Secure High Dynamic Range Images

Secure HDR Images

Med Amine Touil, Noureddine Ellouze

Dept. of Electrical Engineering
National Engineering School
Tunis, Tunisia

Abstract—**In this paper, a tone mapping algorithm is proposed to produce LDR (Limited Dynamic Range) images from HDR (High Dynamic Range) images. In the approach, non-linear functions are applied to compress the dynamic range of HDR images. Security tools will be then applied to the resulting LDR images and their effectiveness will be tested on the reconstructed HDR images. Three specific examples of security tools are described in more details: integrity verification using hash function to compute local digital signatures, encryption for confidentiality, and scrambling technique.**

Keywords—high dynamic range; tone mapping; range compression; integrity verification; encryption; scrambling; inverse tone mapping; range expansion

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.

In this paper, mechanisms suitable for HDR images are developed to protect privacy and to minimize risks to confidential information.

The structure of this paper is the following. The existing standard is first reviewed in Section 2. Three specific use cases are then discussed dealing with integrity verification, encryption and scrambling in Section 3. Some conclusions are finally drawn in Section 4.

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.

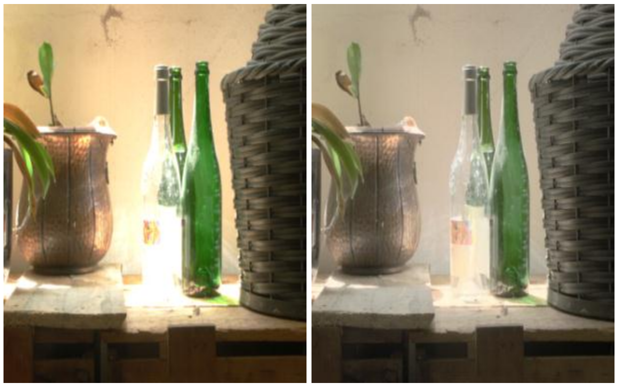
The problem of protection of visual privacy in digital image and video data has attracted much interest lately. The capacity of HDR imaging to capture fine details in contrasting environments, making dark and bright areas clear, has a strong implication on privacy. However, the point at which the HDR representation affects privacy if used instead of the SDR (Standard Dynamic Range) is not yet clear and 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.

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

III. Methodology

In this section, a system based on DCT (Discrete Cosine Transform) is proposed to secure HDR images.

For tone mapping (Fig. 1), sub-bands architectures [7] are applied using a multi-scale decomposition with Haar pyramids splitting a signal 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

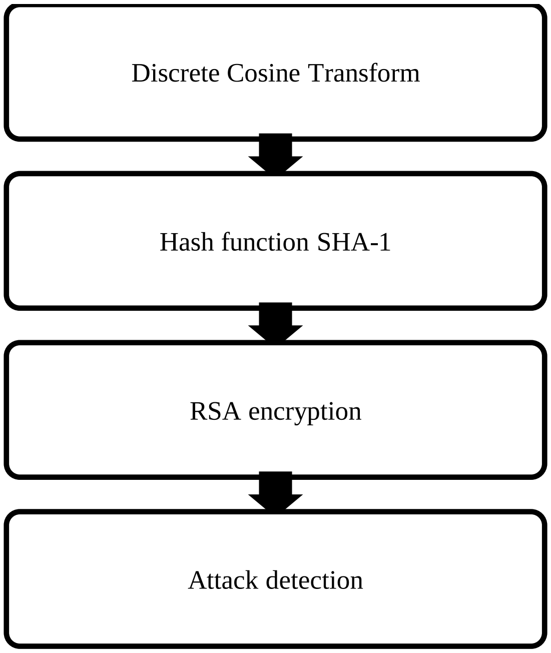
Hereafter, three specific examples of security tools are described in more details: integrity verification, encryption and scrambling.

A. Integrity Verification

To detect manipulations to the image data, the integrity verification (Fig. 2) is used where a bit exact verification is considered in this use case as a technique applied in the transform-domain based on hash function and digital signature. More specifically, hash function SHA-1 [8] is applied on the DCT coefficients generating a 160 bits value which is then encrypted by the public-key algorithm RSA [9] to generate a digital signature. It is possible to use other hash functions and encryption algorithms obviously. If new hash values computed and compared with those decrypted are not equal or if the digital signature is missing then an attack is detected. Enabling to locate a potential attack, the integrity verification is performed for each macro-block.

While a single digital signature is computed to verify the integrity of the whole image, multiple ones are computed to identify locations in the image data where the integrity is in doubt. As an alternative, a digital signature is generated for each macro-block composed of several DCT blocks not for each 8x8 DCT block because of a significant increase of the overall bit-rate resulted from a very large number of digital signatures and added bytes.

An original and a tampered image are shown in Fig. 3. Integrity verification is performed on macro-blocks composed of 100 DCT blocks corresponding to square shaped regions of 80x80 pixels. The attack is identified in the upper left 160x80 pixels by a comparison between the hash values obtained from the two images.



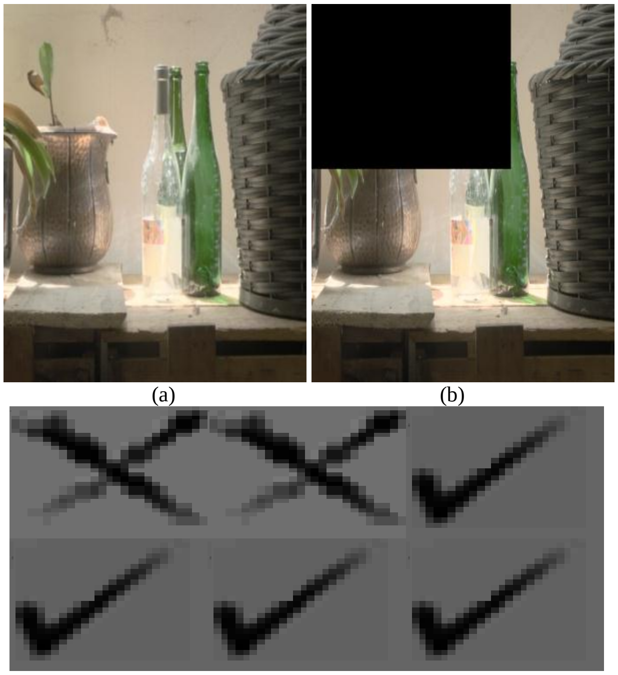
Discrete Cosine Transform

Hash function SHA-1

RSA encryption

Attack detection

Fig. 2. Flowchart of integrity verification



(a) (b)

(c)

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

B. Encryption

For confidentiality, the use case of encryption (Fig. 4) is now considered. 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. The whole image or alternatively the ROI (Region of Interest) AES [10] encryption is restricted to selected DCT blocks.

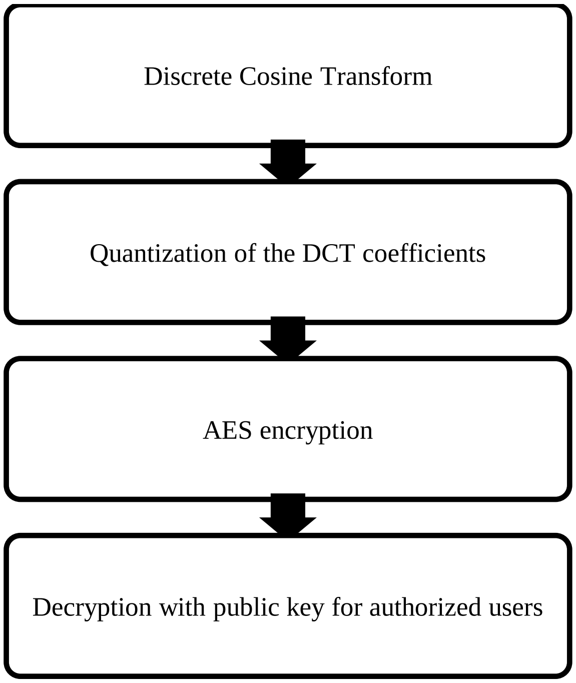
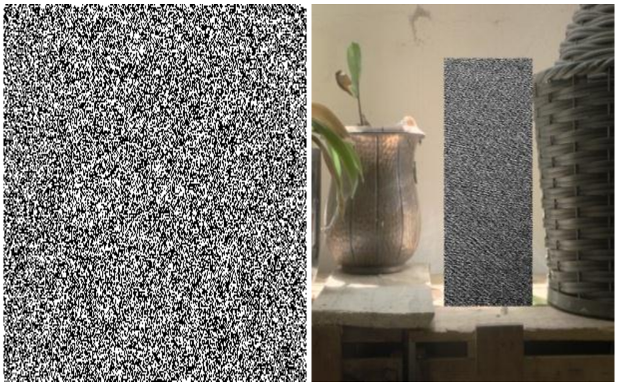

Discrete Cosine Transform
Quantization of the DCT coefficients
AES encryption
Decryption with public key for authorized users

Fig. 4. Flowchart of encryption

An example of a whole image or a ROI encryption is shown in Fig. 5 by restricting the shape of the encrypted region to match the 8x8 DCT blocks boundaries.



(a) (b)

Fig. 5. Example of encryption (a) whole image encryption, (b) region of interest encryption

C. Scrambling

Image and video content 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 non-negligible complexity increase and are therefore not optimal in this case.

While keeping complexity very low, scrambling (Fig. 6) is a compromise to protect image and video data. A scrambling technique applied on the quantized DCT coefficients is considered in this use case. Authorized users perform unscrambling of the coefficients allowing for a fully reversible process for them.

In the way confidentiality will be guaranteed, a pseudo-random noise consisting in pseudo-randomly inverting the sign of the quantized DCT coefficients is introduced. The whole image or alternatively the ROI scrambling is restricted to fewer DCT coefficients as in the previous case. The technique requires negligible computational complexity as it is merely flipping signs of selected DCT coefficients where other extensions such as flipping of least or most significant bits of the quantized DCT coefficients can be considered.

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

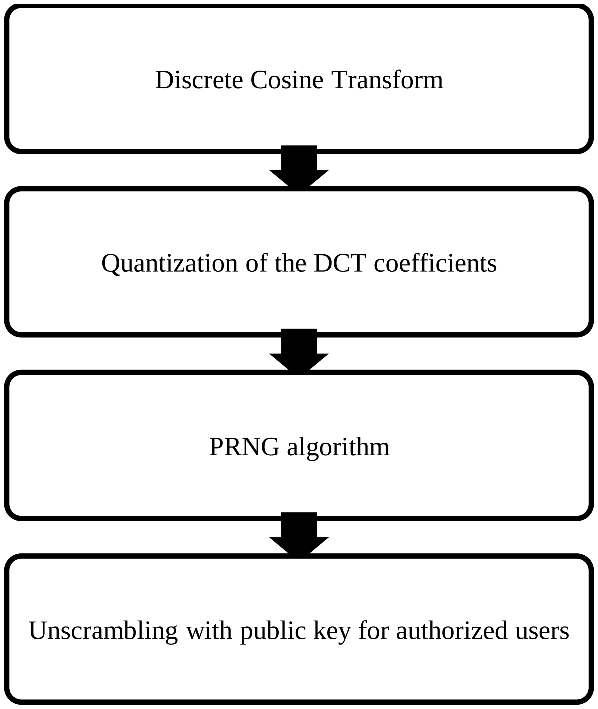

Discrete Cosine Transform
Quantization of the DCT coefficients
PRNG algorithm
Unscrambling with public key for authorized users

Fig. 6. Flowchart of scrambling

An example of a whole image or a ROI scrambling is shown in Fig. 7 by restricting the shape of the scrambled region to match the 8x8 DCT blocks boundaries.

A reconstructed HDR image is shown in Fig. 8 after inverse tone mapping of the resulting LDR image.

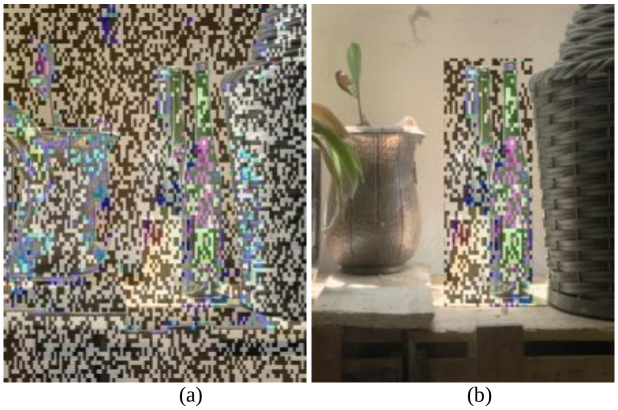


Fig. 7. Example of scrambling (a) whole image scrambling, (b) region of interest scrambling

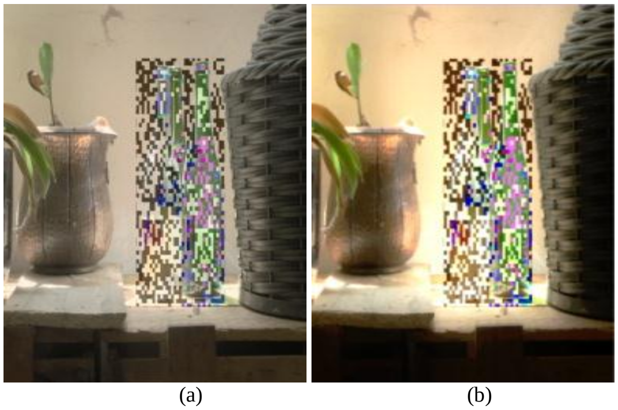


Fig. 8. Inverse tone mapping (a) resulting LDR image, (b) reconstructed HDR image

IV. Conclusions

In this paper, a system consisting of security tools was introduced to provide services similar to those in the standard JPSEC. As illustrative use cases, three specific examples of security tools are described in more details: integrity verification, encryption and scrambling techniques. Indeed, the system allows the use of different tools in support of a number of security services.

As perspective, the scrambling technique implemented will be integrated 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. Authorized users perform unscrambling (inverse scrambling) of the resulting DCT coefficients of entropy decoding at the decoder side. 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 and 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.