Multi-Layer Watermarking Aimed at Closed Information Systems

Roumen Kountchev[1], Vladimir Todorov[2] and Roumiana Kountcheva[3]

Abstract – **A new method for image watermarking, aimed at documents archiving is presented in this paper. This specific application is very useful in all cases, when large amounts of original paper documents have to be stored for many years, in accordance with financial lows. The substitution of these originals with their electronic copies ensures easy access and security. The new watermarking method is based on the Inverse Difference Pyramid (IDP) decomposition, performed in the image spectrum.**

Keywords – **Information assurance, Watermarking, Image compression, Web-based information systems.**

I. Introduction

In correspondence with the financial lows' requirements, all companies are obliged in their everyday practice to store large amounts of original paper documents (invoices, etc.). As it is known, the long-term storage of paper documents creates many troubles for the owner, most of which are connected to the fact, that they require too much physical space. Most up-to-date computer technologies permit the creation of electronic copies of the documents and their archiving and saving on diskettes, optical disks, etc., which in result makes their storage much easier. To do this, the documents must be scanned and thus obtained digital images - compressed and saved. The most frequently used compression methods are based on the standards JPEG or JPEG2000. The traditional approach in the big enterprises is to store the compressed images on CD, using WARM (Write-Once-Read-Many) technologies. In some cases electronic signature is used as well, but this is not enough for the secure document storage: as it is known, there are many software products, which permit easy image editing. This requires additional security levels in the archived image files, in order to ensure their original contents untouched and to prove any kind of un-authorized access. Part of these problems could be solved using image watermarking [1-3]. In some applications, the watermark extraction is performed without comparison with the original image, and in other cases, the original must be available. The second case is suitable for documents archiving, because the original image will be easily available, when requested, and the comparison will ensure the watermark extraction [4,5]. A new method for multi-layer image watermarking, ensuring the document content authenticity, is proposed in this paper. The watermarking is performed using a new method for image decomposition, called Inverse Difference Pyramid (IDP) [6]. In this case, the decomposition is performed in the image spectrum area, and the image content is processed in consecutive layers with increasing resolution. This approach permits the insertion of different watermark in every layer. Any change in the watermark image, noticed after the extraction, is a proof for un-authorized image content editing. To perform the watermarking the original paper documents have to be scanned and saved as bmp or JPEG files, and after that - watermarked.

[1]Roumen Kountchev is with the Faculty of Communications and Communications Technologies, Technical University of Sofia, Kliment Ohridsky 8, 1000 Sofia, Bulgaria, E-mail1: rkountch@tu-sofia.bg

[2]Vladimir Todorov is with T&K Engineering Co., Sofia 1712, P.O.Box.12, Bulgaria. E-mail:vtodorov@yahoo.com

[3]Riumiana Kountcheva is with T&K Engineering Co., Sofia 1712, P.O.Box.12, Bulgaria. E-mail: rkountcheva@yahoo.com

II. Basic Principles of the IDP Decomposition

In the general case, every digital image $[B(2^n)]$, consisting of $2^n \times 2^n$ pixels could be represented with inverse difference pyramid (IDP) [6] in accordance with the expression:

$$[B(2^n)] = [\tilde{B}_0(2^n)] + \sum_{p=1}^{n-1} [\tilde{E}_{p-1}(2^n)] + [E_{n-1}(2^n)] \ , \quad (1)$$

where $p = 0, 1, 2, \ldots, n$ is the number of the pyramidal decomposition level.

The first component $[\tilde{B}_0(2^n)]$ in Eq. (1) corresponds with the level $p = 0$ and defines the coarse image approximation as a result, obtained after applying the inverse orthogonal transform of the truncated image spectrum $[\tilde{S}_0(2^n)]$ with the matrix $[T_0(2^n)]$ with size $2^n \times 2^n$, i.e.:

$$[\tilde{B}_0(2^n)] = [T_0(2^n)]^{-1}[\tilde{S}_0(2^n)][T_0(2^n)]^{-1} \ . \quad (2)$$

The coefficients of the spectrum matrix $[\tilde{S}_0(2^n)]$ are defined with the expression:

$$\tilde{s}_0(u,v) = m_0(u,v)s_0(u,v), \text{ for } u,v = 0,1,..,2^n-1. \quad (3)$$

Here the elements $m_0(u,v)$ of the matrix-mask $[M_0(2^n)]$ define the position of the retained coefficients from the two-dimensional image spectrum $[S_0(2^n)]$:

$$m_0(u,v) = \begin{cases} 1 \text{ if } (u,v) \in V_0; \\ 0 - \text{in other cases,} \end{cases} \quad (4)$$

where V_0 is the area of the retained spectrum coefficients $s_0(u,v)$. The corresponding spectrum matrix $[S_0(2^n)]$ is obtained in result of applying the direct orthogonal transform for $[B(2^n)]$ with the matrix $[T_0(2^n)]$, i.e.

$$[S_0(2^n)] = [T_0(2^n)][B(2^n)][T_0(2^n)]. \quad (5)$$

In the decomposition levels $p = 1, 2, ..., n-1$ from Eq. (1) the corresponding component is defined as:

$$[\tilde{E}_{p-1}(2^n)] = \begin{bmatrix} [\tilde{E}^1_{p-1}(2^{n-p})] & [\tilde{E}^2_{p-1}(2^{n-p})] & \cdots & [\tilde{E}^{2^p}_{p-1}(2^{n-p})] \\ [\tilde{E}^{2^p+1}_{p-1}(2^{n-p})] & [\tilde{E}^{2^p+2}_{p-1}(2^{n-p})] & \cdots & [\tilde{E}^{2^{p+1}}_{p-1}(2^{n-p})] \\ \cdots & \cdots & \cdots & \cdots \\ [\tilde{E}^{4^p!-2^p+1}_{p-1}(2^{n-p})] & [\tilde{E}^{4^p!-2^p+2}_{p-1}(2^{n-p})] & \cdots & [\tilde{E}^{4^p}_{p-1}(2^{n-p})] \end{bmatrix} \quad (6)$$

The sub-matrices $[\tilde{E}^{k_p}_{p-1}(2^{n-p})]$ for $k_p = 1, 2, .., 4^p$ of the matrix $[\tilde{E}_{p-1}(2^n)]$ are obtained as a result of its quad tree division in 4^p equal parts. Each sub-matrix in Eq. (6) has size $2^{n-p} \times 2^{n-p}$ and is defined in similar way as shown in Eq. (2).

$$[\tilde{E}^{k_p}_{p-1}(2^{n-p})] = [T_p(2^{n-p})]^{-1}[\tilde{S}^{k_p}_p(2^{n-p})][T_p(2^{n-p})]^{-1}, \quad (7)$$

where

$$\tilde{s}^{k_p}_p(u,v) = m_p(u,v)s^{k_p}_p(u,v) \quad (8)$$

for $u, v = 0, 1, .., 2^{n-p} - 1$.

The elements of the matrix-mask $[M_p(2^{n-p})]$ of the retained coefficients are defined with:

$$m_p(u,v) = \begin{cases} 1 & \text{if } (u,v) \in V_p; \\ 0 - & \text{in other cases.} \end{cases} \quad (9)$$

Here V_p is the area of the retained spectrum coefficients $s^{k_p}_p(u,v)$, whose matrix $[S^{k_p}_p(2^{n-p})]$ is obtained after applying a direct orthogonal transform on the difference matrix $[E_{p-1}(2^{n-p})]$, using the transform matrix $[T_p(2^{n-p})]$:

$$[S^{k_p}_p(2^{n-p})] = [T_p(2^{n-p})][E^{k_p}_{p-1}(2^{n-p})][T_p(2^{n-p})] \quad (10)$$

In Eq. (10) the term $[E_{p-1}(2^{n-p})]$ is defined as:

$$[E_{p-1}(2^{n-p})] = \\ = \begin{cases} [B(2^n)] - [\tilde{B}_0(2^n)] \text{ for } p = 1; \\ [E_{p-2}(2^{n-p})] - [\tilde{E}_{p-2}(2^{n-p})] \text{ for } p = 2,..,n\text{-}1. \end{cases} \quad (11)$$

The remaining component, corresponding to the last level $p = n$ in Eq. (1), is presented with the difference:

$$[E_{n-1}(2^n)] = [E_{n-2}(2^n)] - [\tilde{E}_{n-2}(2^n)] \, . \quad (12)$$

In the case, when the decomposition from Eq. (1) is truncated up to the component r, the so-called "truncated" IDP is obtained, presented by the expression:

$$[\hat{B}(2^n)] = [\tilde{B}_0(2^n)] + \sum_{p=1}^{r} [\tilde{E}_{p-1}(2^n)] \quad (13)$$

In the image frequency domain the IDP pyramid consists of the spectrum coefficients $s^{k_p}_p(u,v)$, for $k_p = 1, 2, .., 4^p$. For the level p their number is as follows:

$$M(p) = 4^p M_p = 4^p \sum_{u=0}^{2^{n-p}-1} \sum_{v=0}^{2^{n-p}-1} m_p(u,v) \quad (14)$$

for $p = 0, 1, 2, .., n-1$.

Then the total number of coefficients for IDP pyramid with r levels is:

$$M_\Sigma(r) = \sum_{s=0}^{r} 4^s M_s = \\ = \sum_{s=0}^{r} \sum_{u=0}^{2^{n-s}} \sum_{v=0}^{2^{n-s}} 4^s m_s(u,v) \;\; \text{for} \;\; r < n \, . \quad (15)$$

In particular, for $M_0 = M_1 = ... = M_r$=4 one can get from Eq. (15):

$$M_\Sigma(r) = \sum_{s=0}^{r} 4^{s+1} = \frac{4^2}{3}(4^r - \frac{1}{4}) \approx \frac{1}{3}4^{r+2} \, . \quad (16)$$

In case, when the matrix $[B(2^n)]$ represents one image block with size $N \times N$ pixels, the total number of coefficients for all blocks is correspondingly:

$$M_\Sigma = \frac{N^2}{4^n} M_\Sigma(r) = N^2 \sum_{s=0}^{r} \sum_{u=0}^{2^{n-s}} \sum_{v=0}^{2^{n-s}} 4^{s-n} m_s(u,v) \, . \quad (17)$$

Then for $M_0 = M_1 = ... = M_r$=4, Eq. (17) is producing $M_\Sigma = (N^2/3)4^{r-n+2}$.

After a lossless compression for all coefficients' values $s^{k_p}_p(u,v)$, from pyramid level p a corresponding binary massif $\{X_p(r) : r = 1, 2, .., l_p\}$ with length l_p, is obtained. At the beginning of this massif $\{X_p(r)\}$ is inserted a special header, H_p. It contains information about the pyramid level p, the elements of the matrix-mask $[M_p]$, the kind of the orthogonal transform, the arrangement of coefficients in the massif, etc.

III. Image Watermarking Based on IDP

The decomposition, represented by Eq. (1), permits the insertion of different watermark in every level of the IDP pyramid. For this, elements $Z_p(r)$ for the level p of the data massif, are represented as follows:

$$Z_p(r) = \begin{cases} X_p(r) \text{ for } r = 1, 2, .., l_p; \\ W_p(r) \text{ for } r = l_p + 1, l_p + 2, .., l_p + l_{wp}. \end{cases} \quad (18)$$

Here $W_p(r)$ is the compressed data with length l_{wp} representing the watermark in the level p, obtained after applying the password, Y_p. The password itself is a code, with length $l^y_p \leqslant l_p$. The number N_{wp}, corresponding to the watermark for the level p, is defined with the equation:

$$N_{wp} = l_p \oplus Y_p = \sum_{i=0}^{l^y_p - 1} (l^p_i \oplus y^p_i) \, , \quad (19)$$

where l^p_i and y^p_i are the corresponding i-th digits of l_p and Y_p, and with "$\oplus$" is noted the operation "exclusive OR". The number N_{wp}, corresponding to the watermark, is inserted in the header H_{wp} of the compressed data, W_p(r).

The watermark image (prepared in advance) is compressed with lossless compression. For this reason it is suitable to use relatively small watermark (256x256 or 512x512 pixels) and in the process of decomposition to apply it on the document image as many times, as necessary, to cover it. The IDP decomposition permits watermark images with size 512x512 pixels to be compressed losslessly in a file with size 500-600 Bytes, depending on image contents. This size is negligible, compared to the size of the digital image of the paper document. Even after compression is used, the corresponding file is very large, because the quality of the restored document image must be good, and the compression ratio could not be high. The following (higher) pyramid level creates a new

data sequence $Z_p(r)$, where another watermark image could be inserted. Then all the information is arranged in one common massif. The data, obtained in result of the image compression, and the inserted watermark, is saved and stored, or sent to the receiver in accordance with the application, using the existing standard communication nets. The watermark insertion in the image data is equivalent to the creation of additional level in the pyramid.

IV. Image Decoding and Watermark Visualization

The decoding is done, performing the already described operations in reverse order:

- The components $X_p(r)$ and $W_p(r)$ are extracted from the massif of the received data $Z_p(r)$ and the watermark image $W_p(i,j)$ for the level p is restored;
- The information $X_p(r)$, obtained in result of the lossless compression, is decoded, and the values of coefficients $s_p^{k_p}(u_r, v_r)$, are calculated;
- The model of the sub-image $[\tilde{B}_0]/[\tilde{E}_{p-1}^{k_p}]$ is calculated, using inverse orthogonal transform, as presented with Eqs. (2) and (6);
- The values of the elements $\hat{B}_w(i,j)$ of the restored image are calculated. This image can contain two (or more) watermarks in the lower IDP pyramid levels, in correspondence with the expression:

$$[\hat{B}_w(i,j)] = [\tilde{B}_0(i,j) + W_0(i,j)] + [\tilde{E}_0(i,j) + W_1(i,j)] + \sum_{p=2}^{r} [\tilde{E}_{p-1}(i,j)] \quad (20)$$

In the already described watermarking method the IDP decomposition starts from the lowest level, where the square, corresponding with one sub-image is 16x16 or 8x8 pixels (resp. n=4 or n=3). In this image layer the document owner can insert his (or her) own watermark. Example image for original image document is shown in Fig. 1. This watermark is visible, and it is the first authentic watermark, inserted in the document image. It corresponds to the "public" document watermark. The result is shown in Fig. 2 - the example text image with inserted visible watermark. The same watermark could be made invisible as well. This is performed, choosing a watermark in which the brightness value is smaller than the sensitivity threshold of the human visual system.

The choice of a visible or invisible watermark is a result of a decision, made by the document owner, and usually is the same in all documents, created by him. The size of the watermark image usually is smaller then that of the document and in the process of the image recovering it is applied as many times, as necessary, to cover all the document image.

The next level of the decomposition (the higher pyramid level) is the place to insert the second watermark – usually, invisible. In the method, offered here, this watermark depends on the image contents, and correspondingly – on the

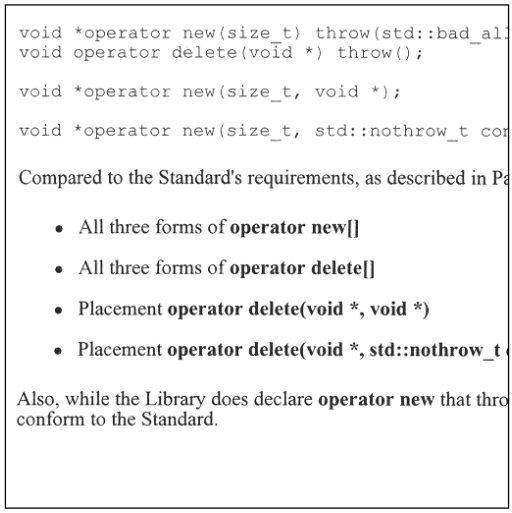

Fig. 1. Original text image

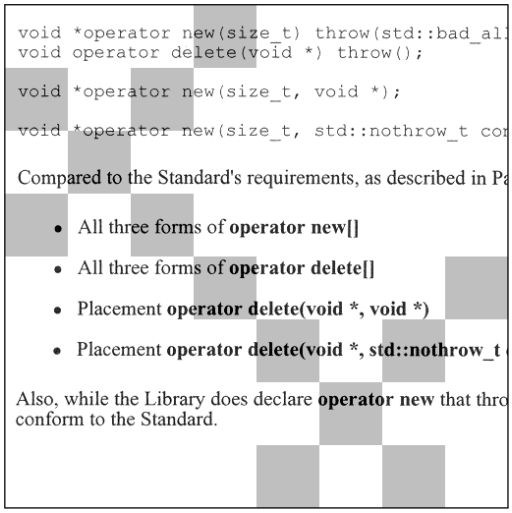

Fig. 2. Watermarked Text image

result, obtained after the compression of the data from the second pyramid level. As watermark images could be used all two-dimensional Walsh-Hadamard functions, or another images, included in the special image library. The choice of the watermark is performed, after the compressed data is obtained, and the number of the compressed bits is known, Eqs. (12) and (13). The fact, that the watermark is invisible, and the requirement to use a password ensures, that the possession of the decompression software will not permit the watermark visualization and the existence of watermark will not be known. The watermark visualization will be possible only if the password is available. The analysis of the image header (in case, that somebody knows the algorithm in detail and is able to analyze it) will show that the image contains inserted invisible watermarks, but the extraction will be impossible without the password.

In case of un-authorized image contents change (using special software for image editing) the visible watermark should be changed as well, but the invisible one will not be

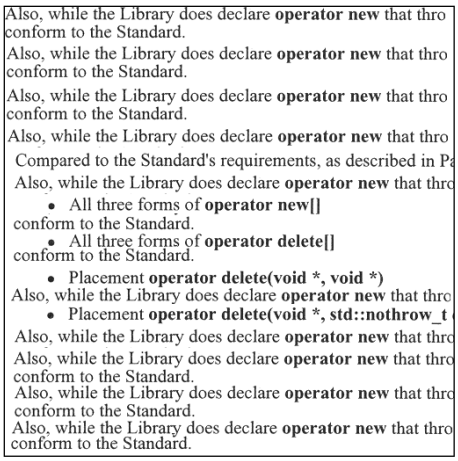

Fig. 3. Original text image

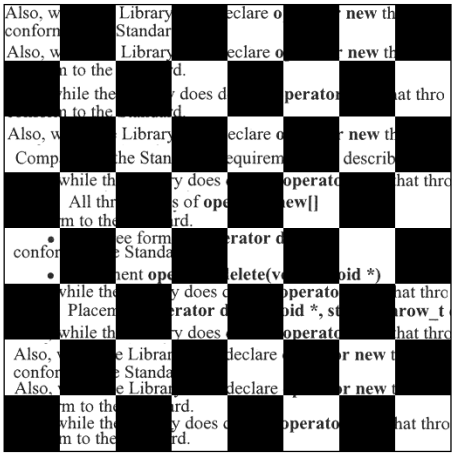

Fig. 4. Watermarked text image with masking watermark

touched. There are two reasons for this. The first is that in result of the use of the algorithm for lossless coding of the equal symbols, and of the adaptive modified Huffman code, the length of the compressed file could not be calculated or defined in advance. The data, obtained in result of the compression, are changed in accordance with the image contents and any change in this contents results in change of the file length l_p. Because of this peculiarity of the algorithm, the first indication that the image had been edited is the change in the compressed data length. If the password is known, the new value of the data file length together with the password, will point at another watermark image from the library after the processing. Even the document owner does not know this, because the process of choosing the invisible watermark image is performed automatically. The same approach is used in the next, higher pyramid level, where another invisible watermark is inserted. The watermark visualization is performed in a way, similar to visualization of the classic paper watermarks: for them we use light with higher brightness, and in our case, algorithm for sharpening the brightness transitions is used. All watermarks are visualized layer by layer, until all of them are processed.

In some cases the watermark could be used to cover (hide) the original image, or a selected part of it. Example for such application is shown in Figs. 3 and 4. In this case, instead of an invisible watermark, is applied a watermark, which destroys the original image. This example illustrates that the text information could not be used until the watermark is successfully removed. The recovery of the original document is possible only if the password is available.

All watermarks must answer the following requirements:

- The watermark image must be a drawing, consisting of relatively large figures (8x8 pixels, or larger), with constant brightness. Such image is resistant against JPEG compression with high compression ratio.
- In order to ensure that the watermark is invisible, its brightness value must be relatively small. In the cases, when it is applied on parts of the original document, where the total brightness is high, the brightness value of the watermark image should be under the sensitivity threshold of the human visual system. In other cases, where the document brightness is lower, the brightness value of the watermark image could be higher. Such approach requires the creation of intelligent, adaptive algorithm, which in most cases would make its application difficult. In result, it is easier to use watermarks with small brightness value, which could be applied over the whole document and remain invisible.

The basic application of the described method is aimed at closed information systems for saving and storage the images of the electronic copies of documents with paper originals. This application area defines some restrictions:

- The watermark extraction requires a password;
- The method requires the document creator to have a library of watermark images, one or more of which to be inserted in the document image in correspondence with the described algorithm;
- The volume of the compressed data, representing the original document, is increased with the watermark insertion, and in result, the compression ratio is reduced.

V. Basic Method Advantages

1. The knowledge of the algorithm and the usage of decompression software do not permit the watermark extraction. This is possible only if the password is available;

2. Any change, noticed in the visualized invisible watermark, proves un-authorized access and image contents editing;

3. The fact, that the inserted watermark becomes a part of the image, makes it resistant against another compression methods, cropping, shifting, resizing, etc.;

4. The ability to insert more than one watermark in a single image increases the image contents security.

VI. Conclusion

The IDP decomposition permits easy watermark insertion in the consecutively processed image layers with increasing res-

olution. In result, the image editing and the watermark extraction are very complicated and together with the requirement to know the password and to have access to the image library of the document creator, the un-authorized access becomes practically impossible. The method could be used in PC image processing, Windows environment.

References

[1] J. Tzeng, W. L. Hwang, I. L. Chern. Enhancing Image Watermarking Methods with/without Reference Images by Optimization on Second-order Statistics. IEEE Transactions on Image Processing, Vol. 11, No. 7, July 2002, pp. 771-782.

[2] J. Brassil, S. Low, N. Maxemchuk, L.O'Gorman. Electronic Marking and Identification Techniques to Discourage Document Copying. IEEE J. Select. Areas Commun., Vol. 13, Oct. 1995, pp. 1495- 1504.

[3] W. Szepansky. A Signal Theoretic Method for Creating Forgery-proof Documents for Automatic Verification. Carnahan Conf. On Crime Countermeasures, Lexington,KY,1979,pp.101-109.

[4] B. J. Falkowsky, Lip-San Lim. Image Watermarking Using Hadamard Transforms. Electronics Letters, 3^{rd} February 2000, Vol. 36, No. 3, pp. 211-213.

[5] M. Hartung, M. Kutter. Multimedia Watermarking Techniques. Proceedings of the IEEE, Vol. 87, No. 7, July 1999, pp. 1079-1086.

[6] R. Kountchev, V. Haese-Coat, J. Ronsin. Inverse Pyramidal Decomposition with multiple DCT. Signal Processing : Image Communication, Vol. 17, January 2002, pp. 201-218.