Security and Watermarking of Multimedia Contents
Vol. 3657, January 1999
San Jose, California, USA

OCTALIS benchmarking : Comparison of four watermarking techniques

Laurent Piron [a], Michael Arnold [b], Martin Kutter [a], Wolfgang Funk [b],
Jean Marc Boucqueau [c], Fiona Craven [d]
[a] Ecole Polytechnique Fédérale de Lausanne, Lausanne, Switzerland
[b] Institute für Grasphischte Datenverarbeitung, Darmstadt, Germany
[c] Université Catholique de Louvain, Louvain la Neuve, Belgium
[d] Circuits Test and Systems Technology Ltd., Dublin, Ireland

ABSTRACT

In this paper, benchmarking results of watermarking techniques are presented. The benchmark includes evaluation of the watermark robustness and the subjective visual image quality. Four different algorithms are compared, and exhaustively tested. One goal of these tests is to evaluate the feasibility of a Common Functional Model (CFM) developed in the European Project OCTALIS and determine parameters of this model, such as the length of one watermark. This model solves the problem of image trading over an insecure network, such as Internet, and employs hybrid watermarking. Another goal is to evaluate the resistance of the watermarking techniques when subjected to a set of attacks. Results show that the tested techniques do not have the same behavior and that no tested methods has optimal characteristics. A last conclusion is that, as for the evaluation of compression techniques, clear guidelines are necessary to evaluate and compare watermarking techniques.

Keywords: Watermarking, benchmarking, copyright protection, image trading, evaluation

1. INTRODUCTION

Copyright protection has become a key point in the digital world. Because of the possibility to duplicate digital images without any quality loose, new tools are required. In the framework of the European project OCTALIS, image trading over the Internet has been considered. A global solution, which includes image protection, secure transmission, and user authentication, has been developed. Image protection is obtained through the use of watermarking techniques, which allow to invisibly embedding of a signature into the image. A key point is the robustness of watermarking techniques to standard and malicious image manipulations. Furthermore, it should be possible to embed several signature with different algorithms, so-called *hybrid watermarking*. These are the main requirements for the OCTALIS solution. Therefore, benchmarking of watermarking techniques is as necessary. The benchmarking consists of (1) testing the concept of hybrid watermarking, and (2) evaluating the robustness of the methods to standard image manipulations, such as JPEG compression. In addition, the visual image quality is subjectively evaluated since there is a tradeoff between the watermark robustness and the distortion introduced through the watermarking process.
This paper is organized as follows. Section 2 presents the OCTALIS Common Functional Model. Section 3 introduces the watermarking algorithms and Section 4 presents the benchmarking, including robustness and quality tests. Finally, conclusions are given in Sec. 5.

2. OCTALIS COMMON FUNCTIONAL MODEL

1. OCTALIS Common Functional Model

Trading of digital data has to face security problems that cannot be solved with a single technology. Several mechanisms have to be integrated in a hierarchical concept that provides controlled access to and copyright protection of multimedia data. Meeting such security demands requires the mastering of both tasks simultaneously in an integrated system. Related European projects, TALISMAN [1], and OKAPI [2] are developing tools and contribute to standardization bodies to meet these requirements. OCTALIS [3] intends to unify and integrate these results into one system. The main purpose is to validate this system through large-scale trials and to drive it towards a commercial exploitation.
The approach is driven by two guidelines: (1) The OCTALIS functionality, and (2) the specificity of the trials environments. The OCTALIS functionality is, to provide all the necessary means in order to be able to say:

« I sell remotely my creation to you in a secure way »

This sentence has to be split into three parts:

«... My creation... » Implies a strong link between the creator and the creation. This corresponds to the work protection step and is solved by technologies like watermarking and labeling.
« I sell remotely ... in a secure way » implies at least buyer and seller authentication, confidentiality, privacy and integrity. Conditional access systems provide those functionality. Within OCTALIS, those are extended to establish a reliable electronic contract over an open and unsecured network.
« ... To you ... » implies a customization of *« ...my creation... »*, regarding the buyer. This is done by an additional watermark (fingerprint).
OCTALIS trials were chosen to cover the major on-line distribution channels. On one hand, the point-to-multipoint (broadcasting) environment, with real time constraint, is tackled by securing of the European Broadcasting Union (EBU) primary network exchanges. On the other hand, point-to-point connections are addressed through the secure access and delivery of multimedia content via the Internet.
The solutions developed in the OCTALIS project rely on two core technologies: Conditional access control and watermarking. Conditional Access System (CAS) aims at managing access control for a specified set of users. This set of users is set-up and maintained through a registration process (e.g. when buying a decoder, a SIM card or an X.509 certificate is issued). In general, well designed CAS offer the following functionality:

- Access control to the creations.
- A-priori identification and authentication of recipient.
- Secured data transfer.

This makes CAS a powerful, but incomplete tools for the protection of Intellectual Property Rights (IPR). Access to creations can be controlled, and rights to its use can be a-priori negotiated and legally formalised. But when it has been accessed, there is no technical mean to control its use. Other technologies to track the accessed creations are necessary. Therefore the second OCTALIS core technology, digital watermarking. In the rest of this article we focus on the watermarking issue.

2. Hybrid watermarking

Actors in the OCTALIS scenario have different security demands. On one hand, copyright owners want to get revenue for the IPR linked to their images. On the other hand, customers need certification of the origin of the material. Furthermore, service providers as well as content owners want to be able to prove commercial piracy in court. Therefore, an environment for secure distribution of digital contents must contain the following features

- The protection of the copyright.
- The authentication of the data.
- The tracing of illegal copies.

In general, these security mechanisms benefit from links between data and a corresponding entity, like copyright owner, Registration Authority (RA), or buyer of the image. These links have to be robust against manipulations such as lossy compression, filtering, format conversion and other types of image processing manipulations. Strong cryptography (e.g. digital signatures) or overlaid copyright labels are not sufficient for providing a practical solution to this problem. Digital watermarks are the most promising answer. The OCTALIS infrastructure makes use of three different digital watermarks to fulfil the above requirements.
Embedding of copyright information into images and registration procedures should take place as early as possible during the production process of the digital data. Three watermarks are embedded in each image. The embedding of the first two watermarks, W1 and Wpub, has to be performed at the service producer's site. Tracing of commercial piracy and illegal copying implies the authentication of the person who violated the IPR. The starting point of this unauthorized distribution of the image is the buyer of the image; therefore the service provider has to embed a fingerprint authenticating the buyer, the third watermark W2. The embedding method depends on the application scenario. The watermarks protecting the copyright and tracing illegal copying should be readable only by authorized persons. These watermarks have to be kept secret, so that, $W1 = W_{priv-1}$, and $W2 = W_{priv-2}$. In contrast everyone should be able to authenticate the data by reading the second watermark, which has to be a public one.
Therefore, as mentioned above, the image delivered to the customer contains three watermarks:

- A secret watermark, W_{priv-1}, for IPR protection. In OCTALIS, W_{priv-1} is the hash value $H(\hat{O})$ over the original image $\hat{O}$. This information is sufficient because only the copyright owner possesses the original image from which $H(\hat{O})$ can be computed [4]. We use MD5 or SHA hash algorithms resulting in a 128-bit and 160-bit watermark, respectively.
- A public watermark, Wpub, to authenticating the data. Wpub is the so-called license plate, which is a 64-bit unique identification code associated to the registration authority (RA) registering the image. The license plate will be referenced in the license agreement.

- A secret watermark, $W_{priv-2,}$ to identifying the customer. This 32-bit identification number will be referenced in the license agreement.

The secret watermark W_{priv-1} is qualified for proofing ownership of an image without contacting a RA. Registration of the license plate and $H(\hat{O})$ by a RA is an additional service for end-users. Although W_{priv-1} is not really necessary to prove ownership it simplifies this step, and makes it less complex.

3. Conclusion

In this section, the scenario developed within the OCTALIS project has been presented. It has been shown how watermarking techniques can be used for image trading over an insecure network such as the Internet. The proposed solution uses three watermarks, with different semantic meaning. Hence, a total of 224 or 256 bits are embedded in each image, depending on the hash algorithm used for W1. Two different watermarking algorithms can be used. In this case, an interesting and important issue investigates the interaction between the different methods. In addition, watermarking techniques should be robust to "standard" attacks, such as JPEG compression.

3. WATERMARKING ALGORITHMS DESCRIPTION

4. Introduction

Digital watermarking is a research topic with increasing popularity in the last years. Many algorithms have been and are still developed [5]. The goal of watermarking techniques for IPR protection is to invisibly embed a signature into the image. Many different approaches have been developed. The watermark can be embedded in the spatial domain, frequency domain, or in a multi-resolution environment. In all cases, the human visual system (HVS) plays an important role. By exploiting the HVS, the watermark robustness can be increased and visual artifacts decreased.

In this section the different watermarking algorithms considered within the project are presented. The algorithms were provided by (1) Circuits Test and Systems Technology Ltd. (C.T.S), Dublin, Ireland, (2) Institute für Grasphische Datenverarbeitung (I.G.D), Darmstadt, Germany, (3) Ecole Polytechnique Fédérale de Lausanne (E.P.F.L), Lausanne, Switzerland, and (4) Université Catholique de Louvain-la-Neuve (U.C.L), Louvain-la-Neuve, Belgium.

5. Description of C.T.S algorithm

The watermark is first coded using spread spectrum modulation. The image is divided into blocks. For example, a block size of 64 can be used. The Discrete Cosine Transform of each block is obtained using luminance values and certain coefficients of the transformation are modulated using bi-directional coding. The modulated coefficients are those that are most relative to the intelligibility of the image. The inverse transform is obtained and the new image block replaces the old one in the image. In order to store three independent watermarks in an image, a different frequency band is modulated for each watermark inserted.

6. Description of I.G.D algorithm

The algorithm is block based and shares some features with the JPEG standard for still-image compression [6]. The luminance component of an image is divided into 8x8 pixel blocks. The algorithm selects a sequence of blocks and applies the DCT to each of the selected blocks. The transformed blocks are quantized with the luminance quantization table proposed in the JPEG standard. The quantization step divides a DCT coefficient's value by an integer number that depends on the coefficient's position within the block matrix. High frequency coefficients are divided by higher quantification values than low frequency ones. The integer values forming the quantization table can be multiplied or divided by a constant value to allow scaling of the quantization impact on the coefficients.

Two components of the algorithm must be considered:

- The position for the watermark embedding must be generated. A key is used to initialize a pseudo-random number generator that determines the order of block processing and the coefficient to be modified within the block.
- A method that modifies the coefficients selected during the position-generation step must be chosen to embed the watermark.

The algorithm can embed up to four different, non-interfering watermarks in an image. This is accomplished by dividing the frequency range for watermarking into four sub-bands. Three sub-bands can be used for secret watermarking, while the fourth band is used for public watermarking.

In each selected block, one bit is encoded as follows (t_i is used to denote the absolute value of quantified DCT coefficients, and the subscript i identifies the coefficient position within the sub-band):

- The pixel values within the block are DCT transformed.
- A mechanism for detecting edges is applied that takes advantage of the block's DCT representation.

- A pair of DCT coefficients is selected from the appropriate sub-band of the transformed block. Each sub-band consists of three coefficients, leading to six possible coefficient pairs.
- The selected coefficient set is quantized.
- The t_i values of the set are used to determine if the block is well textured and suited for watermark embedding.
- Depending on the bit value to be embedded, t_k and t_l must hold a predefined relationship. The condition for encoding a "1" bit is $t_k \geq t_l + d$, and the relationship for encoding "0" is $t_k + d \leq t_l$. If the required relationship does not occur, the coefficients are changed accordingly. This is equivalent to overlaying a 2D-cosine pattern on the original block data. Adjusting the noise level d (the difference) one can scale the impact of the pattern on the block's visual quality in the pixel domain.
- The changed coefficients are multiplied by the quantization value at the corresponding position of the quantization matrix and embedded into the DCT transformed block. The block data is inverse DCT transformed to the spatial domain, and the altered one replaces the original block in the image.

To increase the watermark's robustness, the watermark is embedded with maximum redundancy. All available blocks are used.

The retrieving process is symmetrical to the embedding one. The key is needed to find the correct sequence of blocks and the coefficients within these blocks. These coefficients are evaluated, and if a pattern from the predefined set is found, the corresponding bit value is recorded. If no valid pattern is found ($t_k = t_l$) the bit is marked as not readable.

7. Description of E.P.F.L algorithm

This technique embeds single signature bits by exploiting the low sensitivity of the human visual system (HVS) towards changes of high frequencies and blue colors [7,8]. The bit embedding process modifies pseudo-randomly selected pixels in the blue image component. The pixel modifications are proportional to the luminance and the signature bits determine the signs of the modifications, leading to the relation $B(i,j) \leftarrow B(i,j)+(-1)^b \cdot \alpha \cdot L(i,j)$, where B(i,j) is the blue pixel, b, the signature bit, α, the scaling factor, and L(i j), the luminance. Robustness is achieved through multiple signature embedding. This not only increases robustness towards image attacks such as filtering, but also allows signature retrieval after image alterations such as translation, cropping and rotation. To retrieve the signature from a signed image, an estimate of the embedded watermark is computed using a cross-shaped prediction filter. Then the bits are extracted using hypothesis testing. A key is used to determine the pseudo-random locations. For the benchmarking $\cdot\alpha\cdot$ was set to 1/5, and 80% of all pixels were modified.

8. Description of U.C.L algorithm

The picture is divided into 8x8 pixel blocks, and one bit is embedded in each block [9]. The first step consists in dividing the blocks in three different zones: Zone "1", "2" and "0", depending on their features (edges, textures
pixels that will not be modified. Zone "1" and "2" are then divided into two parts. Four categories of pixels are then created. The mean value of the categories is modified according to a pattern in order to embed the bit:

$$M10 = M11 + \alpha . level$$
$$M20 = M21 + \alpha . level$$

Where M10, M11, M20 and M21 are the categories mean values, $\alpha . = \pm 1$ if bit is 0 or 1, and level is a parameter. The mean value of the block must remain unchanged. When decoding, the picture is divided into blocks, and categories using the same features. The bit is extracted by comparing the mean values of the categories.

9. Conclusion

In this section, the four watermarking algorithms considered in the framework of the OCTALIS project have been presented. Two techniques use the frequency domain, while the two others work in the spatial domain. The next section presents the benchmarking results of these techniques using hybrid watermarking.

4. BENCHMARKING

10. Introduction

The robustness evaluation of the different watermarking algorithm is a key issue. The goals of this evaluation are as follows: (1) Test the robustness to "standard" image manipulations, such as gamma correction and cropping. Publishers often use these manipulations to enhance images. Watermarking algorithms should be resist to these "attacks". (2) Determine algorithmic parameters for a good robustness/invisibility tradeoff. In addition, subjective visual quality evaluations of the watermarked images are also performed.

Test conditions for the robustness evaluation are presented in Sec. 11, transformations applied on images are presented in Sec. 12, and benchmarking results are given in Sec. 13. Conditions for quality evaluation and results are given in Sec. 14. Finally, conclusions are given in Sec. 15.

11. Tests conditions, images, watermarks, and keys

We considered a set of ten images displayed in Figure 1. Image size, numbers of bits per pixel, and a short description of the images is given in Table 1. The set includes color and gray levels images, natural and computer generated images.
Three watermarks are embedded in each image, as described in the OCTALIS scenario [3]:

1. W1 is either the SHA (160 bits) or MD5 (128 bits) hash value of the image,
2. Wpub is a license plate of 64 bits.
3. W2 is a watermark of 32 bits.

Two different watermarks are used, referred as (a) and (b) in the following, in order to avoid special cases and unexpected correlation. The tests are repeated twice using different key, k1 and k2. These keys are used for W2. The keys for Wpub and W2 are derived from these ones, by adding 100 and 1000, respectively.
The following watermark-key combinations were used for the tests:

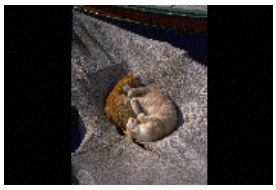
1. MD5 for W1 and watermark (a) for W2, key k1,
2. SHA for W1 and watermark (b) for W2, key k1,
3. MD5 for W1 and watermark (b) for W2, key k2,
4. SHA for W1 and watermark (a) for W2, key k2.

According to the CFM scenario, W1 and Wpub are embedded with the same algorithm, while W2 is embedded using a different method. All possible combinations between the four algorithms presented in Sec. 3 were tested.

Image Name	Size in pixels	Bits/pixel	Description
CATS	3072X2048	24	Two cats over a net
TOOLS	1524X1200	24	Collection of various tools
WATER	1536X1024	24	Landscape with water
Benz	640X480	24	Computer generated car
Diver4	640X480	24	Computer generated landscape
House	768X512	24	Landscape with house
Island	768X512	24	Tropical island
Parrot	768X512	24	Two parrots
sar1	1024X1024	8	Satellite view of Pentagon
Txtur2	1024X1024	8	Texture used for mapping on a mesh

Table 1: Size, number of bits per pixel, and description of test-images.

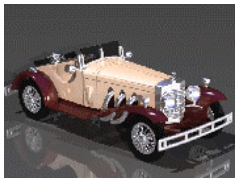
Figure 1: Images used for the robustness tests. Images are (a) “Cats”, (b) “Tools”, (c) “Water”, (d) “Benz”, (e) “Diver4”, (f)



(a)

(b)

(c)



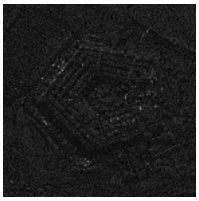
(d)

(e)

(f)

(g)

(h)



(i)

(j)

12. Transformations

The following transformations were applied to the images for robustness evaluation. Except for the hybrid watermarking, only those containing the three watermarks embedded with the same algorithm are considered for the transformations.

Hybrid watermarking	W2 is embedded with a different watermarking method.
JPEG compression	Quality factors are 75 % and 55 %.
Color reduction	Reduction from 24 to 8 bits per pixel.
Gamma correction	Factors are 0.6 and 1.5.
Scaling	Factors are 50 % and 150 %.
Rotation	Rotation of 5 ^{o} and 45 ^{o} are applied.

If the retrieving process failed, the inverse transformation was applied before reading the watermarks. Two sets of parameters were considered, corresponding to a non-invasive and an invasive transformation.

13. Robustness results

The results of the retrieving processes for each of the four algorithms are presented in Table 2 to Table 5, corresponding to the algorithms proposed by C.T.S, I.G.D, E.P.F.L, and U.C.L, respectively. In each table, the first row shows the names of the transformation and the corresponding parameters. An asterisk (*) at the end of the transformation name indicates that the inverse transformation was applied prior to the retrieving process. The second row lists the embedded watermarks. The third column displays the mean percentage of true retrieved bits and the fourth column shows the corresponding standard deviation. Please note that the tables contain only results of those tests, which were not 100% successful.

Hybrid		JPEG 75 %			JPEG 55 %			Color reduction			Gamma 0.6			Gamma 1.5		
W1	Wpub	W1	Wpub	W2	W1	Wpub	W2	W1	Wpub	W2	W1	Wpub	W2	W1	Wpub	W2
81.12	84.59	71.42	82.45	89.27	76.77	86.97	92.32	77.9	84.12	86.15	71.1	81.97	89.27	72.02	81.65	88.4
13.66	18.03	7.92	7.43	5.75	6.88	6.79	5.77	8.12	3.11	13.90	7.61	7.01	5.75	7.28	7.29	6.00

Scaling 50% (*)			Scaling 125% (*)			Rotation 5 ^{o} (*)			Rotation 45 ^{o} (*)		
W1	Wpub	W2	W1	Wpub	W2	W1	Wpub	W2	W1	Wpub	W2
64.75	82.95	83.05	70.22	81.82	88.45	71.25	81.8	87.75	71.05	81.55	86.57
5.87	7.14	5.15	6.97	7.81	5.56	7.42	7.57	5.82	6.80	7.71	6.05

Table 2: CTS robustness results.

JPEG 75 %			JPEG 55 %		
W1	Wpub	W2	W1	Wpub	W2
99.57	99.95	100	98.27	99.87	100
0.95	0.31	0	2.84	0.40	0

Table 3: EPFL robustness results[1].

JPEG 75 %			JPEG 55 %			Color reduction			Gamma 0.6			Gamma 1.5		
W1	Wpub	W2	W1	Wpub	W2	W1	Wpub	W2	W1	Wpub	W2	W1	Wpub	W2
93.75	100	98.1	87.77	96.77	93.1	99.02	100	100	97.37	100	99.22	97.65	100	99.52
12.26	0	4.82	15.87	7.38	13.1	1.79	0	0	4.26	0	2.39	4.41	0	1.50

Scaling 50% (*)			Scaling 150% (*)			Rotation 5 ^{o} (*)			Rotation 45 ^{o} (*)		
W1	Wpub	W2	W1	Wpub	W2	W1	Wpub	W2	W1	Wpub	W2
97.4	100	99.72	97.4	100	99.72	97.65	100	99.72	97.62	100	99.72
6.49	0	1.26	6.49	0	1.26	6.03	0	1.26	6.02	0	1.26

Table 4: IGD robustness results.

Hybrid		JPEG 75 %			JPEG 55 %			Colour reduction			Gamma 0.6		
W1	Wpub	W1	Wpub	W2	W1	Wpub	W2	W1	Wpub	W2	W1	Wpub	W2
90.18	90.68	97.39	91.79	95.46	92.89	87.61	92.26	94.35	89.45	92.96	92.93	87.81	91.09
20.45	17.12	6.10	12.76	8.06	7.74	11.88	7.81	12.96	16.82	12.31	16.69	20.18	17.13

Gamma 1.5			Scaling 125% (*)			Rotation 5 ^{o} (*)			Rotation 45 ^{o} (*)		
W1	Wpub	W2	W1	Wpub	W2	W1	Wpub	W2	W1	Wpub	W2
93.66	88.98	92.65	97.67	93.71	96.17	49.87	49.45	51.64	49.99	47.10	53.67
14.80	17.90	13.07	6.00	11.53	8.17	4.90	5.46	9.33	4.57	7.01	9.98

Table 5: UCL robustness results[2].

[1] No errors occurred for the EPFL method after scaling of 50% and 150%, and rotation of 5 ^{o} and 45 ^{o} degrees. As for the other methods, the inverse transformation was applied prior to the watermark extraction process.

[2] UCL didn't provide results for scaling at 50%.

The first obvious remark is that the robustness is algorithm dependent, and that no tested algorithm is able to retrieve a watermark after a scaling or rotation without applying the inverse transformation. Two algorithms, UCL and CTS, do not resist to hybrid watermarking (embedding W2 with a different algorithm destroys W1 and Wpub).
It should be noticed that so far the visual degradation due to the marking process has not been taking into account. However, for a fair comparison of the methods subjective quality tests are necessary.

14. Visual quality evaluations

The goal of the visual quality evaluation is not to define general conditions for watermarking algorithm comparisons, but to introduce a relative scale in order to determine if an algorithm is more aggressive than another one.
Subjective tests were performed for three images, “Benz”, “House”, and “Txtur2”. The images were printed on a high quality color printer [10]. “Benz” and “House” were printed with a resolution of 133 d.p.i., and “Txtur2” was printed with a resolution of 200 d.p.i. The four different algorithms were tested, using four possible sets of watermarks and keys.
The following recommendations, extracted from the JPEG tests [11], were used for the subjective evaluation. (1) The room should be well illuminated. If possible, the illumination needs to be indirect or diffuse so as not to produce a reflecting glare off the surface of the prints. (2) The original and four images, corresponding to the four algorithms and a specific watermark-key combination, were displayed per session. (3) Viewing distance should be the same for all the images. For “Benz” and “House”, the viewing distance was between 30 to 40 cm, and for “Txtur2” the distance was between 40 to 50 cm. (4) Display time should not exceed 1 minute for each set of four images.
Two different tests were performed. The first one gives a relative quality evaluation, and the second one provides an absolute quality measure.
First test: While displaying the images, the observer is asked to rank the images from best (rank 1) to the worst (rank 4).
Second test: While displaying the images, the viewer is asked to give an absolute note for each image. We use the Institute for Telecommunication Science metric [12], listed in Table 6.

Rating	Impairment	Quality
5	Imperceptible	Excellent
4	Perceptible, not annoying	Good
3	Slightly annoying	Fair
2	Annoying	Poor
1	Very annoying	Bad

Table 6: Absolute quality metric definition.

These two tests are complementary. It is possible that the algorithm ranked best in the first test has a non-acceptable absolute quality in the second test. In addition, two sets of observers were considered, the first one is composed of professionals, such as photographers, and the second one of non-professional. Table 7 to Table 10 show the results. The following naming convention was used. “128” and “160” define the length of W1. “
watermark W2. The keys are named k1 and k2. For example “Benz128k1a” means that the image “Benz” was watermarked with W1 equal to the MD5 hash value of the image, W2 equal to watermark (a), and key k1 was used for W1. The tables show the mean and standard deviation of the rates for each algorithm. Results from professional and non-professional viewers are listed separately. A total of 16 persons participated in the first test (8 professionals and 8 non-professionals), and 22 persons in the second test (11 professionals and 11 non-professionals).

Image Name	Test 1				Test 2			
	Professional		Non Professionnal		Professional		Non professional	
	Mean	Std	Mean	Std	Mean	Std	Mean	Std
Benz128k1a	2.25	1.488048	3.625	1.06066	2.363636	1.501514	1.454545	0.522233
Benz128k2b	2	1.309307	3.125	1.356203	2	1.264911	1.636364	0.924416
Benz160k1b	1.875	1.356203	3.125	1.356203	2	1.341641	1.727273	1.00905
Benz160k2a	2.125	1.552648	3.375	1.06066	1.727273	1.00905	1.818182	0.98165
House128k1a	1.875	1.125992	2.125	1.246423	3.272727	1.420627	3.727273	1.420627
House128k2b	1.5	1.069045	1.25	0.707107	3.272727	1.420627	4.090909	1.044466
House160k1b	1.75	1.38873	1.75	1.38873	3.545455	1.572491	4	0.774597
House160k2a	1.5	1.069045	1	0	3.363636	1.361817	4.272727	0.786245
Txtur2128k1a	1.25	0.46291	1.375	1.06066	3.454545	1.439697	3.363636	0.924416
Txtur2128k2b	2.125	1.356203	3	0.92582	2.818182	1.662419	2.090909	0.700649
Txtur2160k1b	3.125	0.991031	3	0.92582	3.090909	0.94388	2.272727	0.786245
Txtur2160k2a	3.25	0.886405	2.875	0.991031	3.181818	0.98165	2.545455	0.687552

Table 7: CTS subjective results.

Image Name	Test 1				Test 2			
	Professional		Non Professionnal		Professional		Non professional	
	Mean	Std	Mean	Std	Mean	Std	Mean	Std
Benz128k1a	2.625	1.06066	2.375	1.06066	2.454545	1.29334	2.545455	1.128152
Benz128k2b	2.5	1.195229	2.375	1.187735	2.454545	1.439697	2.363636	1.286291
Benz160k1b	2.375	1.06066	2.75	0.886405	2.454545	1.29334	1.909091	0.831209
Benz160k2a	2.625	1.187735	2.375	1.187735	2.272727	1.103713	2.181818	1.07872
House128k1a	3.125	1.125992	3.375	0.744024	2.363636	1.286291	2.454545	1.439697
House128k2b	3.375	0.744024	3.25	1.035098	2.363636	1.286291	2.363636	1.433369
House160k1b	3.375	0.744024	3	0.92582	2.272727	1.190874	2.272727	1.3484
House160k2a	3.375	0.744024	3.375	0.916125	2.272727	1.190874	2.363636	1.286291
Txtur2128k1a	3.75	0.46291	3.125	0.64087	2.181818	1.32802	1.818182	0.603023
Txtur2128k2b	3.25	0.886405	2.875	0.64087	2.363636	1.433369	1.909091	0.700649
Txtur2160k1b	3.25	0.707107	2.75	0.707107	2.272727	1.3484	2	0.774597
Txtur2160k2a	3.125	1.125992	2.625	0.744024	2.272727	1.3484	2	0.774597

Table 8: EPFL subjective results.

Image Name	Test 1				Test 2			
	Professional		Non Professionnal		Professional		Non professional	
	Mean	Std	Mean	Std	Mean	Std	Mean	Std
Benz128k1a	2	1.069045	2.125	0.64087	2.636364	1.120065	2.636364	0.6742
Benz128k2b	2.75	1.035098	2.625	0.744024	2.636364	0.924416	2.363636	0.504525
Benz160k1b	2.875	1.125992	2.375	1.06066	2.454545	1.035725	2.727273	0.467099
Benz160k2a	2.375	1.187735	2.375	1.06066	2.818182	0.873863	3	0.894427
House128k1a	2.375	1.06066	2.5	1.309307	2.909091	1.136182	3	1.183216
House128k2b	2.75	1.035098	2.75	1.164965	2.363636	0.924416	2.727273	0.904534
House160k1b	2.125	0.64087	2.5	0.755929	2.636364	1.120065	2.727273	0.904534
House160k2a	2.5	0.92582	2.375	0.517549	2.636364	0.924416	3	0.774597
Txtur2128k1a	1.75	0.46291	2.75	0.886405	2.818182	1.401298	2.090909	0.700649
Txtur2128k2b	2.25	1.28174	1	0	3	1.183216	3.545455	0.8202
Txtur2160k1b	1	0	1	0	3.454545	1.368476	3.363636	1.120065
Txtur2160k2a	1.25	0.707107	1	0	3.454545	1.368476	3.545455	0.8202

Table 9: IGD subjective results.

Image Name	Test 1				Test 2			
	Professional		Non Professionnal		Professional		Non professional	
	Mean	Std	Mean	Std	Mean	Std	Mean	Std
Benz128k1a	3.125	0.64087	1.875	0.991031	2.363636	1.120065	2.909091	1.044466
Benz128k2b	2.75	1.035098	1.75	0.707107	2.454545	1.128152	3	0.894427
Benz160k1b	2.875	0.834523	1.75	0.886405	2.636364	1.120065	2.727273	1.00905
Benz160k2a	2.875	0.353553	1.875	0.834523	2.363636	1.206045	2.727273	1.00905
House128k1a	2.625	1.06066	2	0.755929	2.636364	1.120065	3.090909	1.044466
House128k2b	2.375	0.916125	2.75	0.46291	2.727273	1.272078	2.909091	0.700649
House160k1b	2.75	1.035098	2.75	1.164965	2.818182	0.98165	2.727273	1.00905
House160k2a	2.625	1.06066	3.25	0.707107	2.636364	1.026911	2.909091	0.94388
Txtur2128k1a	3.25	0.46291	2.875	1.125992	2.363636	1.286291	2	0.894427
Txtur2128k2b	2.375	0.744024	3.125	0.991031	2.727273	1.489356	1.909091	0.700649
Txtur2160k1b	2.625	0.744024	3.25	0.886405	2.545455	1.29334	1.909091	0.700649
Txtur2160k2a	2.375	0.517549	3.5	0.534522	2.636364	1.361817	1.909091	0.700649

Table 10: UCL subjective results.

The second test shows that the watermarks are visible in most images. It should be noticed that more than 200 bits were embedded in each image. Hence, the visual quality of the watermarked image cannot be excellent. It is interesting to note that the visual quality is image dependent and that no algorithm has superior performance for all images. Performing further comparisons is hard because of the standard deviations. Embedding 250 bits seems a maximum for images of 1000x1000 pixels.

15. Conclusion

The results presented in this section show that the resistance of the watermarking techniques is different, and depends on the image and the attack. Only two of the tested methods, namely EPFL and IGD, resist to hybrid watermarking. The quality of the watermarked images is in general between “fair” and “poor”. The benchmarking showed that the OCTALIS CFM is functional, but that the employed techniques must be tested, in order to evaluate their resistance to hybrid watermarking. In addition, in order to obtain an acceptable image quality, image trading must be done with images of acceptable sizes. As a last remark, improvements of watermarking techniques are still necessary, regarding the resistance to standard transformations.

5. CONCLUSION

In this paper the Common functional Model for image trading, developed within the OCTALIS project, has been presented. Emphasis has been given to the solution of hybrid watermarking solving some security problem. It has been shown how this method allows IPR protection, data authentication, and image tracing. In order to study of the feasibility of this scenario, four watermarking algorithms have been tested. The goal of this benchmarking was to determine parameters of the CFM, and to evaluate the robustness of the techniques. The tests showed that no method resists to geometrical transformations and that all of them require the computation of the inverse geometrical transformation prior to the watermark extraction process. Subjective quality evaluation showed that the quality of the largely images is decreased due to the watermark embedding process. Considering the overall performance, no tested method is satisfactory. It should be noticed that the conditions under which the benchmarking were performed were extreme. Over 200 bits were embedded in each image.

The results show that the OCTALIS solution for image trading over an insecure network is functional, but with some limitations due to the watermarking techniques. Watermarking techniques must first be tested in order to evaluate their resistance to hybrid watermarking. In addition, to obtain an acceptable quality the images must not be too small. As a last remark, improvements of watermarking techniques are still necessary, especially regarding the resistance to geometrical transformations.

As a last remark, for fair benchmarking clear evaluation rules and strategies are required. Besides testing the watermark robustness, subjective or quantitative evaluation of the image quality is of high importance.

6. REFERENCES

1. TALISMAN ACTS European project AC019. Home page http://www.tele.ucl.ac.be/TALISMAN/
2. OKAPI ACTS European project AC051. Home page http://ns1.tele.ucl.ac.be./OKAPI/
3. OCTALIS ACTS European project AC242. Home page http://ns1.tele.ucl.ac.be./OCTALIS/
4. S. Craver, N. Memon, B. L. Yeo, and M. Yeung. “Can Invisible Watermarks Resolve Rightful Ownership? ”, 1996.
5. Mitchell D. Swanson, Mei Kobayashi, and Ahmed H. Tewfik. “Multi-media data-embedding and watermarking technologies”. In Proceedings of the IEEE, Vol. 8, No. 6, pp. 1064-1087, June 1998.
6. J. Zhao and E. Koch. “A digital watermarking system for multimedia copyright protection”. In Proceedings of ACM Multimedia, November 1996.
7. Martin Kutter, Frédéric Jordan, and Frank Bossen. “Digital signature of color images using amplitude modulation”. Journal of Electronic Imaging, vol. 7, no. 2, pp. 326-332, April, 1998.
8. Martin Kutter. “Watermarking resisting to translation, rotation and scaling". Proc. of SPIE, Boston, USA, November, 1998.
9. Edited by Benoît Macq and Ionnas Pitas. “Special issue on watermarking”. Signal processing, Vol. 66, No. 3, May 1998.
10. http://www.fujifilm.com/home/sbu/electimg/ei_p_p3.htm
11. “Evaluation plan for JPEG 2000: Image coding system”. IOS/IEC JTC1/SC29/WG1/N557, 1997.
12. “Method for the subjective assessment of the quality of television pictures”, 13-th plenary assembly, recommendation CCIR-500, Vol.11, pp. 65-68, 1974.