International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Effective Watermarking Adoption in Digital Imaging Copyright Protection Environment

K. Satya Sri [1], Gunna Kishore[2]

[1]Computer Science and Engineering, Rise Krishna Sai Prakasam Group of Institutions, Ongole, India

Abstract: ***Management of digital images via internet and e-business has witnessed tremendous growth in last decades, resulting in vulnerability to copyright infringement, Manipulation and attacks. This paper reviews some of the current developments in the copyright protection techniques for digital images based on visual cryptography. The approaches reviewed in the paper are lined based on the false positive rate. This paper discusses the main approaches for copyright protection of digital images. This paper also discusses how those approaches can achieve the required security standard. The methods are measured against relevant performance metrics and set according to their respective environments and digital formats being used, thus contributing sufficient knowledge so as to develop more secure scheme.***

Keywords: Copyright Protection, Central Limit Theorem, Digital Watermarking, Visual Cryptography

1. Introduction

Copyright protection techniques have drawn substantial interest from the research community for the last two decades. Resolving rightful ownership of images is important, since they are made available on the Internet as part of the E-business. Though, there are numerous ways to address this problem, a category called Watermarking based on Visual Cryptography (WVC) techniques are particularly designed to protect sensitive images without degrading its quality. Visual Cryptography (VC) [1] is an approach used to share an image into a set of cipher images by means of pixel replacement. WVC techniques do not modify the picture elements of the target image during watermarking and hence successfully balances its characteristics such as imperceptibility, robustness, capacity and security, without any conflict. Hence they are often called as lossless watermarking techniques and are useful in protecting high resolution images.

Typical steps involved in WVC methods are Owner Share Generation (OSG) and Watermark Extraction (WE). Given a target image to be copyrighted and a secret key, a feature vector is computed from them and a threshold technique is used to convert the feature vector into a secret binary matrix, called master key. The bits of this master key and a (2, 2) VC code table are used to generate an owner share in accordance with the pixels of the watermark. The owner share is then time stamped and is registered with a certified authority, who acts as an arbitrator. Whenever there is a controversy regarding ownership identity, the other share called public share is computed from the controversial image using a similar process and the same secret key. But, to generate public share, the extraction algorithm does not require the original watermark. Both the shares are then combined using a combination function, to extract the watermark.

The performance of any WVC scheme depends on the features extracted from the target image, the thresholds used in the master key construction, the VC code tables used in share generation process and the combination functions used in the retrieval of watermarks. The major requirements of any WVC scheme are satisfaction of C3 Rule (Code rule, Column rule, and Color rule) [2], small false positive rate and high robustness [3] to a variety of attacks. Other parameters that can be improved are size of shares, capacity of watermark, complexity of the scheme used, and the format of images that the system supports.

Many WVC methods with their own performance criteria have been developed. Hwang [4] composed a simple spatial domain WVC method, whose features are MSBs of randomly selected target image pixels. Later, Surekha and Swamy [5] proposed a similar technique by combining the MSB's with the spatial information bits of the target image to improve the security of Hwang's work. Y.C. Huo et al. [6] used Probability Based Visual Secret Sharing (PBVSS) [7] to reduce the pixel expansion and the concept of law of large numbers to generate feature vectors. Here the feature vector itself acts as a master key to generate the owner share. To reduce the false positive rate C.S Hsu [8, 9] generated a master key using sample statistics. Alternatively, Manglem Singh et al. [10] have chosen global mean of target image as a threshold. Recently, Wang et al. [11] extracted a master key from singular values of the target image to survive against many attacks and to reduce the false positive rate when compared to Hwang's method.

The transform domain WVC methods which resulted in the highest false positive rate are LTL's [12] method and Park's [13] method. They both used modified DWT's LL sub-band coefficients as feature vectors. While the former method used the LL sub-band coefficients as the threshold, the later used its average as a threshold. Xing [14], used a modified code table and a non-binary master key to reduce false positives. Fu et al. [15] used the median of the LL sub-band as threshold to further cut down the false positive rate. Alternately, B. Pushpa et al. [16], used global mean of the LL sub-band as a threshold.

Wang et al. [17] was the first to construct owner share from the features obtained by applying two transform domains on the target image sequentially. While Wang uses DWT and

SVD domains, Sanjay et al. [18] constructed owner share from features obtained by combining Fractional Fourier transform (FrFT) and Singular Value Decomposition (SVD) on the target image.

In all the WVC methods discussed above, the copyright information (watermark) is never hidden in the target image. Instead they hide it in the owner share and is kept at the arbitrator. Hence there is no problem of detecting, distorting or removing the watermark by the attackers. However, the major problem is increased false positive rate. According to I. J. Cox [19] a false positive rate of 10í6 can meet the security requirement and hence there is still a good scope for development of techniques which can further reduce the false positive rate.

Further, most of the WVC methods results in pixel expansion i.e., the shares generated are larger than the original watermark image size. It is important to reduce the share size as they are needed to be maintained by the arbitrator. Finally all the above mentioned techniques can't survive against rotations and flipping attacks, and are defined to hide binary watermarks only.

All these concerns of existing WVC schemes have motivated to do this research. This paper focuses on improving the efficiency of WVC methods by reducing the false positive rate and size of shares, and improving the robustness to flipping and rotation attacks.

2. Block Visual Cryptography

Visual Cryptography (VC) is an image coding technique, where decoding can be achieved by means of human hands or with simple logical operations. The proposed WVC method use the concept of Block VC to generate two non-expanded cipher shares from the watermark image. The corresponding code table is given in Table I.

In contrast to the existing WVC schemes, where one picture element is encoded at a time, the BVC coding algorithm inputs a block of two pixels each time. If the input pixel block is 00 (11), the algorithm selects one code column from the code table, in accordance with the secret key bit. when each code block containing dissimilar pixels i.e., 01/10 is encountered, the coding algorithm increments a counter. Based on the counter value (even/odd), it selects either 00 or 11 coding columns, in accordance with the secret key bit. Note that, this code table meets the requirements of C3 rule. Also, since a block of two pixels is replaced every time with another block of two pixels, the size of the shares is unexpanded. Further, to improve the quality of the reconstructed watermark, a logical XOR operation is used in combining both the shares. Sample results of BVC are shown in Fig. 1. From the figure it is clear that, the size of the original watermark image, the owner and public shares, and the decoded watermark are one and the same, without any pixel expansion. Also, the quality of decoded watermark is much high as shown in Fig. 1 d. Note that, using BVC, the quality of the reconstructed image is affected only at the edges.

Table 1: Code Table Used In Proposed Method

Watermark Pixel	01 or 10			
	00		11	
Secret Key bit	0	1	0	1
Share 1 (public)	[1 0]	[0 1]	[01]	[0 1]
Share 2 (owner)	[1 0]	[0 1]	[0 1]	[1 0]
Share1 ⊕ Share2	[00]	[00]	[1 1]	[1 1]

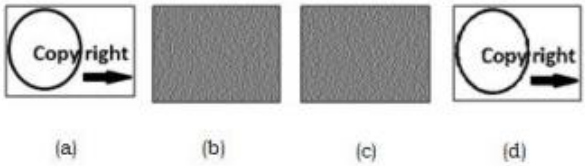

Figure 1: Sample Results of BVC

3. The Proposed Method

The Owner Share Generation (OSG) and Watermark Extraction (WE) process of the proposed method hides and detects the watermark in spatial domain by generating the owner and public shares one at a time. The feature extraction stage is common in generating both the shares. The method exploits Correlation Matrix (CM) [20] as a feature vector to improve the security and robustness. CM is a statistical feature that combines the spatial information with color. For an image of size M×N, CM is a matrix of R rows and C columns. While R indicates the total number of colors used to represent the image, C corresponds to the maximum possible D8 distance between any two pixels in the image. The proposed method also takes the advantage of the Central Limit Theorem to further improve the security of VC. In order to have memory wise improvement, the BVC code table is used.

The OSG and WE algorithms operate directly on the image to be copyrighted, if it is gray. When a color image is needed to be copyrighted, the algorithms operate on the intensity component extracted from it. This is done in the preprocessing stage. Let the relevant component image on which the algorithms operate is called the target image. The owner share generation process is as follows:

3.1. Owner Share Generation (OSG)

Inputs: Target image T of size M×N, watermark image of size c×d, secret key k

Output: Copyrighted image of size M×N, owner share of size c×d.

Step 1: Using the parameters Į and ù, resize and remap the image T to obtain a modified image G of size $MN/2^{\alpha}$ and with 2^{β} colors.

Step 2: Obtain the feature CM from image G.

Step 3: Calculate mean µ of CM.

Step 4: Use secret key k as a seed to obtain sample means μ_i, each of size n from CM.

Step 5: Compare each sample mean µi with the mean µ so as to obtain the elements of binary key matrix called master key.

Step 6: Construct an owner share from the binary watermark and master key matrix using the BVC code table given in Table I.
Step 7: Time stamp the owner share and register it at certified authority. Safely publish the copyrighted image.

From the steps in OSG algorithm, it is clear that the copyrighted image is same as the original target image. Hence, their PSNR is infinite. Also, the size of the owner share is same as watermark image size, suggesting that there is no pixel expansion. Hence it reduces the memory requirements of the arbitrator for maintenance of the owner shares.

3.2. Watermark Extraction (WE)

The process of extracting the watermark from a controversial image involves much similar steps as above. The public share is first constructed from the unique features of the controversial image and is then XORed with the owner share to extract the hidden watermark. The owner share is constructed using the following procedure:

Inputs: Controversial image T' of size M×N, owner share of size c×d, secret key k.

Output: Extracted watermark of size c×d.

Step 1: Using the parameters Į and ù, resize and remap the image T' to get a modified image G' of size MN/2Į and 2^{β} colors.
Step 2: Obtain the feature CM from image G'.
Step 3: Calculate mean μ' of CM.
Step 4: Use a secret key k as a seed to obtain sample means $\mu_i^{'}$, each of size n from CM.
Step 5: Compare each sample mean$\mu_i^{'}$,with mean μ', so as to obtain the elements of binary key matrix called master key.
Step 6: Construct a public share from the binary key matrix using the BVC code table given in Table I. From the table it is clear that the public share can be generated solely from the extracted key matrix.
Step 7: Perform XOR operation on the owner and public shares to extract the shared watermark.

The security of the proposed method is guaranteed by the generation of Master key matrix. Due to the property of the Central Limit Theorem the number of sample means that are greater than the population mean are almost equal to the number of sample means which are less than the population mean. Hence the distribution of 1's and 0's in the key matrix is nearly equal, thereby satisfying the VC's column rule. Since, both OSG and WE algorithms make use of the BVC code table, the requirements of the VC's code and color rule are also satisfied. The proposed method also requires less memory as the shares are unexpanded. Further, since the combination function used is XOR, the quality of extracted watermark has drastically improved.

3.3 The selection of, α, β, and n

In addition to the secret key k, this method requires extra input parameters α, β and n to vary the performance of the OSG and WE algorithms. The parameter Į specifies the resizing level of the target image and should be a positive integer. The number of D8 distances to be calculated for CM are reduced to (MN/2^{α})-1 instead of (MN-1). As the value of Į increases, the size of target image reduces, CM size reduces and eventually computation time scales down. But, at the same time, the increase in the value of Į also increases the false positive rate. The parameter ù specifies the bit depth of the target image and hence2^{β} specifies the size of the color map. β must be an integer between 1 and 8. As the value of β decreases, the number of colors to which the target image is mapped decreases and the robustness to contrast changes increases. But, at the same time, too much decrease of β results in an increase in the false positive rate. Another parameter which affects the security of this method is n. It indicates the sample size and is used in calculating the sample means. The value of n has no much effect on execution time. As the sample size n (usually >30) increases, the probability of false positives decreases and hence security increases.

4. Conclusion

In this paper, the concept of Correlation Matrix (CM) has been introduced into the copyright protection of digital images to reduce the ambiguity in detecting the right owners and to improve the robustness to rotation and flipping attacks. The proposed method applied Central Limit Theorem (CLT) on the CM to result a very small false positive rate (0.003) and hence the method is considered secure. Unlike other WVC methods in the literature, the proposed method is particularly robust to flipping attacks and rotation attacks (900 , 1800 , 2700). Further, this method does not expand the size of shares and hence reduce the memory requirements. This is achieved with Block Visual Cryptography. Unlike some WVC methods, the size of watermark image is not restricted.

References

[1] M. Naor and A. Shamir, "Visual Cryptography", in Advances in Cryptology – Eurocrypt'94, Vol. 950 of Lecture Notes in Computer Science, Springer-Verlag, Berlin, 1995, pp 1-12.
[2] B.Surekha,.G.N.Swamy, "Sensitive Digital Image Watermarking for Copyright Protection", International Journal of Network Security (IJNS), Vol. 15, No. 2, pp. 95-103, March 2013.
[3] I.J. Cox, M.L. Miller and J.A. Bloom, "Watermarking applications and their properties", Proceedings of the International Conference on Information Technology: Coding and Computing- ITCC2000, 2000, pp. 6–10.
[4] R. Hwang, "Digital image copyright protection scheme based on visual cryptography," Tamkang Journal of Science and Engineering, Vol.3, No. 2, 2002, pp. 96-106.
[5] B.Surekha, Dr.G.N.Swamy, Dr.K.Srinivasa Rao, A.Ravi Kumar, "A Watermarking Technique based on Visual Cryptography", International Journal of Information Assurance and Security(JIAS), ISSN 1554-1010, Dynamic Publishers, USA, Vol. 4, Issue 6, pp. 470-473, 2009.

[6] Y.C Hou and P.H. Huang, "Image Protection based on Visual Cryptography and Statistical Property", IEEE SSP, 2011, pp. 481-484.
[7] C. N. Yang, "New visual secret sharing schemes using probabilistic method", Journal of Pattern Recognition Letters, Vol. 25, No. 4, 2004, pp. 481-494.
[8] C.S Hsu and Young-Chang Hou, "A Visual Cryptography and Statistics Based Method for Ownership Identification of Digital Images", World Academy of Science, Engineering and Technology, Vol. 2, 2005, pp.172-175.
[9] C. S. Hsu and Y. C. Hou, "Copyright protection scheme for digital images using visual cryptography and sampling methods", Optical Engineering, Vol. 44, No. 7, 2005, pp. 1-10.
[10] Kh. Manglem Singh, "Dual Watermarking Scheme for Copyright Protection", International Journal of Computer Science and Engineering System, Vol. 3, No. 2, April-July 2009, pp. 99-106
[11] M.S. Wang and W.C. Chen, "Digital image copyright protection scheme based on visual cryptography and singular value decomposition", Opt. Eng., 46, Vol. 6, 2007, pp 1-8.
[12] D.C. Lou, H.K. Tso, J.L. Liu, "A copyright protection scheme for digital images using visual cryptography technique", Comput. Stand. Interfaces, 29, 2007, pp.125–131.
[13] G.D. Park, EI. Yoon, and K.Y. Yoo, "A new copyright protection scheme with visual cryptography", In: Proc. of the Second Int. Conf. on Future Generation Communication and Networking Symposia, 2008, pp. 60-63.
[14] Y.B. Xing and J.H He, "A new robust copyright Protection scheme for digital image based on Visual Cryptography", In: Proc. of the 2010 Int. Conf. on Wavelet Analysis and Pattern Recognition, Qingdao, 11-14 July, 2010, pp.6-11.
[15] R. Fu and W. Jin, "A Wavelet-Based Method of Zero-Watermark Utilizing Visual Cryptography", In: Proc. of the 2010 Int. Conf. on Multimedia Technology (ICMT), Oct 2010, pp.1-4, 29-31.
[16] B. Pushpa Devi, Kh. Manglem Singh, and Sudipta Roy, "Dual Image Watermarking Scheme based on Singular Value Decomposition and Visual Cryptography in Discrete Wavelet Transform", International Journal of Computer Applications, Vol. 50, No. 12, July 2012, pp. 6-13.
[17] M.S. Wang and W.C. Chen, "A hybrid dwt-svd copyright protection scheme based on k-means clustering and visual cryptography", Comput. Stand. Interfaces, 31, (4), pp. 757–762, 2009.
[18] Sanjay Rawat and Balasubramanian Raman, "A blind watermarking algorithm based on fractional Fourier transform and visual cryptography", Signal Processing 92 (2012) 1480–1491.
[19] I.J. Cox, M.L. Miller and J.A. Bloom, "Watermarking applications and their properties", Proceedings of the International Conference on Information Technology: Coding and Computing- ITCC2000, 2000, pp. 6–10.
[20] R.M. Haralick, K. Shanmugam, I. Dinstein, "Textural Features for Image Classification", IEEE Transactions on Systems, Man, and Cybernetics, Vol. 3, No. 6, 1973, pp. 610–621