International Journal of Science and Engineering Vol.4 No.4(2014):19-23

Image encryption on HDR images for OpenEXR format

適用於 OpenEXR 格式的高動態範圍影像加密技術

Tzung-Her Chen

Department of Computer Science and Information Engineering
National Chiayi University
No.300 University Rd., Chia-Yi City
60004, Taiwan

thchen@mail.ncyu.edu.tw

Sheng-Shiang Chang

Department of Computer Science and Information Engineering
National Chiayi University
No.300 University Rd., Chia-Yi City
60004, Taiwan

shyangsnt@gmail.com

Abstract

The higher dynamic ranges can represented larger pixel values no longer under 255. Due to the new formats of HDR images, traditional image encryption for low dynamic range (LDR) images is not suitable for meeting the need of encryption of HDR images. Thus, HDR image encryption should be designed especially for its novel for-mat. To the best of our knowledge, this paper is the first research for OpenEXR HDR image encryption. After encryption, the encrypted results are compatible with commonly image applications like Adobe Photoshop, which are also called format-compliance

Keywords: *high dynamic range image, OpenEXR format, image encryption.*

摘要

高的動態範圍可以使得像素值不再侷限於 255 之內。由於高動態範圍影像的新格式，使得低動態範圍影像的影像加密法不能直接解決高動態範圍影像的加密的需要。因此，高動態範圍影像加密應當特別以其新穎的形式設計。據我們所知，本文是第一個對於 Open-EXR 高動態範圍影像的加密研究。加密後，加密的結果依然能被目前最常使用的影像處理軟體 Adobe Photoshop 正常讀取，這也被稱為格式相容。

關鍵詞：高動態範圍影像、OpenEXR 格式、影像加密。

Introduction

New format of image called high dynamic range (HDR) image appears to be a new choice for image record. Compared with the general common image format (low dynamic range images, LDR images) that people use today, HDR images can be used in more extreme situations. For example, some situation with photographs in LDR format in very bright area may result in an unrecognizable image that contains only white pixels. However, in HDR format, the deeper detail will be recorded with large range for image. Owing to the wider range of pixel value in HDR images, using HDR images is able to record more levels on color so that it also contains more color which is closer to what we see in real life. In past years, some researchers are focusing on the research on HDR images.

Despite the displaying technique or the image processing technique used, using HDR image has been a trend for future world. There are many formats in HDR image such as RGBE [11], LogLUV [12] and OpenEXR [7]. Among these three format, OpenEXR is the most widely used one today. For example, when using the image processing application of Adobe, users can set all parameter adjustment in Photoshop. Photoshop can also generate HDR image by input several LDR image automatically. For video,

*Corresponding author: thchen@mail.ncyu.edu.tw

DOI：10.6159/IJSE.2014.(4-4).04

OpenEXR is also used for making movies in many famous movies such as Harry Potter and the Sorcerers' Stone, Men in Black II, Gangs of New York, and Signs.

Faced with the first problem that great demand of transporting image through the Internet, there is a hot issue about how to protect image. With the open Internet, anyone who is malicious can eavesdrop or tamper the image data by a simple software easily. So making sure that the image data is secure becomes an important problem. At the thought of protecting data, the direct solution is encryption. In the past few years, a lot of methods of encryption have been proposed; for example, the extant encryption like Data Encryption Standard (DES) [1] and Advanced Encryption Standard (AES) [2]. Unfortunately, these kinds of encryption schemes are designed for text data. Unlike text data, image has a great amount of data. Using traditional encryption scheme will encounter with the problem that multimedia have to be fit in the real-time system to reach convenient system for user. Other problem is that image data have strong relationship on each pixel value. If encryption algorithm is not designed for image carefully, the security of encrypted image is still weak that malicious user can break the protection of encryption easily. In summary, the encryption of image should be designed with care. There are some encryption scheme description below. In Li's et al. [8] they used Elliptic curve and ElGamal to reach encryption scheme. Wei et al. [10] combined with DNA sequence operation and chaotic system. Jin [6] applied cellular automata to diffuse the positions of pixels. Still some researchers used chaotic scheme for all the research key-point [3]. Roughly speaking, among the same kinds of encryption methods, the only difference arise from the different chaos generator.

Although image encryption has been studied for a long time, until now there are only a few papers focusing on security issue on HDR image. Due to the trend that HDR will become the new image format standard, security of HDR image must also be put into careful consideration. Yu et al. [14] proposed the first research about data hiding on HDR images for RGBE format. In 2013, Huang and Wang [5] proposed a data hiding scheme with adjustment prediction for OpenEXR format in detail. The other issue on security is applying watermarking technique on HDR image. In Guerrini's et al. [4] scheme, it can against tone-mapping after watermarking was embedded into luminance component with HDR images.

In contrast, there is little researches on HDR image encryption that compared with researches of data hiding and watermarking. Only Lin et al. [9] and Yan et al. [13] proposed tailor-made encryption schemes on HDR images for LogLUV and RGBE format. Until now, no researches proposed encryption scheme on HDR images for OpenEXR format that is the most commonly used format today. Therefore, designing a novel encryption system suitable for OpenEXR format is an extremely urgent need.

To the best of our knowledge, no researches has been proposed on tailor-made HDR image encryption schemes, especially for OpenEXR format. In this paper we firstly propose HDR image encryption scheme for OpenEXR HDR image encryption. Moreover, proposed encryption algorithm is suitable for HDR image of OpenEXR format; in other word, it can still keep the same format as original HDR images do after encryption. That is called format-compliance. Encrypted results will not expand more size than the original HDR images. In our scheme we encrypt the significant parts in pixels' composition instead of modify the coding construction. Therefore, encrypted results have the same file size as original image.

Related works

It is well known that LDR image, such as BMP and JPG which use 8-bit format to store image data does not have enough detail on display. In other word, it is too narrow for the pixel range. Even using the larger bit likes 16-bit integer and 32-bit float point format, there still exists some problems; for example, it will not be correct in record HDR image data and it will use larger storage. Therefore, Industrial Light and Magic developed the HDR image format by their own named OpenEXR product that used 16-bit float. Among the 16-bit format in OpenEXR is following the 32-bit float point in IEEE-754 to simplify and fix. Because of the fact that 32-bit float point in IEEE-754 is called single-precision floating-point, 16-bit float point is called half-precision floating-point.

IEEE-754 half-precision floating-point format consists of sign bit, exponent bit and mantissa bit. Sign bit uses only one bit for recording the positive and negative numbers. Exponent bit uses five bits for recording the transform exponent. Mantissa bit uses ten bits for recording the precision mantissa. By combining the above three bits of Half-precision, it can obtain a floating number by transforming the data using IEEE 754 standard. Figure 1 show the IEEE 754 Half-precision floating-point format.

Figure 1 The structure of IEEE-754 half-precision floating point standard

Analysis of OpenEXR data can be divided into three parts: (1) Header, which records OpenEXR type data. (2) Data descript, which contains channel, bit information and other file detail. (3) Pixel value, Figure 2 is the result of transformation of OpenEXR file in the text editor which composites of three part on OpenEXR. In Figure 2, the red block is header. The second block in pink is data descript. The blue block records all the pixels value. As an ideal encryption scheme, it has to suit the format-compliant property. If encryption scheme destroy the format data by encrypting all image file including Header and Data descript, it will not be readable by any common program or software.

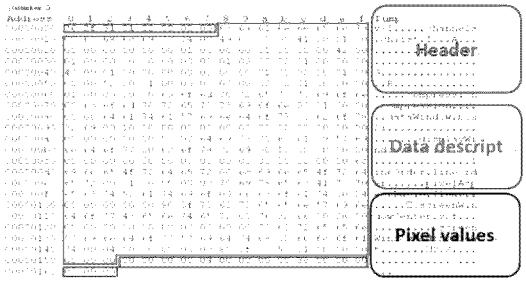

Figure 2 File structure of OpenEXR format

Proposed scheme

Due to the IEEE 754 standard, floating-point number needs be calculated by mantissa bits and exponent bits. Mantissa bits produce a small number in float point number under zero. That is to say, the range of mantissa bits changed is still under zero, which means the changes made by editing the mantissa is very tiny. The exponent bits is calculated by 2's exponential. It will changes very significantly when editing the exponent bits. Therefore the proposed scheme selects the exponent bits to encrypt. With a little encryption on pixels, it will obtain a dramatic change on the result. Figure 3 shows the proposed encryption structure on OpenEXR format.

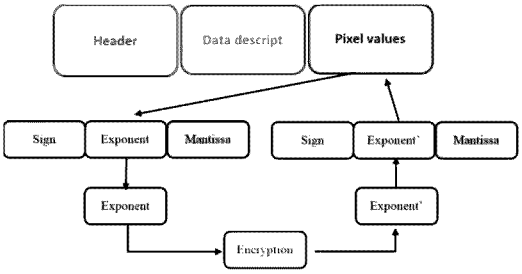

Figure 3 Proposed encrypting structure on OpenEXR format

After proposed encrypting process, the original image will be edited to generate encrypted one. Each step are listed below.

First, we define all parameter for encryption processing: input HDR image *I*, output HDR image *I'*, remainder array *rem [ ]*, exponent array *exp [ ]*, random stream *rs [ ]* and key *K*.

(1) Select the exponent bits of each pixel in each channel from original image *I*, and store the exponent bit in *exp [ ]*. The other part will be stored in *rem [ ]*.

(2) Use *K* to generate random stream *rs [ ]* which has the same length as *exp [ ]*.

(3) Calculate *exp' [ ]* by doing XOR operator with exponent bit *exp [ ]* and random stream *rs [ ]*.

(4) Reconstruct the pixel value by combining the encrypted exponent bit *exp' [ ]* and remainder bits *rem [ ]*.

(5) After editing the exponent bit, the encryption system will give the output encrypted image *I'*.

Experimental Results

In experimental process, the format of the tested image in propose thesis was "memorial" HDR image, using Dev-C++ to implement in the experiment platform. Coding was carried out on CPU Intel Core2 Quad Q8400 at 2.66GHz, the memory was packed with 2 GB, and the operating system was Windows XP. We selected the exponent bits to encrypt. The experimental results were showed in figure 4, the results showed that it also generated successfully encrypts of the original image.

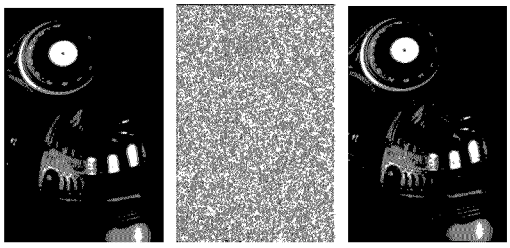

Figure 4 Experiment results of proposed encryption scheme

According to our encryption method proposed, encryption operate bit-wised exclusive-or between different lengths of encrypted parts. We showed all calculation time in table 1 including all image pixel, sign bit, exponent bits and mantissa bits. Intuitively, corresponding to longer length of encrypted part, full encryption have bad performance with longer calculation time. The encryption with the best performance is the one encrypted with sign bit. But encrypted result in figure 5 showed sign bit in float point number on turning pixel into black. In practice, pixel value has no display range in negative. The second calculation time is encryption with exponent bits. Encrypted result showed that it has a noise-like image which is more security than encrypted sign bit.

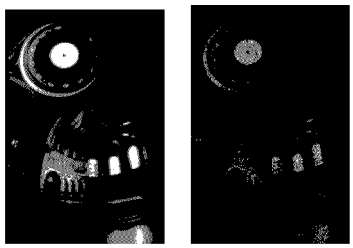

Figure 5 Experiment results of randomly encrypted sign bit

Table 1. The calculation time of encrypting difference part in each processing

Encrypted part	Calculation time (s)
All image pixel	0.503000
Sign bit	0.147000
Exponent bit	0.258000
Mantissa bit	0.442000

We listed all histogram with figure 6 and figure 7 from original image and encrypting result. Original image and encrypting result were divided into three channels including Red channel, Green channel and Blue channel. Each channel was then divided into three part including sign bit, exponent bits and mantissa bits. Due to the reason that floating point numbers have more ranges than those of the LDR images which only cover between 0 to 255, we set histograms of floating point number by using these three parts for easy representation.

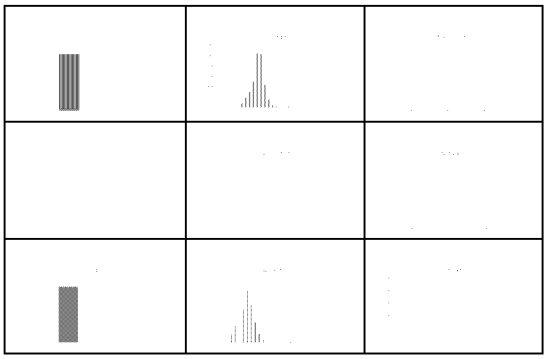

Figure 6 The histograms of original image.

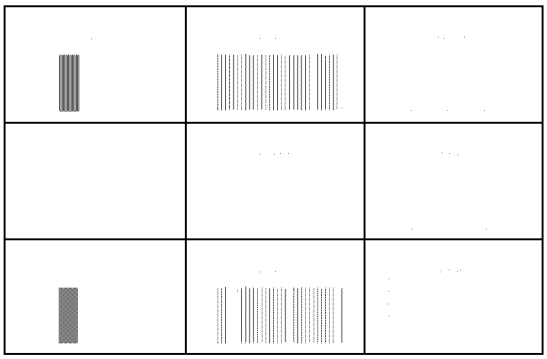

Figure 7 The histograms of encrypting results

Correlation analysis can measure the correlation of two adjacent pixels. Before encryption, the adjacent pixels always have higher correlation because the natural properties of images. After encryption, the correlation of two adjacent pixels will become very low. In other words, the encryption can decrease the correlation between any adjacent pixels. In table 2, correlation coefficient of pixels in original HDR image and encrypted HDR image is shown.

Table 2. Correlation coefficients of original image and between different encrypted processing

	Channel	Correlation
Original image	Blue	0.857295
	Green	0.849416
	Red	0.869511
Encrypted	Blue	-0.00176716

image	Green	0.00207284
	Red	-0.00106432

Conclusions

This paper proposed a novel encryption algorithm which is a specialized design for OpenEXR format. Via only tiny modifying on exponent bit, pixel values will be changed extremely. Compared with the full encrypted pixel values, selective encryption on exponent bits can reduce computational complexity. Moreover, proposed encryption is also suitable for HDR image of OpenEXR format. After the proposed encryption scheme, the encrypted image is still format-compliant. Experimental results and analysis showed that this scheme is feasible.

Acknowledgment

This work was partially supported National Science Council, Taiwan, R.O.C., under contract by NSC 102-2221-E-415-014 and NSC 102-2221-E-415-007.

Reference

[1] Data Encryption Standard, FIPS PUBS 46-2, 1993.

[2] Advanced Encryption Standard, FIPS PUBS 197, 2001.

[3] M. François, T. Grosges, D. Barchiesi, R. Erra, “A new image encryption scheme based on a chaotic function”, Signal Processing: Image Communication, Volume 27, Issue 3, Pages 249–259, 2012.

[4] F. Guerrini, M. Okuda, N. Adami, R. Leonardi, “High Dynamic Range Image Watermarking Robust Against Tone-Mapping Operators”, IEEE Transactions on information forensics and security, Volume 6, Issue 5, Pages 283-295, 2011.

[5] J. R Huang, C. M. Wang, “A reversible data hiding algorithm for high dynamic range images using the adjustment prediction”, Journal of Engineering, National Chung Hsing University, Volume 24, Numbers 1, Pages 37-64, 2013.

[6] J. Jin, “An image encryption based on elementary cellular automata”, Optics and Lasers in Engineering, Volume 50, Issue 12, Pages 1836–1843, 2012.

[7] F. Kainz, R. Bogart, “Technical Introduction to OpenEXR”, published by Industrial Light & Magic, pages 4-13, 2009.

[8] L. Li, A. Abd El-Latif , X. Niu, ”Elliptic curve ElGamal based homomorphic image encryption scheme for sharing secret images”, Signal Processing, Volume 92, Issue 4, Pages 1069–1078, 2012.

[9] K. S. Lin, T. H. Chen, C. H. Lin, S. S. Chang “A Tailor-Made Encryption Scheme for High-Dynamic Range Images”, Proceeding of the Seventh International Conference on Genetic and Evolutionary Computing(ICGEC 2013), Pages 183-192, 2013.

[10] X. Wei, L. Guo, Q. Zhang, J. Zhang, S. Lian, “A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system”, Journal of Systems and Software, Volume 85, Issue 2, Pages 290–299, 2012.

[11] G. Ward, “Real Pixels”, Graphics Gems II, pages 80-83, 1991.

[12] G. W. Larson, R. Shakespeare, “Rendering with radiance”, The Art and Science of Lighting Visualization, pages 267-275, 1998.

[13] J. Y. Yan, T. H. Chen, C. H. Lin, “Encryption in high dynamic range images for RGBE format”, Proceeding of The Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Pages 493-496, 2013.

[14] C. M. Yu, K. C. Wu, C. M. Wang, “A distortion-free data hiding scheme for high dynamic range images”, Displays, Volume 32, Issue 5, Pages 225–236, 2011.