,33 | 0,58 | 0,44 | 0,35 | 0,26 |

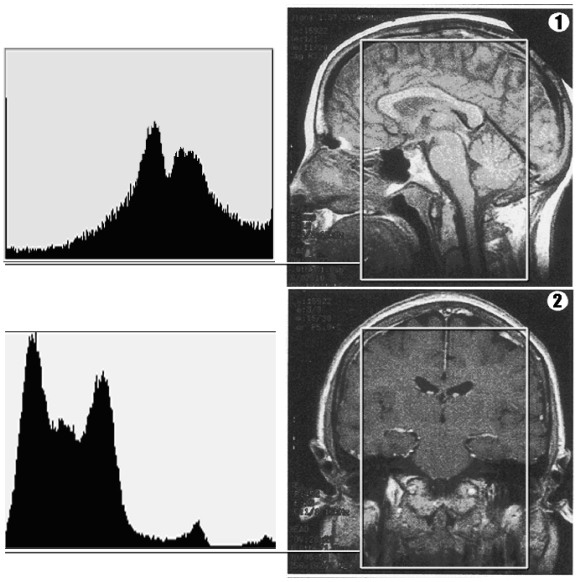


Figure 1. Test images and their corresponding histogram

During the embedding procedure we can choose the WM intensity and the WM detector type by analysing the image histogram. This allows us to choose an embedding algorithm before the application of WM, choose the intensity of WM and its code base. The analytical analyse for MD and SD is very tedious for estimation. We have utilised the Monte Carlo method.

## 3. Results

The proposed WM method has been tested over diverse medical images IRM. The results we provide here have been obtained for two MRI of the head of 640x1024 pixels, illustrated in Figure 1. It has been observed salt-and-pepper noises with $\alpha \geq 4$ using $C_m = 256$ in the modulo. The length of the sequence $w_r(n)$ is chosen as 1000 bits for all experiments. It is obvious that there is no distortion and noise once after the WM has been detected and removed. The detection error probability dependence on WM intensity for all types of the detectors is shown on the Figure 3 for the three detectors presented previously.

It can be seen, that there is a significant phenomenon for modulo embedding procedure comparing to ordinary (not modulo) embedding [5]. The error probability is no longer a monotonic decreasing function of the parameter $\alpha$, and there exists indeed some $\alpha$ for which exists a minimum or a maximum error probability. This fact also complies with the results of the section 2. The results of the Tabl.1 are close enough to the results of simulation presented in Tabl.2.

Let us note that with $\alpha = 5$ for SD the average value of $N_o / N$ for the first image is equals 1, and 0,99 for the second. If we take $\alpha = 30$ then the results are 0,98 and 0,82 respectively. The simulation results confirm the analytical analysis.

Table 2

Error rates for different types of detectors

| Img | Detectors | WM amplitude | | | | | |
|---|---|---|---|---|---|---|---|
| | | 3 | 5 | 6 | 10 | 20 | 30 |
| 1er | CD | 0,03 | 0,005 | 0,001 | 10-4 | 3*10-4 | 0,002 |
| | SD | 0,04 | 0,004 | 0,001 | 10-4 | 2*10-4 | 10-4 |
| | MD | 0,033 | 0,005 | 0,002 | 10-4 | 5*10-4 | 0,01 |
| 2er | CD | 0,08 | 0,35 | 0,55 | 0,61 | 0,55 | 0,3 |
| | SD | 0,07 | 0,35 | 0,54 | 0,6 | 0,4 | 0,3 |
| | MD | 0,02 | 0,1 | 0,16 | 0,11 | 0,09 | 0,08 |

The WM detection error probabilities for the correlation detector and for the selective one in the case of image 2 (with dominance of the black) are almost the same. The use of modulo detector in the same conditions of simulation decreases the error probability more than to 3 times On the contrary, for the image number 1, the use of selective detector decreases the value of $P_e$, especially when $\alpha \geq 10$. However, the image quality with embedded WM is quite mediocre.

We could apply the method described above using the secret protocol: two secret key, one for calculate the identifier (the digital signature or the hash) and another for WM embedding and WM detecting.

A doctor (D1) sends an image signed with his digital signature to a MIS administrator (A). A extracts the signature to verify that the D1 is the owner, and to restore the image to its original state. When A receives a request for some image, he checks the image taken from the database with its UID, taken from the other, to be sure that the image is not compromised by a third-party and to restore the original image. The next step is to add to the image the identity of a person who made this request (ID2) and to send the image to this person. Using this protocol we can preserve the original image from distortion, detect the modifications, and verify each step of information exchange and the identities of the persons involved. It is possible utilise utilize one public WM algorithm for embedding the identifiers of the doctors for witch WM invisibility is character [1].

## 4. Conclusion

In order to provide a content authentication of images based on the embedding of ID into an image itself, a modular embedding technique can be used. The appearance of salt and paper noise in the areas of image, important for the medical diagnostics, is not always acceptable in MIS. We could apply the method described above using the defined protocol.

In this article we have proposed and analysed a combined watermarking method based on modulo 256 addition of the mark, choosing the WM intensity and the detector using the criteria of probability distribution (histogram) of the image, and the final application of the error-correcting codes. For all types of detectors like correlation, selective or modulo detector the error probability is no longer a monotonic function of WM amplitude, and there is an optimum value of $\alpha$ that minimizes the error probability of the detection as well. The analysis of image histogram before WM embedding allows us to select a corresponding detector and WM intensity which allows us to minimise WM detection error probability. There are many open problems in this topic. The repetition of WM-reference several times may result in a significant decrease of the number of errors. But it results in a very large time delay in authentication procedure. It is also necessary to estimate the delay in image authentication taking into account adaptive embedding and a list extracting procedures for different error correcting codes.

We can decrease the computational time needed for the initialisation of verification procedure by using some predefined code-books, that is to say – avoid its creation each time before the initialisation of procedure. Another possible direction is to improve WM invisibility. Requirements in MIS are very different from other multimedia applications concerning the invisibility criterion. We are working in that direction right now.

## References

*1. Coatrieux G. A Review of Image Watermarking Application in healthcare / G. Coatrieux, L. Lecornu, B. Sankur, Ch. Roux // Proc. 28th Annual Int. Conf. of the IEEE EMBS. – 2006. – Vol. 2. – P. 4691-4694.*

*2. Bas P. Tatuoage d'images fixes – Chapture 2, ouvrage "Tatouage de documents audiovisuels numeriques" / P. Bas, D. Delannay, J.-M. Chassery. – Edition HERMES. – Janvier 2004. – 332 p.*

*3. Schou C.D. Information Assurance in Biomedical Information Systeme / C.D. Schou, J. Frost, W.V. Maconachy // IEEE Enginering in Medicine and Biology Magazine. – 2004. – Vol. 23, no 1, P. 110 – 118.*

*4. Cox J. Digital Watermarking / J. Cox, M.L. Miller, J.A. Bloom. – Morgan Kaufman Publishers, 2002. – 280 p.*

*5. Korjik V. A Performance Evaluation of Digital Private Watermarking for the Host Data Known or not at the Decoder / V. Korjik, D. Marakov, I. Marakova, G.L. Morales // Actas de la VII Reunion Espanola de Criptografia y Seguridad de la Information. – Oviedo: Springer, 2002. – Vol. 2. – P. 461-471.*

*Надійшла до редколегії 18.02.2009*

**Рецензент:** канд. техн. наук, доцент С.В. Кавун, Харківський національний економічний університет, Харків.

**ВЕРИФІКАЦІЯ МЕДИЧНИХ ЗОБРАЖЕНЬ**

Л.А. Кузнецова, О.О. Яковенко

*Захищеність медичних зображень може бути поліпшена шляхом впровадження цифрового водяного знаку (ВЗ), який є сформованим з використанням ідентифікатора зображення. Ми пропануємо оборотну систему ВЗ, яка використає додавання по модулю два мітки та зображення-носія (ЗН). Принцип побудови мітки є таємним ключем системи. Використання модульних операцій для впровадження ВЗ дозволяє точно відновити вихідне зображення. Для того, щоб уникнути суттєвого погіршення ефективності детектування ВЗ, ми пропануємо систему з адаптивним вибором типа детектора та інтенсивності ВЗ, а також завадостійким кодуванням. Для того, щоб обрати оптимальний тип детектора, перед впровадженням ВЗ аналізу піддається розподілення освітленості зображення. При використанні такого підходу, зображення, що містить ВЗ не може використатися у медичних цілях «як є» через видимі спотворення. Єдиний спосіб, за яким можна отримати початкове високоякісне зображення, – використати запропонований протокол для зберігання та вилучення зображень.*

***Ключові слова**: верифікація зображень, оборотні цифрові водяні знаки, корегуючи коди, детектування цифрових водяних знаків, невидимість.*

**ВЕРИФИКАЦИЯ МЕДИЦИНСКИХ ИЗОБРАЖЕНИЙ**

Л.А. Кузнецова, А.А. Яковенко

*Защищенность медицинских изображений может быть улучшена путем внедрения цифрового водяного знака (ВЗ), который сформирован с использованием идентификатора изображения. Мы предлагаем обратимую систему ВЗ, использующую сложение по модулю два метки и изображения-носителя (ИН). Паттерн построения метки и является секретным ключом системы. Использование модульных операций для внедрения ВЗ позволяет точно восстановить исходное изображение. Для того чтобы избежать значительного ухудшения эффективности детектирования ВЗ, мы предлагаем систему с адаптивным выбором типа детектора и интенсивности ВЗ, а также помехоустойчивым кодированием. Для того чтобы выбрать оптимальный тип детектора, перед внедрением ВЗ анализируется распределение освещенности изображения. При использовании этого подхода, изображение с ВЗ не может использоваться в медицинских целях «как есть» из-за видимых искажений. Единственный способ, при помощи которого можно получить изначальное высококачественное изображение, – использовать предложенный протокол для хранения и извлечения изображений.*

***Ключевые слова**: верификация изображений, обратимые цифровые водяные знаки, корректирующие коды, детектор цифровых водяных знаков, невидимость.*