Proceedings of the 5th International Conference on Computing and Informatics, ICOCI 2015 11-13 August, 2015, Istanbul, Turkey. Universiti Utara Malaysia (http://www.uum.edu.my)

Paper No. 220

AN APPROACH TO RESTRICT VIEWING OF MEDIA

Norazah Abd Aziz[1] and Raja Mohamad Fairuz R. Mohamad Yusoff [2]

[1]MIMOS BERHAD, Malaysia, azahaa@mimos.my
[2]MIMOS BERHAD, Malaysia, fairuz.yusoff@mimos.my

ABSTRACT. Nowadays, the issue of copyright infringement of media contents becomes more vital since the media content is published on the internet for easy access to users. Due to that, the authors' work affect adversely if their work can be copied or downloaded, modified or shared illegally by unauthorized users. In this paper, we proposed a method to restrict the viewing of images to control the media content accessibility. The method is using basic encryption scheme in order to prevent copyright violations, means, user who does not have specific player and/or with correct password can still view the grey-scale part of the media work in order to accomplish the marketing purposes. The encryption scheme integrates with certain properties such frequency and/or date time which will be used as a salt parameter for Password Based Key Derivation Function 2 (PBKDF2). The method also uses Color Lookup Table (CLUT) as an input to encrypt color table which the decryption process relies on the properties and the correct password.

Keywords: CLUT, PBKDF2, restrict viewing, media, image

INTRODUCTION

Since lately, media works such as images, video and music are published on the internet for wide distribution. The high demand for the media motivates copyright infringements because the media can be downloaded, copied and distributed without authorization easily. This scenario affects the authors and owners of the media revenue adversely. On the other hand, for promotional and marketing purposes, the media should be freely available for previewing by all. Therefore, methods are introduced to allow controlled view of the media. Most of the methods require use of a proprietary media player to view the media, by which media owner can enforce authorization information such as password or token to be presented to view the media in full.

This paper presents an approach to restrict the viewing of images by number of views or time range. Password is also deployed to demonstrate authorization has been obtained from owner of media. Users who view the image as preview or with expired authorization would see the image in a degraded form. In particular, the image is displayed with a modified colour lookup table. This paper starts with related work discussion. Next section briefly describes about the approach components, color lookup table and PBKDF2; and followed by the details description of the approach solution. The paper ends with a conclusion.

RELATED WORK

Due to the copyright infringement issue, Abdmouleh et al. intended that only specific software has the ability to decrypt the image can be used to view the image (encrypted image). They proposed an image encryption based on the chaos theory which uses the Logistic

Map function to generate a dynamic Look-Up Table (LUT). They produce encrypted image in “broken” image format. So, the encrypted image is very different from the original image. For fail decryption process, their method will produce another broken image. They have tested their method's cryptosystem and showed that it is resistant against the known plaintext attack (Abdmouleh et al., 2002). Unlike our approach, for failure decryption process, our method will produce the same image but in greyscale version.

Lu and Jin proposed a new method to protect image based on joint fractional Fourier transform correlator (JFRTC) and phase retrieval algorithm (PRA). Their method using fully-phase image encryption/decryption and protect by the fractional order as a new added key. Their method could be implemented through photo-electric system. They claimed the method's algorithm is simple and converges fast; and unauthorized users will be difficult to recover the decrypted image through blind de-convolution operations without accurate password (Lu and Jin, 2011). Our approach differs in that only color table will be encrypted/ decrypted using any symmetric-key schemes. Our decrypted image is alike the original because the same (original) color palette will be used if it is successfully decrypted.

Wong et al. has created a novel technique named Merged-Color Histogram (MCH). The MCH recover color to do an image retrieval, which includes images with color lookup table. They described that instead of using conventional RGB-based histogram, it is much cleaner way to recover color of the image by using the MCH. The MCH technique is trying to group a certain color and replace the broken color with the new shifted color (Wong et al., 2002).

Droogenbroeck and Benedett proposed another method to encrypt image whilst distorting minimally the visual of the image (Droogenbroeck and Benedett , 2002). Similar with our approach, they encrypt the component of the image without needing to encrypt the whole file. So, it produced visually acceptable encrypted image. They encrypt appended bits corresponding to preselected numbers of AC coefficients, to make the image looks distorted. This will result a viewable image but with lesser quality. But similar to our approach, we did not encrypt the image data (for JPEG, the image data is the compression and its wave length, while in GIF, there is a specific section of image data). This will reduce the computation time to decrypt since only a portion of image is encrypted.

BACKGROUND

This section describes components that used in our approach, Color Lookup Table and Password-Based Key Derivation Function.

Color Lookup Table (CLUT)

All images in the form of Indexed Media Format contain a colour lookup table. A CLUT is a solution to change a range of source colors to new range of colors. It can be built into graphics devices or image processing software (CLUT, 2015). In image processing, lookup table is used to define the intensity and colors values for particular displayed image. As definition, the lookup table is a simpler array indexing operation to replace runtime computation (Lookup table, 2015). The operation is retrieving a value from memory, so it can optimize processing time rather than input output operation. It is cost effective than using expensive computation. During initialization phase, the table may be precalculated, calculated as part of a program and saved in static program memory allocation. The lookup tables are also used to verify input values by matching the values with a list of valid or invalid items in an array. In a few programming languages, the pointer functions or offsets to labels may use to generate the matching input. In our method we modify the color lookup table in the image to produce the preview or unauthorized version of the image.

Password-Based Key Derivation Function 2 (PBKDF2)

PBKDF2 is a key derivation function in the RSA Laboratories' Public Key Cryptography Standard (PKCS) series (Kaliski, 2000). Given a password and a salt, the PBKDF2 produces 160-bit binary key after repetition for many times. PBKDF2 uses pseudorandom functions in its process. It generates a key and initialization vector (IV). The initialization vector (IV) is a non-repeating random number that used only once. We use this function in our method to make password cracking more difficult.

RESTRICT VIEWING OF MEDIA

Our approach is to provide a restrictive mechanism for the media data from being fully viewed by user. In other word, the unauthorized users can still view the image of the media but in degraded form (greyscale version). We also used a set time range or number of view to restrict the viewing of image. Figure 1 illustrated the example of images in degraded and original form.

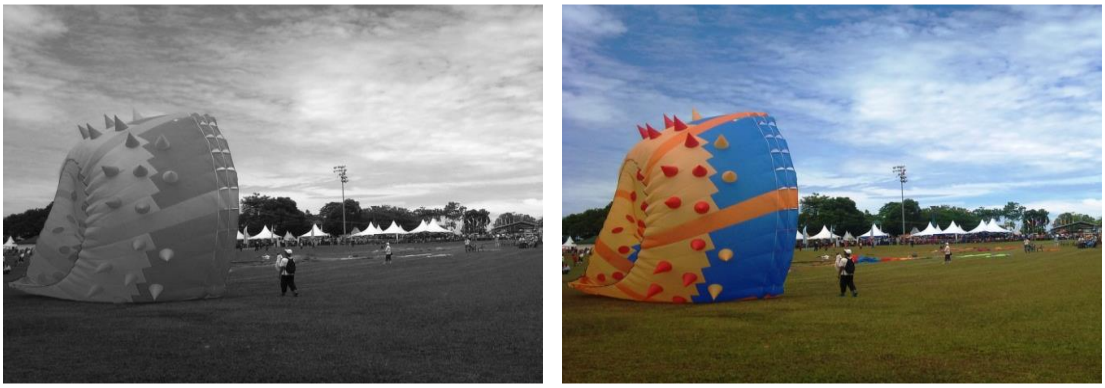


Figure 1. Left: Image in Degraded Form which Rendered by Un-Authorized User and/or Outside Allowed Frequency/Time Limit. Right: Image with Correct Password and Within Allowed Frequency or Time Range

In order to generate we utilized a media content information blocks. The media content contains multiple information blocks such as Images Block, Graphic Control Extension Block, Plain Text Extension Block and Application Extension Block. The blocks used in this approach are Transformed Color Lookup Table Block, Application Extension Block and Encryption Extension Block as shown in Figure 2.

Referring to Figure2, the CLUT block is modified for storing transformed CLUT. The Encryption Extension Block is created for storing attribute data and also a calculated attribute data identifier. The attribute data is the encrypted original CLUT and attribute data identifier is a calculated hash value and size of the original CLUT. The encrypted modified attribute data and identifier are retrieved from the Encryption Extension Block during the decryption of the media content.

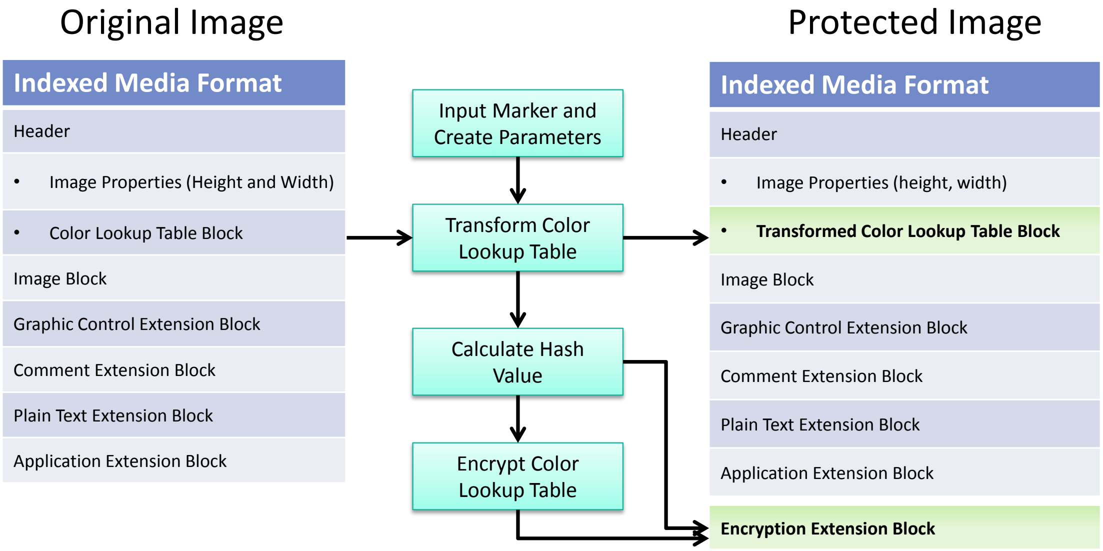
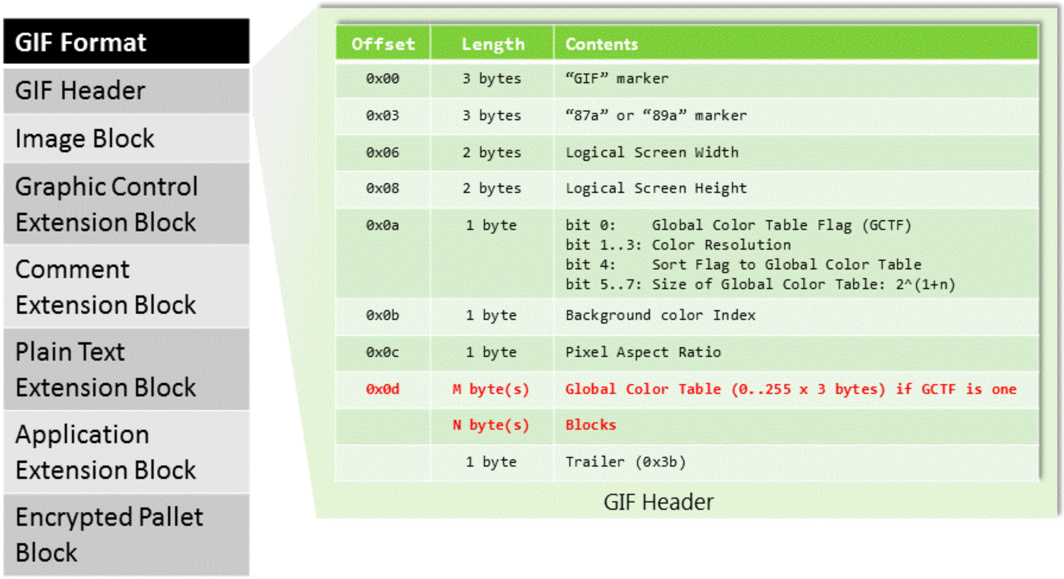

Original Image
Protected Image
Indexed Media Format
Header
• Image Properties (Height and Width)
• Color Lookup Table Block
Image Block
Graphic Control Extension Block
Comment Extension Block
Plain Text Extension Block
Application Extension Block
Input Marker and Create Parameters
Transform Color Lookup Table
Calculate Hash Value
Encrypt Color Lookup Table
Indexed Media Format
Header
• Image Properties (height, width)
• Transformed Color Lookup Table Block
Image Block
Graphic Control Extension Block
Comment Extension Block
Plain Text Extension Block
Application Extension Block
Encryption Extension Block

Figure 2. Scope of Image Restrict Viewing Approach

In order to identify the image for specific format, a marker is used. As example, for GIF format, its marker is set in GIF Header as illustrated in Figure 3. In our approach, we decided to define a marker in the Application Extension Block to identify our modified CLUT. The block contains details of specific application, such as Application Identifier and Application Authentication Code. The Application Authentication Code is sequence of three bytes and can be used to identify the owner of the application.



Offset	Length	Contents
0x00	3 bytes	“GIF” marker
0x03	3 bytes	“87a” or “89a” marker
0x06	2 bytes	Logical Screen Width
0x08	2 bytes	Logical Screen Height
0x0a	1 byte	bit 0: Global Color Table Flag (GCTF) bit 1..3: Color Resolution bit 4: Sort Flag to Global Color Table bit 5..7: Size of Global Color Table: 2^(1+n)
0x0b	1 byte	Background color Index
0x0c	1 byte	Pixel Aspect Ratio
0x0d	M byte(s)	Global Color Table (0..255 x 3 bytes) if GCTF is one
	N byte(s)	Blocks
	1 byte	Trailer (0x3b)

Figure 3. Gif Header Contents

After input the marker, next step is to generate restriction parameter. The restriction parameter is generated based on range of date or time information and/or number of view. A sigmoid function is used to convert the parameter to be a salt. The salt and password are input to PBKDF2 to produce a symmetric key. The symmetric key is used to encrypt the color lookup table. For authentication purposes, the hash of color lookup table is calculated. The hash value and the cipher text including size and encrypted CLUT is save in the Encryption Extension Block.

The image is degraded by transforming the image CLUT. After the encryption process, the color lookup table and its offset is obtained from the media content. To transform the image, media owner can decide either chooses custom or template transformation menu. If the owner chooses to allow the shapes in the image to be visible the degraded image, the color components will be modified to the RGB, YUV or YC_bC_r components. Alternatively, if the owner option for the shapes to be 'distorted', the image will display only monotone graphics (as illustrated in Figure 4). Finally, the original color lookup table is replaced with the modified color lookup table at the Color Lookup Table Block.

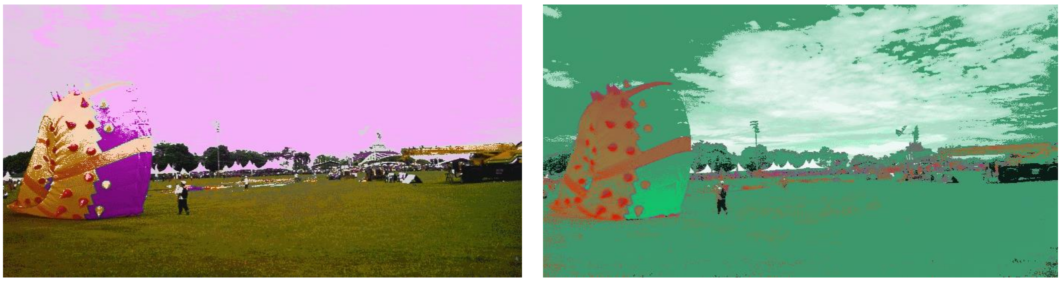


Figure 4. Left: Image with Lower Distorted Shape. Right: Image with Higher Distorted Shape.

The image to be displayed during viewing by user relies on the frequency of media view, date value and the correct password. To control expiry of the media, an equation such as sigmoid (Sigmoid Function, 2015) can be used. By setting time limitation at the first tangent changed, a sigmoid function is created.

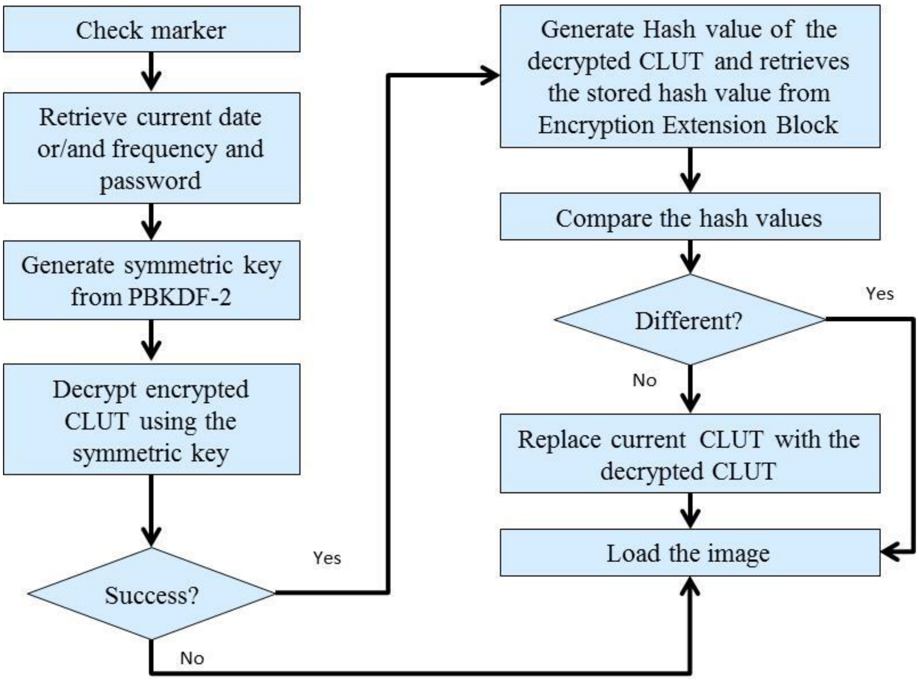

Check marker
Retrieve current date or/and frequency and password
Generate symmetric key from PBKDF-2
Decrypt encrypted CLUT using the symmetric key
Success?
Yes
No
Generate Hash value of the decrypted CLUT and retrieves the stored hash value from Encryption Extension Block
Compare the hash values
Different?
Yes
No
Replace current CLUT with the decrypted CLUT
Load the image

Figure 5. Process of Decryption/Viewing Image

Figure 5 illustrates the image decryption process flow. The process starts by checking the marker in the Application Extension Block. If exists, the current date time or/and frequency are recovered to generate a salt using the sigmoid function. As mentioned earlier, the symmetric key is produced based on the salt and password input. The symmetric key is required to decrypt the encrypted CLUT. To verify the authenticity of the decrypted CLUT, we hash the decrypted value and compare it with the hash value retrieved from the Encryption Extension Block. If the hash values are matches, the CLUT will be replaced with the decrypted CLUT and the image is loaded with the decrypted CLUT. Otherwise, the image will be loaded with the transformed CLUT.

CONCLUSION

The method presented in this paper is for restricting viewing of an image to authorized users within a set time range or number of view. The control is implemented by replacing the CLUT in the image with a modified one, and the encrypted original CLUT is attached to the image. Password and the restriction parameters are input to PBKDF2 to produce a symmetric key. If the key is correct, the user will view the image in full. Otherwise, the user will see a colour degraded image. By this method, viewing of images can be effectively controlled by the owner or author while allowing for preview.

ACKNOWLEDGMENTS

We would like to thanks our colleague, Moesfa Soeheila Mohamad for fruitful discussion and for proofreading this paper..

REFERENCES

Abdmouleh, M.K., Khalfallah and A., Bouhlel, M.S. (2002). Image Encryption with Dynamic Chaotic Look-Up Table. *Technologies of Information and International Conference on Science of Electronics (SETIT)*, 331-337.

CLUT (2015, April 23). Retrieved from http://www.computerhope.com/jargon/c/clut.htm

Cover Sheet fro the GIF89a Specification (2015, April 23). Retrieved from http://www.w3.org/Graphics/GIF.spec-gif89a.txt

Droogenbroeck, M. V. and Benedett, R. (2002), Techniques for a Selective Encryption of Uncompressed and Compressed Images, *In Advances Concept for Intelligent Vision System (ACIVS)*, Retrieved from http://orbi.ulg.ac.be/handle/2268/1496.

Kaliski, B. (2000), PKCS #5: Password-Based Cryptography Specifcation Version 2.0, Network Working Group, *RSA laboratories*. Retrieved from https://www.ietf.org/rfc/rfc2898.txt

Lookup table (2015, April 23). Retrieved from http://en.m.wikipedia.org/wiki/Lookup_table

Lu, D. and Jin, W. (2011), Fully phase color image encryption based on joint fractional Fourier transform correlator and phase retrieval algorithm. *Chinese Optics Letters*, 09(2), pp. 021002.

Sigmoid Function (2015, May 31). Retrieved from http://en.wikipedia.org/wiki/Sigmoid_function

Wong, K.M., Cheung, C.H. and Pa, L.M. (2002). Merged-Color Histogram for Color Image Retrieval. *International Conference on Image Processing (ICIP), IEEE*, 3, 949-952.