Scientific Research

A Visual Cryptography Based Digital Image Copyright Protection

Adel Hammad Abusitta

College of Engeenering & IT, Al Ain University of Science and Technology, Al Ain, UAE
Email: adel.abussitta@aau.ac.ae

ABSTRACT

A method for creating digital image copyright protection is proposed in this paper. The proposed method in this paper is based on visual cryptography defined by Noor and Shamir. The proposed method is working on selection of random pixels from the original digital image instead of specific selection of pixels. The new method proposed does not require that the watermark pattern to be embedded in to the original digital image. Instead of that, verification information is generated which will be used to verify the ownership of the image. This leaves the marked image equal to the original image. The method is based on the relationship between randomly selected pixels and their 8-neighbors' pixels. This relationship keeps the marked image coherent against diverse attacks even if the most significant bits of randomly selected pixels have been changed by attacker as we will see later in this paper. Experimental results show the proposed method can recover the watermark pattern from the marked image even if major changes are made to the original digital image.

1. Introduction

The proliferation of digitized images has made the digital images to be modified, distributed, duplicated and accessed easily. It is creating a pressing need to develop copyright protection methods. A watermarking technology is now providing highly attention as a desired method and technology for protecting copyrights for digital data [1-7]. A watermarking has been defined as the practice of embedding identification information in an image, audio, video or other digital media element to provide privacy protecttion from attackers [8-9]. The identification information is called "watermark pattern" and the original digital image that contains watermark pattern is named "marked image". The embedding takes place by manipulating the contents of the digital image [10]. Also, a secret key is given to embed "watermark pattern" and to retrieve it as well. **Figure 1** gives summarize of standard watermarking embedding scheme.

Basically, if the owner wants to protect his/her image, the owner of an image has to register the image with the copyright office by sending a copy to them. The copyright office archives the image, together with information about the rightful owner. When dispute occurs, the real owner contacts the copyright office to obtain proof that he is the rightful owner. If he did not register the image, then he should at least be able to show the film negative. However, with the rapid acceptance of digital photography,

there might never have been a negative. Theoretically, it is possible for the owner to use a watermark embedded in the image to prove that he/she owns it [11].

A typical image watermark algorithm must satisfy the following two properties: transparency and robustness. Transparency means that the embedded watermark pattern does not visually spoil the original image fidelity and should be invisible. Robustness means the watermark pattern is not easy to detect and remove illegally. Moreover, any modifications of the image values have to be invisible, and the watermark method has to be robust or fragile in order to provide protection against attackers.

In 1994, Noor-Shamir proposed the concept of visual cryptography [12]. The concept nowadays is being developed and/or improved several times for different purposes of applications by authors [13-24]. A good survey on visual cryptography can be found in [25]. Actually, Visual cryptography is describing as a secret sharing scheme extended of digital images, this will be discussed in the next section. Hwang [26] is the first author proposed
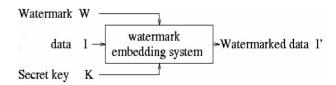

Figure 1. Watermarking embedding scheme.

a method of how to take a benefit of visual cryptography to create digital image copyright protection. According to Hwang method, the watermark pattern does not have to be embedded into the original image directly, which makes it harder to detect or recover from the marked image in an illegal way. [27-30] improved different methods to overcome Hwang method's shortcomings. We will come to these shortcomings in Section 3.

This paper proposes new digital images copyright protection based on Hwang method. The proposed method is based on visual cryptography defined by Noor-Shamir and Hwang method. Marking images will be conducted without embedding patterns into images. This leaves marked images unchanged with sizes exactly equal to the original ones. This paper is organized as follows. Section 2 reviews the concept of visual cryptography and digital image copyright protection. Section 3 presents our proposed digital image copyright protection method. Section 4 reports some experimental results and makes some discussions concerning our method. Finally, conclusions appear in Section 5.

2. Visual Cryptography and related Digital Image Copyright Protection

Naor and Shamir in 1994 proposed the concept of visual cryptography during EUROCRYPT 94. **Figure 2** from [31] demonstrates a simple version of visual cryptography. In their method, they introduced encoding scheme to share a binary image into two shares Share 1 and Share 2. A pixel P is divided into two subpixels in each of the two shares. If P is white one of two rows above in **Figure 2** is selected to create Share 1 and Share 2. But, if P is black one of two rows below in **Figure 2** is selected to create Share 1 and Share 2. A binary image at the end becomes secret image or invisible unless both shares are superposition.

Hwang created the first and typical idea for a digital image copyright protection based on the visual cryptography. The method use a simple (2, 2) visual threshold scheme defined by Naor-Shamir. Referring to Hwang's algorithm, the owner must select h × n black/white image as his/her watermark pattern P and a key S which must be kept securely. Then, verification information V is generated from the original k × 1 image M and the watermark pattern P using the key S; as follows:

1) Use S (the secret key) as the seed to generate h x n different random numbers over the interval [0, k × 1]. (Ri represents the i-th random number).

2) Assign the i-th pair (Vi1, Vi2) of the verificatin on information V based on the following **Table 1**:

Collect all the (Vi1, Vi2) pairs to construct the verification information V. This verification information must be kept by neutral organization. When the owner of an image M wants to claim the ownership of an image M' as
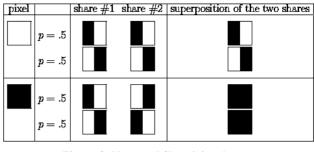

Figure 2. Naor and Shamir's scheme.

Table 1. The rules to assign the value of verification information.

The color of the i-th pixel in watermark pattern is	The left most bit of the Ri-th pixel of Image M is	Assign the i-th pair, (vi1, vi2), of *verification information V* to be
Black	"1"	(0,1)
Black	"0"	(1,0)
White	"1"	(1,0)
White	"0"	(0,1)

a copy of the original image M, the owner has to provide the secret key S, and the watermark pattern P is restored using the image M' and verification information V as follows:

1) Use S as a seed to generate h × n different random numbers over the interval [0, k × 1]. (Ri represents the i-th random number).

2) Assign the color of the i-th pixel of the watermark pattern P' based on the image M' as follows:

Get the left-most bit, b, of the Ri-th pixel of image M', and if b is 1 then, assign fi = (1, 0); otherwise assign fi = (0, 1).

If fi is equal to i-th pair of V then assigns the color of the i-th pixel of P' to be white; otherwise, assign it to be black.

3) If P' can be recognized as P through the human, the neutral organization shall adjudge that the image M' is a copy of M.

According to the previous method and also the related methods, these methods are strongly related to the values of the most significant bits of pixels selected randomly from the original digital image; therefore, if the most significant bit to some pixels selected randomly has been changed, the modified image M' will fail to retrieve the watermark pattern P successfully. Also, since the method does not consider the relationship between pixels and its neighbors, the watermark pattern would not be retrieved, if part of image has been cropped. Moreover, if we have an image X with some similarities with the original image M. The watermark pattern P might be restored successfully, despite the image X is not the same as the image M.

3. The Proposed Digital Image Copyright Protection

In this section, we present the proposed watermark method. The method acctually use the relationship between 8-neighbours pixels of pixel P(x, y) as a base of embedding algorithm as you will see later. **Figure 3** shows the 8-neighbours of pixel P(x, y).

We assume that the owner wants to embed the h × n watermark pattern into the image M that is a k × l 256 gray-leveled image. The owner embeds the watermark pattern P into the image M by generating the secret key, S, and the verification information, V, as the following steps.

Step Embedding-1. Select number S randomly as the secret key of the image M.

Step Embedding-2. Use S as the seed to generate h × n different random numbers over the interval [0, k × 1]. Where Ri is the i-th random number.)

Step Embedding-3. Calculate the number of Ri-th pixel's neighbours pixels from its 8-neighbours pixels that are less than or equal to the Ri-th pixel, this number named, Number_of_neighbors_less_or_equal_Ri-th_pixel. Also, calculte the number of Ri-th pixel's nieghbour pixels from its 8-nieghbour pixels that are greater than Ri-th pixel, this number named Number_of_ neighbor_greater_Ri-th_pixel.

For example, as in **Figure 4**, the Number_of_neighbors_ less_or_equal_Ri-th_pixel = 3, because we have three pixels {97, 98, 100} less or equal the Ri-th pixel, which equals 100. Also, Number_of_neighbors_greater_Ri-th_ pixel = 5, because we have 5 pixels in the following set {101, 103, 101,105,111} greater than Ri-th pixel.

It is obvious, in case the Ri-th pixel is a border pixel, this pixel do not have a full 8-nighbours. In this case, the available nighbours should be considerd and calculate Number_of_neighbors_less_or_equal_Ri-th_pixel and Number_of_neighbors_greater_Ri-th_pixel same as in step Embedding-3.

Step Embedding-4. Find the i-th pair (vi1, vi2) of the verification information V based on **Table 2**.

Step Embedding-5. Assemble all the (vi1, vi2) pairs to create the verification information V.

Note that Step Embedding-5 constructs the verification Information V based on the watermark pattern P and the relationship result between Number_of_neighbors_ less_ or_equal_Ri-th_pixel and Number_of_neighbors_ greater_ Ri-th_pixel as shown in **Table 2**, and moreover the proposed method does not make any change into image M or alter any pixel of image M.

The verification information V genrated from Step Embedding-5 must be given to the notarial organization. If an image M is appropriated by somebody as the image M', The owner of an image has to provide the secret key S to the notarial organization. The notarial organization retrives the verification information V and the watermark pattern P, which the owner has registered, and verifies the ownership of the image M' as follows:

X − 1, y − 1	X − 1, y	X − 1, y + 1
x, y − 1	x, y	x, y + 1
X + 1, y − 1	X + 1, y	X + 1, y + 1

Figure 3. 8 Neighbours pixels of pixel P(x, y).

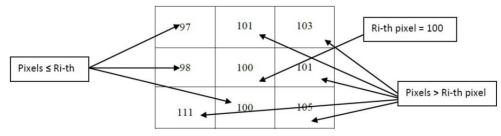**Figure 4. Example of Ri-th pixel's neighbors.**

Table 2. The proposed method's rules to assign the value of verification.

The Color of the i-th pixel in watermark pattern is	The relationship between *Number_of_neighbors_less_or_equal_Ri-th_pixel* and *Number_of_ neighbors _ greater_Ri-th_pixel*	Assign the i-th pair, (vi1, vi2), of *verification information V* to be
Black	*Number_of_neighbors_less_or_equal_Ri-th_pixel* ≤ *Number_of_neighbors_greater_Ri-th_pixel*	(0,1)
Black	*Number_of_neighbors_less_or_equal_Ri-th_pixel* > *Number_of_neighbors_greater_Ri-th_pixel*	(1,0)
White	*Number_of_neighbors_less_or_equal_Ri-th_pixel* ≤ *Number_of_neighbor_greater_Ri-th_pixel*	(1,0)
White	*Number_of_neighbors_less_or_equal_Ri-th_pixel* > *Number_of_neighbors_greater_Ri-th_pixel*	(0,1)

Step Verification-1. Use S as the seed to generate h × n different random numbers over the interval [0, k × 1]. Where Ri is the i-th random number.)

Step Verification-2. Assign the color of the i-th pixel of the watermark pattern based on image M' as follows:

If (*Number_of_neighbors_less_or_equal_Ri-th_pixel* ≤ *Number_of_neighbors_greater_Ri-th_pixel*) **AND** (the i-th pair, (vi1, vi2), of verification information V = (0,1)) **then**

Assign the color of the i-th pixel of P' to be <u>white</u>

Else If (*Number_of_neighbors_less_or_equal_Ri-th_pixel* ≤ *Number_of_neighbors_greater_Ri-th_pixel*) **AND** (the i-th pair, (vi1, vi2), of verification information V = (1,0)) **then**

Assign the color of the i-th pixel of P' to be <u>black</u>

Else If (*Number_of_neighbors_less_or_equal_Ri-th_pixel*>*Number_of_neighbors_greater_Ri-th_pixel*) **AND** (the i-th pair, (vi1, vi2), of verification information V = (1,0)) **then**

Assign the color of the i-th pixel of P' to be <u>white</u>

Else If (*Number_of_neighbors_less_or_equal_Ri-th_pixel* > *Number_of_neighbors_greater_Ri-th_pixel*) **AND** (the i-th pair, (vi1, vi2), of verification information V = (0,1)) **then**

Assign the color of the i-th pixel of P' to be <u>black</u>.

Step Verification-3. If P' equals the original watermark pattern P or can be recognized as it, then the notarial organization can conclude that image M' is a copy of M.

Note that the code written in Step Verification-2 can be concluded directly from **Table 2** which displays the proposed method's rules to assign the value of verification information.

The security of the proposed method is based on the relationship of pixels selected randomly and their 8-neighbor's pixels. This happened because whenever a change is applied into original digital image pixels, the result of the relationship mostly becomes the same. In other words, the relationships between Number_of_ neighbors_less_or_equal_Ri-th_pixel and Number_of_ neighbors_greater_Ri-th_pixel will not be affected by some majer changes in image pixels' bits. Experimental results in the next section will reflect that fact.

4. Experimental Results

The proposed algorithms are studied using Matlab 7. Images used are 256 × 256 pixels images Lina, Baboon and F-16 (shown in **Figure 6**). In Matlab 7, we made some changes in the three images before applying the proposed method. The changes are applied in the most significant bits of randomly selected pixels. Also, we did make changes in images quality using Adobe Photoshop CS 5 by applying diverse compressions in the three images. The watermark pattern used in the experiment is "cheng" in **Figure 5**. From the results shown in **Table 3**, we find that the watermark pattern "cheng" get some noise but still can be recognized even if the three images have been compressed and the size of those files is changed.

5. Conclusion

This paper presents a digital image copyright protection method using watermarking technology. The method proposed in this paper does not require that the watermark pattern to be embedded in to the original digital image. Instead, Verification information is generated which will be used to verify the ownership of the image. This leaves the marked image equal to the original image. The proposed method is tested and shows that a watermark pattern can be retrieved easily from marked image even the image is attacked by major changes in pixels bits.
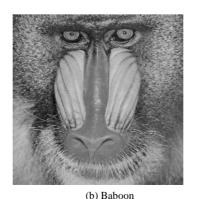

Figure 5. The watermark pattern "cheng".

| (a) Lena | (b) Baboon | (c) F-16 |

Figure 6. Three images of our Experiments.

A. H. ABUSITTA

Table 3. Experimental results.

(a) Use the proposed method to embed "Cheng" into "Lena"

The Marked Image	The Digital Image Quality with Adobe Photoshop CS 5	The Recovered Watermark Pattern "Cheng"
	0/low (the size of compressed file is 10,463 Bytes)	
	1/low (the size of compressed file is 12,501 Bytes)	
	2/low (the size of compressed file is 13,830 Bytes)	
	3/middle (the size of compressed file is 15,643 Bytes)	
	4/middle (the size of compressed file is 17,344 Bytes)	
Marked Image = Original Image	5/middle (the size of compressed file is 17,139 Bytes)	
	6/high (the size of compressed file is 19,113 Bytes)	
	7/high (the size of compressed file is 24,385 Bytes)	
	8/maximal (the size of compressed file is 30,930 Bytes)	
	9/maximal (the size of compressed file is 39,177 Bytes)	
	10/maximal (the size of compressed file is 48,199 Bytes)	

(b) Use the proposed method to embed "Cheng" into "Baboon"

The Marked Image	The Digital Image Quality with Adobe Photoshop CS 5	The Recovered Watermark Pattern "Cheng"
	0/low (the size of compressed file is 17,930 Bytes)	
	1/low (the size of compressed file is 22,112 Bytes)	
	2/low (the size of compressed file is 23,856 Bytes)	
	3/middle (the size of compressed file is 27,115 Bytes)	
	4/middle (the size of compressed file is 30,103 Bytes)	
Marked Image = Original Image	5/middle (the size of compressed file is 27,992 Bytes)	
	6/high (the size of compressed file is 33,120 Bytes)	
	7/high (the size of compressed file is 38,004 Bytes)	
	8/maximal (the size of compressed file is 44,759 Bytes)	
	9/maximal (the size of compressed file is 53,992 Bytes)	
	10/maximal (the size of compressed file is 62,951 Bytes)	

(c) Use the proposed method to embed "Cheng" into "F-16"

The Marked Image	The Digital Image Quality with Adobe Photoshop CS 5	The Recovered Watermark Pattern "Cheng"
	0/low (the size of compressed file is 9850 Bytes)	
	1/low (the size of compressed file is 11,451 Bytes)	
	2/low (the size of compressed file is 12,344 Bytes)	
	3/middle (the size of compressed file is 13,949 Bytes)	
	4/middle (the size of compressed file is 16,278 Bytes)	
Marked Image = Original Image	5/middle (the size of compressed file is 14,929 Bytes)	
	6/high (the size of compressed file is 17,930 Bytes)	
	7/high (the size of compressed file is 21,125 Bytes)	
	8/maximal (the size of compressed file is 25,920 Bytes)	
	9/maximal (the size of compressed file is 32,852 Bytes)	
	10/maximal (the size of compressed file is 40,877 Bytes)	

The watermark pattern cannot be retrieved from the marked image unless the key is given, and the key is only known by the owner. Also, the watermark pattern cannot be retrieved from the marked image unless the secret key and the verification information are given.

REFERENCES

[1] B. Surekha and G. N. Swamy, "A Spatial Domain Public Image Watermarking," *International Journal of Security and Its Applications*, Vol. 5, No. 1, 2011, 12 p.

[2] R. J. Anderson, "Information Hiding," *First International Workshop*, Vol. 1174, 1996, pp. 1-7.

[3] I. J. Cox, M. L. Miller and J. A. Bloom, "Digital Watermarking," Morgan Kaufmann Publishers Inc., San Fransisco, 2002.

[4] M. Kutter and F. A. P. Petitcolas, "Fair Benchmark for Image Watermarking Systems," *Proceedings of the Conference on Security and Watermarking of Multimedia Contents*, San Jose, 25 January 1999, pp. 226-239. doi:10.1117/12.344672

[5] G. C. Langelaar, J. C. A. van der Lubbe and J. Biemond, "Copy Protection for Multimedia Data Based on Labelling Techniques," *Proceedings of the 17th Symposium on Information Theory in the Benelux*, Enschede, May 1996, pp. 33-39.

[6] M. S. Fu and O. C. Au, "Joint Visual Cryptography and Watermarking," *Proceedings of the IEEE International Conference on Multimedia and Expo*, Taipei, 30 June 2004, pp. 975-978. doi:10.1109/ICME.2004.1394365

[7] R.-H. Hwang, "A Digital Image Copyright Protection Scheme Based on Visual Cryptography," *Tamkang Journal of science and Engineering*, Vol. 3, No. 2, 2002, pp. 97-106.

[8] H. Inoue, A. Miyazaki, A. Yamamoto and T. Katsura, "A Digital Watermark Technique Based on the Wavelet Transform and Its Robustness on Image Compression and Transformation," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, Vol. 82, No. 1, 1999, pp. 2-10.

[9] G. W. Braudaway, K. A. Magerlein and F. C. Mintzer, "Protecting Publicly Available Images with a Visible Image Watermark," *Proceedings of the SPIE*, San Jose, 1 February 1996, pp. 126-133. doi:10.1117/12.235469

[10] L. Hawkes, A. Yasinsac and C. Cline, "An Application of Visual Cryptography to Financial Documents," *Technical Report TR*001001, Florida State University, Tallahassee, 2000.

[11] C.-N. Yang, "A Note on Efficient Color Visual Encryption," *Journal of Information Science and Engineering*, Vol. 18, 2002, pp. 367-372.

[12] M. Noar and A. Shamir, "Visual Cryptography," *Advances in Cryptography Eurocrypt*'94, Vol. 950, 1995, pp. 1-12.

[13] W.-P. Fang, "Non-Expansion Visual Secret Sharing in Reversible Style," *International Journal of Computer Science and Network Security*, Vol. 9, No. 2, 2009, pp. 204-208.

[14] J. Weir and W.-Q. Yan, "Sharing Multiple Secrets Using Visual Cryptography," *Proceedings of the IEEE International Symposium on Circuits and Systems*, Taipei, 24-27 May 2009, pp. 509-512. doi:10.1109/ISCAS.2009.5117797

[15] Z. X. Fu and B. Yu, "Research on Rotation Visual Cryptography Scheme," *Proceedings of the International Symposium on Information Engineering and Electronic Commerce*, Ternopil, 16-17 May 2009, pp. 533-536. doi:10.1109/IEEC.2009.118

[16] X.-Q. Tan, "Two Kinds of Ideal Contrast Visual Cryptography Schemes," *Proceedings of the 2009 International Conference on Signal Processing Systems*, Singapore, 15-17 May 2009, pp. 450-453. doi:10.1109/ICSPS.2009.119

[17] H. B. Zhang, X. F. Wang, W. H. Cao and Y. P. Huang, "Visual Cryptography for General Access Structure by Multi-Pixel Encoding with Variable Block Size," *Proceedings of the International Symposium on Knowledge Acquisition and Modeling*, Wuhan, 21-22 December 2008, pp. 340-344. doi:10.1109/KAM.2008.91

[18] M. Heidarinejad, A. A. Yazdi and K. N. Plataniotis, "Algebraic Visual Cryptography Scheme for Color Images," *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing*, Las Vegas, 31 March-4 April 2008, pp. 1761-1764. doi:10.1109/ICASSP.2008.4517971

[19] F. Liu1, C. K. Wu and X. J. Lin, "Colour Visual Cryptography Schemes," *IET Information Security*, Vol. 2, No. 4, 2008, pp. 151-165. doi:10.1049/iet-ifs:20080066

[20] W. Qiao, H. D. Yin and H. Q. Liang, "A Kind of Visual Cryptography Scheme for Color Images Based on Halftone Technique," *Proceedings of the International Conference on Measuring Technology and Mechatronics Automation*, Zhangjiajie, 11-12 April 2009, pp. 393-395. doi:10.1109/ICMTMA.2009.294

[21] L. M. E. Bakrawy, N. I. Ghali, A. E. Hassanien and A. Abraham, "An Associative Watermarking Based Image Authentication Scheme," *Proceedings of the 10th International Conference on Intelligent Systems Design and Applications* (*ISDA* 2010), Cairo, 29 November-1 December 2010, pp. 823-828. doi:10.1109/ISDA.2010.5687160

[22] V. V. R. Prasad and R. Kurupati, "Secure Image Watermarking in Frequency Domain Using Arnold Scrambling and Filtering," *Advances in Computational Sciences and Technology*, Vol. 3, No. 2, 2010, pp. 236-244.

[23] P. Fakhari, E. Vahedi and C. Lucas, "Protecting Patient Privacy from Unauthorized Release of Medical Images Using a Bio-Inspired Wavelet-Based Watermarking Approach," *Digital Signal Processing*, Vol. 21, No. 3, 2011, pp. 433-446. doi:10.1016/j.dsp.2011.01.014

[24] A. De Bonnis and A. De Santis, "Randomness in Secret Sharing and Visual Cryptography Schemes," *Theoretical Computer Science*, Vol. 314, No. 3, 2004, pp. 351-374. doi:10.1016/j.tcs.2003.12.018

[25] P. S. Revenkar, A. Anium and Z. Gandhare, "Survey of Visual Cryptography Schemes," *International Journal of Security and Its Applications*, Vol. 4, No. 2, 2010, pp. 49-56.

[26] R. Hwang, "A Digital Image Copyright Protection Scheme Based on Visual Cryptography," *Tamkang Journal of*

science and Engineering, Vol. 3, No. 2, 2002, pp. 97-106.

[27] M. A. Hassan and M. A. Khalili, "Self Watermarking Based on Visual Cryptography," *Proceedings of the World Academy of Science, Engineering and Technology*, October 2005, pp. 159-162.

[28] A. Sleit and A. Abusitta, "A Visual Cryptography Based Watermark Technology for Individual and Group Images," *Journal of Systemics, Cybernetics and Informatics*, Vol. 5, No. 2, 2008, pp. 24-32.

[29] A. Sleit and A. Abusitta, "A Watermark Technology Based on Visual Cryptography," *Proceeding of the* 10*th*

World Multi Conference on Systemic, Cybernetics and Informatics, 2006, pp. 227-238.

[30] A. Sleit and A. Abusitta, "Advancedd Digital Image Copyright Protection Based on Visual Cryptography," *Proceeding of the* 4*th International Multi Conference on Computer Science & Information Technology*, Amman, 5-7 April 2006, pp. 365-375.

[31] D. Stinson, "Doug Stinson's Visual Cryptography Page," 2003.
http://www.cacr.math.uwaterloo.ca/~dstinson/visual.html