3rd International Conference on Automation, Control, Engineering and Computer Science (ACECS'16)
Proceedings of Engineering & Technology (PET)
pp. 841-845

Secure High Dynamic Range Images

Secure HDR Images

Med Amine Touil, Noureddine Ellouze
Dept. of Electrical Engineering
National Engineering School
Tunis, Tunisia
amine.touil@yahoo.fr

***Abstract*—In this paper, we propose a tone mapping algorithm to produce LDR (Limited Dynamic Range) images from HDR (High Dynamic Range) images. In our approach, we apply non-linear functions to compress the dynamic range of HDR images. Security tools will then be applied to the resulting LDR images and their effectiveness will be tested on the reconstructed HDR images. We describe in more details three specific examples of security tools: the first one addresses integrity verification using a hash function to compute local digital signatures, the second one considers the use of encryption for confidentiality, and the third one describes a scrambling technique.**

***Keywords*—tone mapping, integrity verification, encryption, scrambling**

I. INTRODUCTION

Thanks to recent advances in computer graphics and in vision, HDR imaging has become a new generation technology becoming a new standard representation in the field of digital photography. Advances in techniques, equipment acquisition and display, handsets with the powerful increasing of processors in professional and consumer devices, as well as the continued efforts to get content more photo-realistic with higher quality image and video; have attracted attentions to HDR imaging.

Nowadays, several industrials offer cameras and displays capable of acquiring and rendering HDR images. However, the popularity and the public adoption of HDR images are hampered by the lack of file formats, compression standards and security tools.

The problem of protection of visual privacy in digital image and video data has attracted much interest lately. The capacity of HDR imaging to capture fine details in contrasting environments, making dark and bright areas clear, has a strong implication on privacy. However, the scenarios of use are not fully understood. Indeed, there is no mechanism of protection of privacy specific to HDR representation. Currently, many challenges are open for research related to the intrusion in privacy for HDR images.

In this paper, we propose to develop mechanisms to protect privacy, suitable for HDR images, to minimize risks to the privacy and confidential information.

This paper is structured as follow. We first review the JPSEC standard in Section 2. We then talk about tone mapping in Section 3, we discuss three specific use cases dealing with integrity verification, encryption and scrambling in Section 4. We finally draw some conclusions in Section 5.

II. OVERVIEW

The protection of privacy is important in our civilization and is also essential in several social functions. However, this fundamental principle is rapidly eroding due to the intrusion tolerated by some modern information technology. In particular, the protection of privacy is becoming a central issue in the transfer of images through open networks and especially in video surveillance systems.

The digital images are distributed via the network so they can be easily copied and modified legally and/or illegally. In this spirit, there has been a strong demand for a security solution JPEG2000 images. To meet this demand, the JPEG [1][2] committee has created an extension of the JPEG2000 [3][4] encoder by integrating security tools such as integrity verification, encryption and scrambling. This extension is part 8 of standard JPEG2000 coder (JPEG2000 Part 8) designated by JPSEC. JPSEC [5][6] defines the framework, concepts and methods for the safety of JPEG2000. It specifies a specific syntax for the encoded data and provides protection JPEG2000 bit stream. The syntax defines the security services associated with the image data, the tools required for each service and how to apply its tools, and parts of the image data to be protected.

The visual privacy protection problem in digital image and video data generated a lot of interest lately. The HDR imaging capability to capture fine details in contrasting environments, making obvious dark and bright regions clearly has a strong involvement on the familiarity. However, the point at which the HDR representation affects privacy if used instead of the SDR (Standard Dynamic Range) is not yet clear. Usage scenarios are not fully understood. Indeed, there is no protection mechanism of the specific privacy HDR representation. Therefore, there are many open challenges of the intrusion-related research in privacy for HDR images.

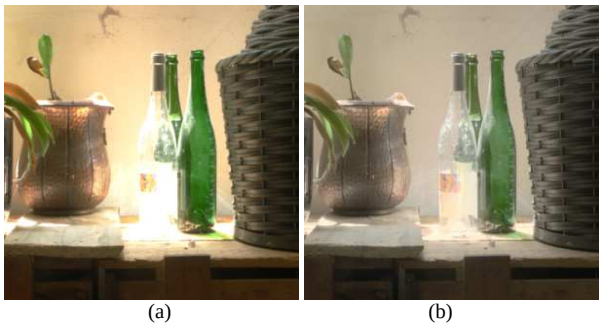
As part of this paper, we intend to develop mechanisms to protect privacy adapted to HDR images. These mechanisms should essentially meet the expectations of consumers concerned about the respect of their privacy and ethics.

ISSN: 2356-5608

III. METHODOLOGY

In this section, we propose a framework based on DCT (Discrete Cosine Transform) to secure HDR images offering similar features as those in JPSEC [5][6].

For tone mapping (Fig. 1), we apply sub-bands architectures [7] using a multi-scale decomposition with Haar pyramids splitting a signal s(x) into sub-bands which are rectified, blurred, and summed to give an activity map. A gain map is derived from the activity map using parameters which are to be specified. Each sub-band coefficient is then multiplied by the gain at that point, and the modified sub-bands are post-filtered and summed to reconstruct the result image.



(a) (b)

Fig. 1. Tone mapping
(a) HDR image, (b) LDR image

Hereafter, we describe in more details three specific examples of security tools: integrity verification, encryption and scrambling.

A. *Integrity Verification*

Integrity verification (Fig. 2) is used to guarantee the truthfulness of the image data. We consider the bit exact verification in this use case. We present a technique applied in the transform-domain based on a hash function and digital signature. More specifically, the DCT coefficients are hashed using SHA-1 [8], generating a 160 bits hash value. The latter is then encrypted by a public-key encryption such as RSA [9] to generate a digital signature. Obviously, other hash functions and encryption algorithms could be used as well. New hash values are computed and compared with those decrypted. When the digital signature is missing or when a hash value is not equal to the decrypted one, an attack is detected. Enabling to locate a potential attack, the integrity verification is performed for each macro-block.

Computing a single digital signature for the whole image allows for the verification of its integrity. Multiple digital signatures can be computed in order to be able to identify locations in the image data where the integrity is in doubt. For instance, a digital signature could be generated for each 8x8 DCT block. However, this may result in a very large number of digital signatures, and henceforth a large number of added bytes resulting in a non-negligible increase of the overall bit-rate. A digital signature can be generated for each macro-block composed of several DCT blocks as a compromise.

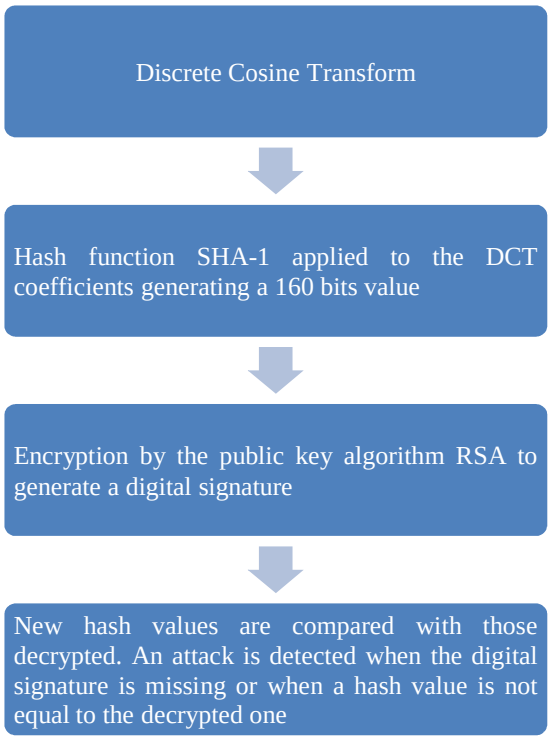
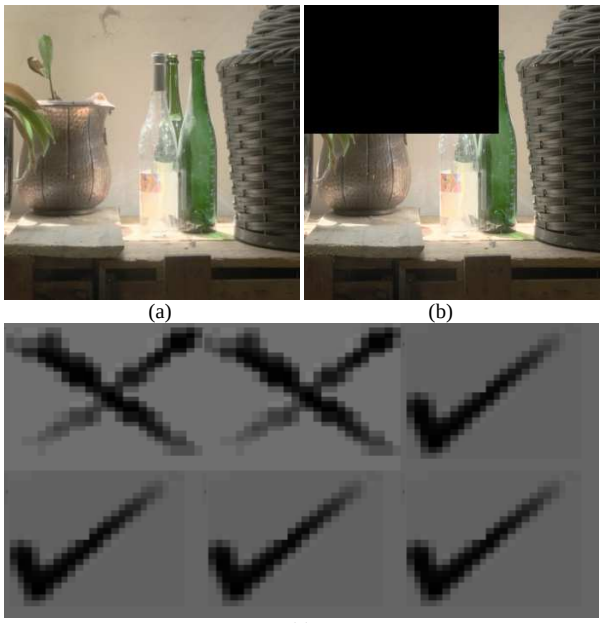


Fig. 2. Integrity verification

Fig. 3 shows an original image and a tampered version. Integrity verification is performed on macro-blocks composed of 100 DCT blocks, corresponding to square shaped regions of 80x80 pixels. It is possible to identify the attack in the upper left 160x80 pixels by comparing the hash values obtained from the original and tampered images.



(a) (b)

(c)

Fig. 3. Example of integrity verification
(a) original image, (b) tampered image, (c) digital signature verification

B. *Encryption*

For confidentiality, we now consider the use case of encryption (Fig. 4). The preferred approach is to apply encryption in the transform-domain. More specifically, encryption is applied on the quantized DCT coefficients. Authorized users are able to decrypt and recover the original data. In our example, we consider AES [10] encryption. The encryption can be applied on the whole image, or alternatively on ROI (Region of Interest) by restricting the encryption to selected DCT blocks.

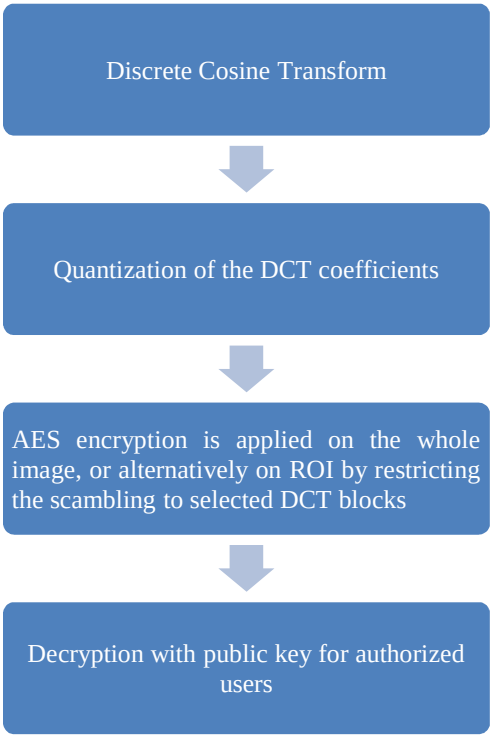
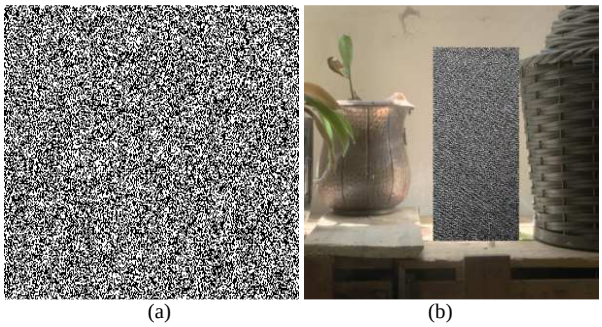


Fig. 4. Encryption

Fig. 5 shows two examples where an entire image or a ROI is encrypted. The shape of the encrypted region is restricted to match the 8x8 DCT blocks boundaries, and signaled to the decoder.



(a) (b)

Fig. 5. Example of AES transform-domain encryption
(a) whole image encrypted, (b) region of interest encrypted

C. *Scrambling*

Image and video data is characterized by a very high bit-rate and a low commercial value when compared to other types of information such as banking data and confidential documents. Conventional encryption techniques entail a significant complexity increase and are therefore not optimal in this case.

While keeping complexity very low, scrambling (Fig. 6) is an attractive alternative to protect image and video content. We consider a scrambling technique, in this use case, which can be effectively applied on the quantized DCT coefficients. Authorized users perform unscrambling of the coefficients allowing for a fully reversible process for them.

Scrambling consists in pseudo-randomly inverting the sign of quantized coefficients. The pseudo-random noise introduced in this way guarantee confidentiality. The amount of scrambling can be adjusted, by restricting it to fewer coefficients, and it can be applied on the whole image, or alternatively on ROI, by restricting it to select DCT blocks. The technique requires negligible computational complexity as it is merely flipping signs of selected coefficients. The shape of ROI is signaled to the decoder as in the previous case. Other extensions than flipping sign bits can be considered, such as flipping of least significant, or most significant bits of the quantized coefficients.

Initialized by a seed value, PRNG (Pseudo Random Number Generator) is used to drive the scrambling process. Multiple seeds can be used in order to improve the security of the system, and they are encrypted using RSA to communicate the seed values to authorized users.

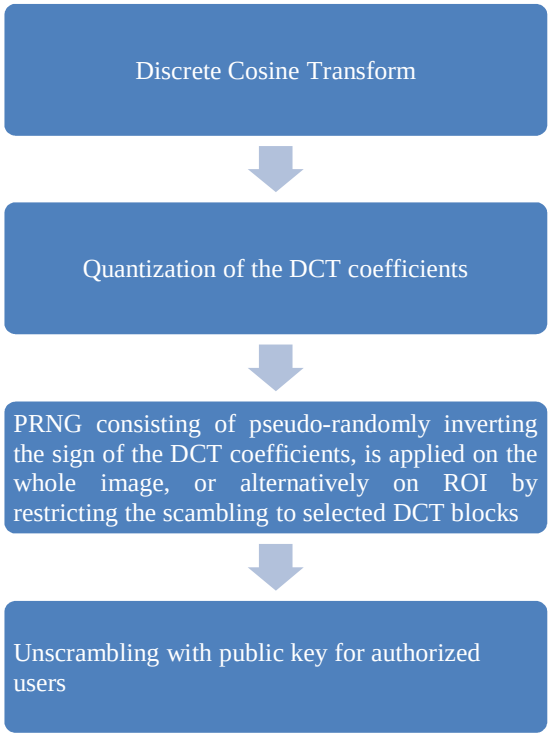


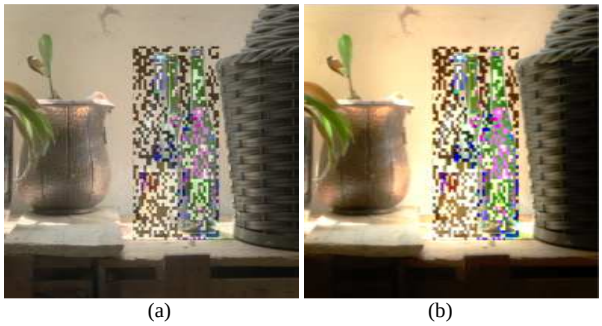
Fig. 6. Scrambling

Fig. 7 shows an example when either the whole image or a ROI is scrambled. The shape of the scrambled region is restricted to match the 8x8 DCT blocks boundaries.

(a) (b)

Fig. 7. Example of transform-domain scrambling
(a) whole image scrambled, (b) region of interest scrambled

Fig. 8 shows a reconstructed HDR image after inverse tone mapping of the resulting LDR image.



(a) (b)

Fig. 8. Inverse tone mapping
(a) resulting LDR image, (b) reconstructed HDR image

IV. CONCLUSIONS

In this paper, we introduced a hybrid system which consists of security tools to provide services similar to those provided by the standard JPSEC.

As illustrative use cases, we described in more details three specific examples of security tools: integrity verification, encryption and Scrambling techniques.

Indeed, our system allows the use of different tools in support of a number of security services.

As perspective, we propose to integrate the scrambling technique implemented in a video coding system adapted to HDR image sequences. Specifically, the scrambling process will be directly applied to the DCT coefficients after quantization and before entropy coding. At the decoder side, authorized users perform unscrambling (inverse scrambling) of the resulting coefficients of entropy decoding. Different results will be presented in terms of subjective and objective measure of the quality and scrambling force.

REFERENCES

[1] G.K. Wallace, “The JPEG Still Picture Compression Standard”, Communications of the ACM, vol. 34, no. 4, pp. 31-44, 1991.

[2] W.B. Pennebaker and J.L. Mitchell, “JPEG: Still Image Data Compression Standard”, Van Nostrand Reinhold, New York, 1993.

[3] A. Skodras, C. Christopoulos and T. Ebrahimi “The JPEG 2000 Still Image Compression Standard”, IEEE Signal Processing Magazine , vol. 18, no. 5, pp. 36-58, Sept. 2001.

[4] D. Taubman and M. Marcellin, “JPEG 2000: Image Compression Fundamentals, Standards and Practice”, Kluwer Academic Publishers, 2002.

[5] “JPSEC Final Draft International Standard”, ISO/IEC JTC1/SC29/WG1/N3820, Nov. 2005.

[6] J. Apostolopoulos, S. Wee, F. Dufaux, T. Ebrahimi, Q. Sun and Z. Zhang, “The Emerging JPEG 2000 Security (JPSEC) Standard”, in IEEE Proc. Int. Symp. on Circuits and Systems (ISCAS), Island of Kos, Greece, May 2006.

[7] Y. Li, L. Sharan, E. H. Adelson, Compressing and Companding High Dynamic Range Images with Subband Architectures, ACM Transactions on Graphics (TOG), 24(3), Proceedings of SIGGRAPH, 2005.

[8] FIPS PUB 180-1, “Secure Hash Standard (SHS)”, NIST, April 1995.

[9] R.L. Rivest, A. Shamir and L.M. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems”, Communications of the ACM, vol. 21, no. 2, pp. 120-126, 1978.

[10] FIPS PUB 197, “Advanced Encryption Standard (AES)”, NIST, November 2001.