CERTIFICATION WATERMARKING FOR DIGITAL HANDHELD-CAPTURED PHOTOGRAPHY

Yves Stadler[1,2]
[1]*CodaSystem France, 79 rue de Sèvres, 92100 Boulogne-Billancourt, France*

Yann Lanuel, Anass Nagih, Francine Herrmann
[2]*Laboratoire d'Informatique Théorique et Appliquée, University of Metz, Ile du Saulcy, 57045 Metz Cedex 1, France*

Keywords: Image watermarking, Handheld device, Certification, Information security, Geolocation.

Abstract: In digital world, photography lost its legal value due to the massive usage and the ease of modifications. This paper presents a watermarking technique which adds a proof of validity to a smartphone-captured photography. By analysing the context of provability issues (attacks, impacts and objectives), the authors derives requirements. The constraints of the domain leads to the specification of a semi-fragile algorithm, which embeds pieces of information like geolocation or timestamp to insure the provability. An evaluation of the process shows the cryptographic robustness of the algorithm.

1 INTRODUCTION

The development of smartphones and the all-surrounding communication networks have modified the handheld's usages. Besides, society-driven interests, *e.g.* sustainable development, lead to paperless office work. In that environment it is more convenient for company to provide their employees with multiple functions devices, which enables them to collect and report field information. Mass market users have contributed to the migration, as an example, by using their devices as electronic wallets. To summarise, handheld devices profits their communication capabilities to send and receive information. But with the lack of information support, there is a problem to take care of: the proof strength of the evidence. With analogue photography, it is fair to consider the shot of the clock tower timestamped and geolocalised. But in the digital world, this obviousness is unclear. Because of the ease of digital manipulations, the proof value of digital evidences becomes none. This article will present a digital-photography cetification-dedicated method for handheld-devices snapshots.

Three constraints have to be met:

- Process has to be cryptographically safe;
- Process has to be adapted to device capabilities;
- image must still be usable, with not too much degradation.

It must be raised, that confidentiality is not targeted. The owner must retain viewing capacity, but the copy have to be considered as original. This makes distinction between the presented watermarking and copy-control system or digital right management.

This article will firstly present a state of the art of watermarking techniques. This part will remind some required definitions and properties, show an overview of security in watermarking techniques and present a context specific attack model. In a second part, we will describe a way to produce certified documents from digital picture taken from mobile equipment. This includes describing the mark, stating specifications and algorithm principles. Finally we will show the result provided by such an algorithm, in terms of security, invisibility, forgeries detection and time of execution.

2 WATERMARKING STATE OF THE ART

2.1 Definitions

As far as certification is concerned, watermarking

Stadler Y., Lanuel Y., Nagih A. and Herrmann F..
CERTIFICATION WATERMARKING FOR DIGITAL HANDHELD-CAPTURED PHOTOGRAPHY.
DOI: 10.5220/0003411305270534
In *Proceedings of the 1st International Conference on Pervasive and Embedded Computing and Communication Systems* (LOCSUE-2011), pages 527-534
ISBN: 978-989-8425-48-5

comes as an essential tool. But there are many kinds of watermarking techniques. As an illustration, in (Furon, 2002), the watermarking is highly bound to the signal processing and is tailored to protect the copy rights, thus the robustness is assumed. In this article, the watermarking definition will be based on the works of Cox *et al.* (Cox et al., 2008): ”watermarking [is] the practice of imperceptibly altering a Work to embed a message about that work” where the work is ”a specific song, video or picture – or to a specific copy of such”.

Mark detection or extraction process depends of the targeted watermarking-characteristics. If original work is required in such process, it is called an informed watermarking, else it is a blind watermarking (Kundur and Hatzinakos, 1999; Eggers and Girod, 2001).

Every watermarking modify the work (or host). However, the host has different formats (equivalent in term of information, but different presentation). As far as image is concerned, two major *insertion domain* can be considered. The *spatial* domain – like a bitmap – is a traditional visual representation, *a.k.a.* raw format. It is a three dimensional array in which the first two dimensions are position information, and the last is colour information. The most famous watermarking using this domain is the Mintzer-Yeung algorithm (Mintzer and Yeung, 1997) which has been further analysed by Fridrich *et al.* in (Fridrich et al., 2002). The second domain is called *frequential domain*. Many transform are used to convert a spatial representation to a frequential one. Interest of such techniques is to benefit the frequencies periodicity for compression purpose. As an example Lin and Chang use this domain to embed a mark in (Lin and Chang, 2000). For other algorithm using wavelets, readers can refer to (Kundur and Hatzinakos, 1999).

2.2 Properties

The principal property of a watermarking algorithm is *robustness* (Atupelage and Harada, 2008; Cayre et al., 2005; Furon, 2005; Lin et al., 2000; zgr Ekici et al., 2004; Rey and Dugelay, 2000). A watermark is called *robust* when it achieves a high degree of robustness, meaning that modifications do not erase the mark (thought they can degrade it). An example can be found in (Rey and Dugelay, 2000), where robustness is use to distinguish malicious manipulations of images. On the contrary a *fragile* watermark has the lowest robustness, as the watermark disappear with the slightest modification. That process is used by Wong (Wong, 1998) to verify authentication and integrity of a digital image. In between stands the *semi-fragile* watermark, which is robust to a finite set of modifications and fragile to all others. *Exempli gratia* (Lin and Chang, 2000), authors proposed a watermarking technique which is robust to JPEG compression.

$$PSNR = 10 \cdot \log_{10}\left(\frac{d^2}{EQM}\right) \quad (1)$$

$$EQM = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}||I_o(i,j) - I_r(i,j)||^2 \quad (2)$$

Figure 1: I_o original image, I_r watermarked image.

Watermarking an image consist in embedding new information into host, *id est* by modifying the host itself. Speaking of digital imagery, *imperceptibility*, as original quality preservation, is required (Fei et al., 2006; Kundur and Hatzinakos, 1999; Lin et al., 2000; Fridrich, 1998). It can be stated that watermark imperceptibility has to meaning: human eye imperceptibility and computer imperceptibility. In both case, the actor must be unable to distinct original image from watermarked image. A way to measure the imperceptibility is PSNR (*Peak Signal-to-Noise Ratio* - see 1 and (Petitcolas. and Anderson, 1999)). In signal processing community, it is admitted than 38dB is a good PSNR. As an example, the watermarking algorithm of Kundur and Hatzinakos (Kundur and Hatzinakos, 1999) provide a ratio of 43dB. *Insertion rate* is the amount of information which can be stored in an image watermark. It is also called *capacity*. In copy control scenario, the capacity may be low. On the contrary it must be high for indexation cases. Technics like *matrix embedding* proposed in (Fridrich and Soukal, 2006) are used to increase the capacity of a watermarking algorithm without increasing the image degradation. For embedded application (such as mobile equipment, video surveillance, *etc*), algorithms have to be adequate with the mobiles capabilities, and specifically for real-time applications. *Complexity* is the indicator that will measure the watermarking process fit (Atupelage and Harada, 2008; Fei et al., 2006; Fridrich, 1998). An analogy can be made with paper copies, within the process the screen imperfections can induce anomalies, but the legal value remains the same. This notion can be transferred to watermarking algorithms by the notion of *localisation*. The principle is to include integrity checking into the process (Atupelage and Harada, 2008; Lin et al., 2000). Detection can reveal defective areas and genuine areas.

2.3 Watermarking Algorithm’s Security

As we can see by the non-exhaustive enumeration of properties given in the previous subsection, most proposed watermarking-algorithms offer different tunable parameters. Before giving specifications, the context must be described.

2.3.1 CODASYSTEM's Context

CODASYSTEM sells certification software based on a secured infrastructure for digital handheld-captured media. With the photographies, CODASYSTEM's objective is making digital proof. The deployed solution is based on watermarking techniques which certifies the location, time and issuer information.

In this context, being able to visualise image without constraint is a requirement.

The certification process is divided in three subactivities:

- Capture phase: meta-data are gathered and inserted by watermarking in the image.
- Transmission phase: data are encrypted and sent via a network to storage.
- Storage phage: data are conserved for long term support and available to user.

The "certification chain" of CODASYSTEM is described by figure 2.

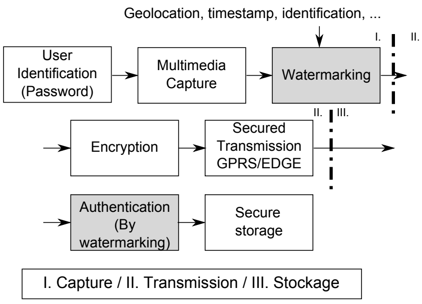
Geolocation, timestamp, identification, ...
I.
II.
User Identification (Password)
Multimedia Capture
Watermarking
II.
III.
Encryption
Secured Transmission GPRS/EDGE
Authentication (By watermarking)
Secure storage
I. Capture / II. Transmission / III. Stockage

Figure 2: CODASYSTEM's certification chain.

However, all these properties does not provide certification by using only watermarking. Cryptographic tools have to be used to protect meta-data. In fact, as it has been said by Cox *et al.* "Watermarking is not cryptography" (Cox et al., 2006). This is the protocol which involves the watermarking and provides the necessary cryptographic quality. To understand these needs, possible attacks on certified images will be presented.

2.3.2 Watermarking Attacks Classification

The literature provides many classifications (see as an example (Kutter et al., 2000)). Most of the presented attacks are grouped by strategies (geometric attacks, noising, etc.). These classifications are interesting so as to get a global overview. But, depending on context, information to embed, or to protect, varies much. Knowing the *impact* and the *potential benefits* of the attack are important to orient the protection effort. This paper propose a contextual classification ordered by risk family. It has to be remind that the current context is proof by image. A digital photography is captured by a device and embed information about author, geolocation, time and integrity. All attacks presented here have a common point: integrity of image. An attack which leads to integrity loss, fails.

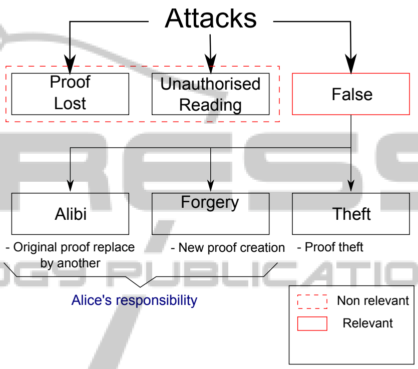

Figure 3: Attacks classification.

On figure 3, the first level describes three families of risk. Firstly, an attacker can choose to destroy (erase) embedded information. In this case, he obtains an non certified image (that is not exactly the same as the original since the watermarking algorithm is non reversible). This attack is not relevant because even if the attacker owns a copy with no certification, the original owner keeps possessing the original and certified photography. In the case of removing the mark from the original document, the problem does not concern the watermarking technique, but the secure storage. This is a strong issue, but is not in the scope of this document. Secondly, the unauthorized access to the mark is not wished, but this aspect is not a strong constraint. If the attacker succeed to read the embedded information such as geolocation or timestamp, nevertheless the image remains certified. These attacks do not belong to the scope of watermarking certification and many cryptography techniques can handle this problem very efficiently. Lastly, the false creation is very relevant and is the critical concern. If such a false certified document would be forged, the validity of the system is compromised. This family can be divided in three sub-objectives: alibi, forgery and theft.

To explain all cases of false and conflicts that can occur, some definitions are required.

- TS is the TimeStamp function. It has an order relation for its values. For all images x and y, if x has been taken before y, then $TS(x) \leq TS(Y)$ is true.
- Geo is the function of geolocation. It has an equivalence relation. For all images x and y captured at the same exact place, $Geo(x) = Geo(y)$.
- $Auth$ is the authentication function. If the image x belongs to user y then $Auth(x,y)$ is true.

The *theft* is defined by the production of a certified document with the intention of appropriating the image of the original author. In other words, a theft consist in putting the signature of the attacker instead of the signature of the original author. For example, Alice makes a photography of an event and certifies it for owning a valuable proof. Oscar who was not at that place, copies this photography and signs it with it's own signature. It is obvious that this new certified photography does not retain Alice's signature. Both owns a certified document. But, to succeed, Oscar must follow these steps:

- Copy the original.
- Erase Alice's signature (formula 3)
- Put his own signature (formula 4)
- Make the timestamp is previous than the original (formula 5)

That can be formalised by:

$$Auth(Image_{Oscar},"Alice") = Faux \tag{3}$$

$$Auth(Image_{Oscar},"Oscar") = Vrai \tag{4}$$

$$TS(Image_{Alice}) > TS(Image_{Oscar}) \tag{5}$$

Avoiding this kind of attack requires to protect two aspects: author authentication and timestamp of the capture. It is mostly the last point that requires the most attention in the certification process. Many works have already been focused on this issues, and have led to reliable protocols. In the certification process, we propose the use of a trusted third party which guaranties and conserves the authenticated document.

Creating an alibi consists in the forging of a false that belongs to the legitimate owner, but translated in time (to prove one's presence at a given place) or in space (to prove that something happened at a given time).

To build such a proof, Alice must at first create a mark at her name with a chosen original. Eventually, she can certified it with other information (formula 6). This condition is common to all type of alibi.

$$Auth(Image_{Alice},"Alice") = True \tag{6}$$

Secondly, Alice should modify the timestamp or the geolocation (formula 7 or 8).

$$TS(Image_{Alice}) \neq TS(Alibi) \tag{7}$$

$$Geo(Image_{Alice}) \neq Geo(Alibi) \tag{8}$$

As it has been evoked previously, reliable technical solutions are available to guaranty the authenticity and the timestamping. However, the geolocation remains unreliable nowadays. Jamming, spoofing and meaconning are relatively easy to set up. This will be described below.

Forgery consists in certifying a document with the identity of the victim. To implement this attack, Oscar must build a mark with the Alice's identity, and with a photo that she has not captured (formula 9).

$$Auth(Image_{Oscar},"Alice") = True \tag{9}$$

In this attack, the authentication system is the essential point to protect. The certification protocol shall not leak any information about the elements that has permit to Alice to authenticate her images. Current signature systems provide such a security.

To conclude, avoiding attacks presented above, one shall meet some requirements : embedding information as close as possible of the capture process, impossibility of forging a timestamp, impossibility of changing geolocation data, impossibility of impersonation. These security assessments lead to specify the certification algorithm, described in the following section.

3 CERTIFICATION WATERMARKING

As it has been described previously, the certification process is a sequence of operations which produces an image that leaves no doubt about geolocation, author and time. The image is considered an original and is stored in a trusted third party digital vault. In other words, information are embedded in such a way that making duplicates is easy and making fakes is difficult. This section presents the structure of the mark, describes more in detail the data capture, then the properties of the watermarking certification will be discussed. At last, technical aspects will be treated.

3.1 Mark for Certification

The host is both the asset to certify and the means to transport the evidence itself. Thus, this mark is composed of the bytes corresponding to the identity of the author, the authenticated timestamp and the geolocation. This set of data, so-called meta-data, represent a payload of almost 500 bytes.

However, the watermarking algorithm must ensure the host integrity. The goal is not to prevent copy, or the author identification, but to guaranty the conformity to original. Different works have covered the granularity of the integrity control. The lowest level consists in detecting any modification. At a higher level, it is possible to localise what has been modified. For this type of watermarking algorithm, Guillemot (Guillemot, 2004) compares the mark with a spy which will testify about the modifications that may have been made. The *pattern* is a set of information computed from the image, and are also inserted.

Meta-data are composed of critical information for the proof. This information must of course be reliable to ensure the legal value. As it has been discussed, securing the timestamp information is relatively easy. But, it is more complicated for geolocation. Technically, geolocation is computed from the signal of, at least, three GPS satellites (four without approximation). But these signals are weak and can be distorted easily, naturally or voluntarily. This becomes of critical interest because such jamming or meaconning devices can be obtain at a reasonable cost. The ongoing FP7 project ATLAS ((Roberts et al., 2010)) target the enhancement of geolocation reliability during image capture. It is declined in several scenarios:

- Indication of current Quality of service (QoS).
- Position enhancement and correction.
- Device integrity monitoring.
- Dedicated receiver.

The QoS indicator and the position enhancement are based on referenced ground stations, that will be compatible with Galileo system. Those services provide the user with the reception quality at its location, indicating him if he is being attacked or not. The integrity monitoring is used to testify that the signal received by the device has not been tampered with. It uses constant monitoring of GPS signal and other captors (GSM, WiFi, *etc.*). Finally, the external receiver can be used to gather more accurate signals than one provided by the phone.

3.2 Algorithm Specifications

Some properties appear to be critical to certification watermarking in the CODASYSTEMcontext. At first, *imperceptibility* is essential to provide user with images not degraded by the mark. As the amount of information to embed is important, the *capacity* must also be important. A trade-off between those two opposite properties is necessary.

A non-author user shall produce a copy of any proof he consult. This implies that a simple screen shot of a certified image shall retain the certification. Knowing that such an operation can lead to compression defects, the localisation properties is required for being able to distinguish a certified copy from a tampered photography. This cannot be achieve by a traditional signature process because of its fragility to all modification. The certification watermarking can be seen as a signature process. This signature must not resist to any modifications. However, since we want to allow to copy and to re-compress, the watermark should resists to this modification. So the algorithm has to be *semi-fragile*. As the re-compression may raise small errors (rounding of floats), the algorithm should make localisation possible, to distinguish malicious and non malicious errors. In other word, all the process must be integrated within the compression phase. The context imposes us to use JPEG format. So, the algorithm is based on this standard.

Then, the algorithm must provide security properties to resist the described attacks. So as to ensure this, geolocation and timestamp information are imported from reliable sources (Timestamping authority, ATLAS). The author owns a certificate with its private key to encrypt meta-data. The public key infrastructure for managing these certificates, is important to the system, but not in the scope of this paper.

3.3 Algorithm Principle

We remind that JPEG compression process 8x8 pixels blocks. After some stage of the compression process, these blocks are converted to a 8x8 Discrete Cosine Transform quantised coefficients block (DCT quantised block). The first of these coefficients is called DC and is never used for embedding (it would degrade the image too much). The others are the AC coefficients whose Least Significant Bits (LSBs) will embed the mark. The watermarking is made in such a way to minimise the impact on image quality.

The algorithm is divided in three stages.

Stage 1: Selection and Exclusion. This is a decision stage that will assign a block to integrity or message data. There are three cases: a block contains integrity information (pattern), contains meta-data or it does not meet the constraints that guaranty the invisibility of the embed. The tuning of this parameter is based on the following statement: when a block is homogeneous, it is composed of massive number of zero coefficients because he has low spatial variation. Those areas are not fit for watermarking since it will be too visible. In addition, watermarking this kind of block may leak information, leading to security flaw. This lead to the definition of the threshold notion in function of the number of zero in the quantised DCT block.

In this phase, the meta-data are divided in five bits chunks. Each chunk will be included in one block. All blocks not used for meta-data are used for the pattern. The selection of which information will be embedded in a block, is derived from the author's key. It is impossible to determine the type of embedding without that key.

Stage 2: Pattern Computation. The pattern of a block is a datum which reflects the visual content of a block. It is comparable to a hash, traditional cryptographic technique which provides integrity check. To embed a chunk of five bits (meta-data or pattern), the 31 first ACs of the block are considered. With the first five Most Significant Bits (MSBs) of each coefficients, a five bit parity number is computed. Combined with the datum to embed and the user key, it produces a cryptic information for embedding that is (approximately) similar to hashing functions. The cryptographic results are sufficient and the computation is fast. Furthermore, adding the authentication data makes it similar to HMAC digests. Each block embeds its own five bits pattern.

Stage 3: Insertion. The principle consists in modifying some bits within the 31 LSBs previously selected. The matrix embedding technique provides an extremely simple and non destructive method to embed five bits by modifying only one bit of those 31 LSBs.

4 EXPERIMENTAL RESULTS

4.1 Security Assessment

To evaluate the cryptographic robustness of the algorithm, it is necessary to determined the information known by the attacker. He knows the threshold value for the selection. He also knows that only one bit is modified to encode the five bits message. He has access to a decoder which takes an image and a key as parameters. This checker tells him true if all the blocks of the image are integrated with the provided key. In case of failure, he does not have the localisation of 3defective blocks.

In case of a theft, Oscar suppress Alice's authentication and watermark his own authentication information. To succeed he needs to embed an earlier timestamping information.

Table 1: PSNR measurements.

Nom	Desk	Babouin	F16	Poivron
PSNR (en dB)	48.88	48.77	48.89	48.79

In case of an alibi, Alice herself needs to determinate the repartition of pattern and meta-data blocks within her images. Once again she has to tamper with meta-data that come from trusted sources.

In both of those cases, each author embeds with it's own keys. Therefore the attacks are only of little difficulty and that is why the meta-data security is critical. The last case, forgery, is different. Oscar wants to assign to Alice a proof. It is supposed that Oscar has access to certified photography of Alice. To identify the key, he needs to call the decoder with a random key. The conditions of this attack are analogue to a collision search for an hash function. The key length must be sufficient to ensure a reasonable probability of collisions and deter from taking brute-force guess. If l is the key length, the birthday paradox (Wagner, 2002) indicates that $2^{l/2}$ tries are enough to have a $p = 1/2$ chance of having collision, *i.e.* guessing the right key. Nowadays, it is admitted than a $l \geq 256$ is sufficient.

4.1.1 Invisibility

References images (cited below) have been used to estimate the quality performance in term of invisibility.

- Baboon
- F16
- Pepper
- mobile taken photography

Quality compression parameters are Q=92 for the mobile device (fixed by the device) and Q=90 for the reference images. This rate of compression is a fine tuning to avoid compression artefacts. It will therefore be more easy to assess the watermarking defects.

The table 1 (formula 1) presents the results.

Average PSNR is 48.83dB which is very good for watermarking algorithm.

4.2 Integrity Check

The tests have been performed with the following protocol.

- Watermark the image
- Modify the image by logo insertion
- Mark extraction

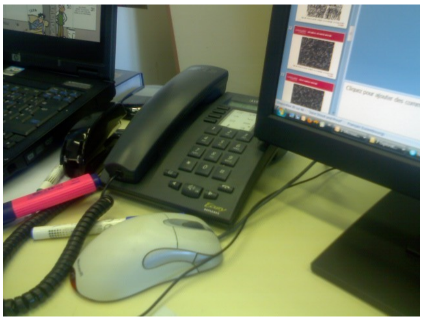

Figure 4: Modified image (a logo has been embedded).

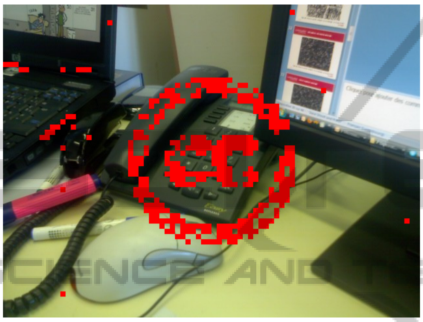

Figure 5: Integrity default (the logo has been detected).

The results (Figure 5) show that defaults in integrity check are detected where the logo has been included. It can be seen that some blocks appears to be defective. They are re encoding errors due to the rounding process in the JPEG compression.

4.3 False Key Checking

In this scenario, an image is decoded with a false author key (Figure 6). 96.95% of watermarked blocks are considered corrupted. These observations prove the efficiency of falsifications. This analysis, with local information of tampered blocs, is unavailable to the attacker, but for a forensics purpose (legal action for example) localisation is obviously important. The judge has the final word on whether he accepts or not the photography as a proof based on the number of unimpaired blocks. [1]

4.4 Execution Time

The table 2 presents the execution times of the algorithm on an ASUS P535 phone (specifications are available on the manufacturer website). The F5 algorithm is described in (Westfeld, 2001) and has been enhanced to fit mobility needs. The results has been obtained on 640x480 photography without sub-sampling. The algorithm that has been developed, shows improvement of five times compare to F5. Considering the time used for JPEG compression, the watermarking process time is compatible with handheld devices.

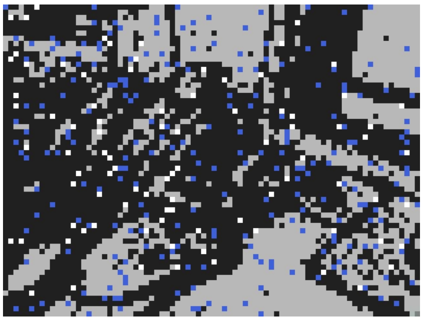

Figure 6: False key decoding.

Table 2: Execution times.

Mobile: ASUS			
F5	Certification watermarking		
	Total	incl. JPEG	incl. Tatouage
3.864	0.800	0.300	0.500

5 CONCLUSIONS

The evolution of mobile devices, in terms of technologies and software, has generated a change of usages in the status of broadcast information. This article has presented an algorithm which provides security to digital capture, in order to use them as proofs. The experiments had proven the good usability and fit of the process. A risk assessment has also been presented to justify the different features that has been selected in the specification process. This algorithm is semi-fragile and provides localisation of tampered areas. The security of the technique is based on the algorithm capacity of preserving integrity and the reliability of meta-data gathering.

Some future works can be foreseen. The first point is related to GNSS. These problems, stated in this article, are the major subject of the ongoing FP7 project ATLAS. A second perspective is the portage of such an algorithm to video. In fact, many standards are based on the same elements such as H.264 and MPEG, which use the Discrete Cosine Transform almost the same way as JPEG does. Nevertheless there would be new problematics, that is to say intra/inter predictions and flow control as an example. To finish with, the algorithm itself may benefits some improve-

[1] This observation is based on French laws.

ments. A good feature to be added would be the ability to use a wider range of recompression parameters within JPEG process without mark loss.

REFERENCES

Atupelage, C. and Harada, K. (2008). PKI based semi-fragile watermark for visual content authentication. *World Congress on Engineering and Computer Science*.

Cayre, F., Fontaine, C., and Furon, T. (2005). Watermarking security part one: Theory and practice. *Proc. SPIE*, 5681:746–757.

Cox, I. J., Dorr, G., and Furon, T. (2006). Watermarking is not cryptography. *Lecture Notes in Computer Science*, 4283:1–15.

Cox, I. J., Miller, M. L., Bloom, J. A., Fridrich, J., and Kalker, T. (2008). *Digital watermarking and steganography*. Morgan Kaufmann.

Eggers, J. J. and Girod, B. (2001). Blind watermarking applied to image authentication. In *IEEE International Conference on Acoustics Speech and Signal Processing*, volume 3. Citeseer.

Fei, C., Kundur, D., and Kwong, R. H. (2006). Analysis and design of secure watermark-based authentication systems. *IEEE Transactions on Information Forensics and Security*, 1:43–55.

Fridrich, J. J. (1998). Image watermarking for tamper detection. In *ICIP (2)*, pages 404–408.

Fridrich, J. J., Goljab, M., and Memon, N. (2002). Cryptanalysis of the yeung-mintzer fragile watermarking technique. *Journal of Electronic Imaging*, 11:262.

Fridrich, J. J. and Soukal, D. (2006). Matrix embedding for large payloads. *IEEE Transactions on Information Forensics and Security*, 1(3):390–395.

Furon, T. (2002). *Use of watermarking techniques for copy protection*. PhD thesis, Ecole Nationale Suprieure des Tlcommunications.

Furon, T. (2005). A survey of watermarking security. *Springer*, 3710/2005:201–215.

Guillemot, L. (2004). *Une approche vectorielle pour exploiter le contenu de l'image en compression et tatouage*. PhD thesis, Universit Henri Poincar, Nancy I.

Kundur, D. and Hatzinakos, D. (1999). Digital watermarking for telltale tamper proofing and authentication. *Proceedings of IEEE*, 87(7):1167–1180.

Kutter, M., Voloshynovskiy, S., and Herrigel, A. (2000). Watermark copy attack. In *Proceedings of SPIE*, volume 3971, page 371.

Lin, C.-Y. and Chang, S.-F. (2000). Semi-fragile watermarking for authenticating jpeg visual content. *SPIE int. soc. opt. eng.*

Lin, E. T., Podilchuk, C. I., and Delp, E. J. (2000). Detection of image alterations using semi fragile watermarks. In *PROC SPIE INT SOC OPT ENG*, volume 3971, pages 152–163. Citeseer.

Mintzer, F. C. and Yeung, M. M.-Y. (1997). An invisible watermarking technique for image verification. *International Conference on Image Processing*, 2:680.

Petitcolas., F. A. P. and Anderson, R. J. (1999). Evaluation of copyright marking systems. In *Proceedings of IEEE Multimedia Systems*, volume 99, pages 574–579. Citeseer.

Rey, C. and Dugelay, J.-L. (2000). Blind detection of malicious alterations on still images using robust watermarks. In *In IEE Seminar: Secure Images and Image Authentication*, pages 7–1.

Roberts, W., Stadler, Y., Herrmann, F., Lanuel, Y., and Larger, S. (2010). Delivering authenticated location within commercial lbs. *The European Navigation Conference on GNSS*.

Wagner, D. (2002). A generalized birthday problem. *Advances in cryptologyCRYPTO 2002*, pages 288–304.

Westfeld, A. (2001). F5-a steganographic algorithm: High capacity despite better steganalysis. *Lecture Notes in Computer Science*, Volume 2137/2001:289–302.

Wong, P. W. (1998). A public key watermark for image verification and authentication. In *Proceedings of the IEEE International Conference on Image Processing*, volume 1, pages 455–459. Citeseer.

zgr Ekici, Sankur, B., Coskun, B., Naci, U., and Akcay, M. (2004). Comparative evaluation of semifragile watermarking algorithms. In *Journal of Electronic Imaging*, volume 13, pages 206–216.