I.J. Image, Graphics and Signal Processing, **2013, 2, 25-30**
Published Online February 2013 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijigsp.2013.02.04

Permutation-based Homogeneous Block Content Authentication for Watermarking

Dr.S.Maruthuperumal[1]
[1] Associate Professor &IT HOD, Godavari Institute of Engineering &Technology, Rajahmundry, A.P, India.
e-mail: maruthumail@gmail.com

G.Rosline Nesa Kumari[2]
[2] Associate Professor, Godavari Institute of Engineering &Technology, Rajahmundry, A.P, India.
e-mail: rosemaruthu@gmail.com

Abstract— In modern days, digital watermarking has become an admired technique for hitting data in digital images to help guard against copyright infringement. The proposed Permutation-based Homogeneous Block Content authentication (PHBC) methods develop a secure and excellence strong watermarking algorithm that combines the reward of permutation-based Homogeneous block (PHB) with that of significant and insignificant bit values with X0R encryption function using Max coefficient of least coordinate value for embedding the watermark. In the projected system uses the relationship between the permutation blocks to embed many data into Homogeneous blocks without causing solemn distortion to the watermarked image. The experimental results show that the projected system is very efficient in achieving perceptual invisibility with an increase in the Peak Signal to Noise Ratio (PSNR). Moreover, the projected system is robust to a variety of signal processing operations, such as image Cropping, Rotation, Resizing, Adding noise, Filtering , Blurring and Motion blurring.

Index Terms— Homogeneous, Permutation blocks, Attacks, Watermarking

I. INTRODUCTION

The swift development of internet distributions of digital media has formed an urgent need for copyright protection because of easy duplication and alteration. With the current spate of cases involving forged currency, no one needs to be reminded of the importance of watermarking. A watermark is a form, image or text that is impressed onto paper, which provides evidence of its authenticity. Digital watermarking is an extension of this concept in the digital world. In recent years the phenomenal growth of the internet has highlighted the need for mechanisms to protect ownership of digital media. Exactly identical copies of digital information, be it images, text or audio, can be produced and distributed easily. Digital watermarks are pieces of information added to digital data (audio, video, or still images) that can be detected or extracted later to make an assertion about the data. This information can be textual data about the author, its copyright, etc; or it can be an image itself.

Digital watermark techniques embed an invisible signal (for example, company logo or personal symbol) into image so as to attest the owner identification of the image and discourage the unauthorized copying. The watermark should be undeletable, perceptually invisible, statistically undetectable and resistant to lossy data compression and common signal processing operations [1] [2]. Digital watermarking has a widely application, including copyright protection, content protection, location content online, and so on. Some traditional application and some novel application are introduced in the paper. In conclusion, digital watermarking gives authentication, identification, and integrity to digital sign helps the owners can use their digital assets under protection. Attacks and accidental signal distortions are thus treated as noise that the engrossed signal must be immune to. The success of watermark for intellectual property rights organization depends on how easily it is adopted with common policy and how successfully contravention cases are addressed. The objective of vigorous watermarking algorithms [3], [4], [5] is to remain the implanted digital watermarks even after some attacks. The attacks include the malicious modifications, i.e., averaging and watermark removal/counterfeit, and unintended processing, i.e., resizing, compression, and filtering. Vigorous watermarking algorithms are developed on t he purpose of copyright protection and ownership identification.

Content authentication applications [6], [7] where any tiny changes to the content are not satisfactory, the embedding distortion has to be rewarded for perfectly. Many digital watermarking schemes have been proposed in the literature for still images and videos and are mainly used in applications. In all these applications, apart from copyright protection, illegal copy protection, proof of ownership problems, identification of manipulations, there is a growing need for the authentication of the digital content. Recently, the searches for more secure watermarking techniques have revealed the fact that the content of the images could be used to improve the invisibility and the robustness of a watermarking scheme [8], [9].

In [9], Xie et al. proposed a novel content based watermarking technique in ridgelet domain. The blocks are classified using image texture characteristics and to improve the robustness middle frequencies of the RT subband is used. Kim and Lee in [10] presented a content based fragile watermarking scheme for image authentication. This model is able to tolerate incidental distortions and indicated tampered regions in case of malicious manipulation. Later in 2007, [11] proposed a fragile watermarking scheme based on DWT domain which is able to resist all kinds of manipulations and had the ability to localize the tampered regions. Parameswaran [12] proposed a content dependent image signature for authentication using wavelet domain. The experimental results proved that the scheme proposed is very effective and it's able to withstand attacks like copy attack, crop attack, protocol attacks and cryptographic attacks.

In this paper, we proposed a content authentication for watermarking using Permutation based homogeneous block and XoR encryption function. A watermark is constructed based on XoR encryption function, and then is embedded into the Max coefficient of least coordinate value. The watermark is detected using statistical correlation between the watermark and the corresponding embedding regions. The rest of this paper is organized as follows. In Section 2 the Watermark Construction is proposed using Permutation based homogeneous block and X0R encryption function. In Section 3 watermark embedding and extracting procedure is introduced. In Section 4, the experimental results are given to demonstrate the superiority of the proposed scheme. Finally, conclusions are given in Section 5.

II. WATERMARK CONSTRUCTION

In this section, we discuss about the watermark generation of the proposed PHBC method. In order to design a good watermarking, first of all, what we must consider is watermark construction, since a good watermark can improve the watermark embedding capacity and the quality of watermarked image. Divide the permutation image into an integral number of M×N blocks. Choose the blocks in perceptually the most important region of the host for the generation of the content watermark. The generation of the watermark is a two step process: first step is the selection of blocks and gathering of host image statistical information and the second step is the recognizable logo watermark image and generated simulated image which create the effective watermark for our scheme.

III. PROPOSED PHBC SCHEME

In the proposed PHBC watermarking scheme, a cover image C with N×N pixels, where $C = (c_1, c_2, \ldots\ldots c_{N\times N})$. The watermark W is a binary image consisting of w×c bits, where $W = (w_1, w_2, \ldots\ldots w_{w\times c})$ and $w_i \in (0,1)$. The overview of the proposed PHBC watermarking scheme is shown in Figure 1.

A. Watermark Embedding Algorithm

Step 1: To improve the security of the watermarking system, the original image is scrambled by random permutation using Torus automorphism. For this purpose the cover data is scrambled in order to ensure additional security.

Step 2: The permutation image is partitioned into (p×p) non- overlapping block where $p = 2^n$, and n = 1, 2, 3.... If the size of the cover image is (N×N), the total N^2/p^2 number of blocks are obtained from the scrambled image, and in general p>N.

Step 3: Calculate the variance value B_{var} of each blocks.

Step 4: Arrange the blocks in ascending order and identify the homogenous block (small B_{var} value).

Step 5: Calculate the variance value C_{var} of cover image C with N×N pixels.

Step 6: Identify the significant block if the condition is ($C_{var} > B_{var\ i}$), then make the block is one.

Step 7: Identify the insignificant block if the condition is ($C_{var} \leq B_{var\ i}$), then make the block is zero.

Step 8: To get new watermark logo, perform the XOR encryption procedure to significant and insignificant bits into watermark logo bits.

Step 9: Consider the max values of least coordinate value, to insert the new watermark logo and add the watermark bit into max values to obtain watermarked pixels.

Step 10: Perform the inverse random permutation, to obtain watermarked image.

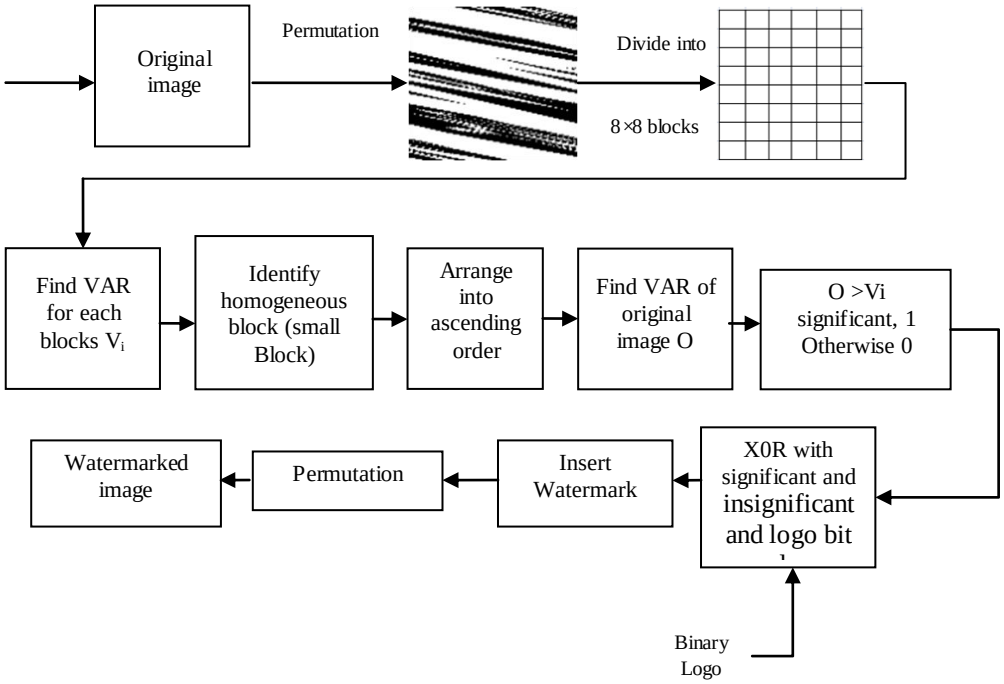


Figure.1 Block diagram of proposed PHBC method

B. Watermark Extracting Algorithm

Step 1: The watermarked image is scrambled by random permutation using Torus automorphism.

Step 2: The permutation image is partitioned into (p×p) non- overlapping block where $p = 2^n$, and n = 1, 2, 3.... If the size of the watermarked image is (N×N), the total N^2/p^2 number of blocks are obtained from the scrambled image, and in general p>N.

Step 3: Calculate the variance value B_{var} of each blocks.

Step 4: Arrange the blocks in ascending order and identify the homogenous block (small B_{var} value).

Step 5: Calculate the variance value W_{var} of watermarked image W with N×N pixels.

Step 6: Identify the significant block if the condition is ($W_{var} > B_{var\ i}$), then make the block is one.

Step 7: Identify the insignificant block if the condition is ($W_{var} \leq B_{var\ i}$), then make the block is zero.

Step 8: Consider the max values of least coordinate value, to extract the new watermark logo.

Step 9: To get watermark logo, perform the XOR decryption procedure to significant and insignificant bits into new watermark logo bits.

Step 10: Perform the inverse random permutation, to obtain original image.

IV. Experiment Results

In this section, some experiments are designed to prove the efficiency of the proposed PHBC scheme. First, the image quality after watermark insertion is investigated. Secondly, the scheme is tested to compression tolerance. Finally, we will show the scheme is capable to image authentication. The 256*256 Lena, Boy, Eye, Food, and House images of 8-bit grayscale are used for experiments as shown in Figure 2. In watermark generation, the permutation image is divided to blocks of 8*8 pixels, forming 1024 blocks. One bit is extracted from each block. The total length of the signature is then 1024 bits. The watermark image Fish is given in Figure 3. The percentage similarity between the extracted watermark and the original watermark is calculated. The same procedure is repeated for all five standard images and results are taken in the form of PSNR and correlation coefficient i.e., measuring correlation between original and retrieved watermark at different quality factor.

(a) (b) (c)

(d) (e)

Figure. 2 Cover images (a) Lena (b) Boy (c) Eye (d) Food (e) House

Figure. 3 Watermark image Fish

TABLE.1 EXPERIMENT RESULTS OF THE PROPOSED PHBC METHOD

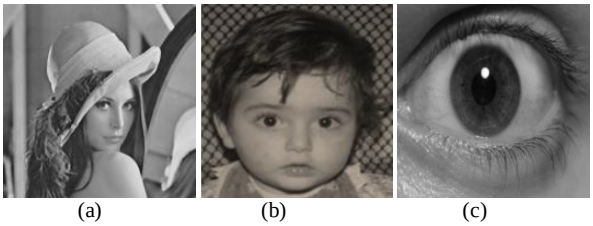
Images	PSNR	NCC
Lena	48.97	0.98
Boy	47.87	0.99
Eye	48.03	0.99
Food	48.73	1
House	47.98	0.98

TABLE.II PSNR VALUES FOR DIFFERENENT ATTACKS

Attacks	Lena	Boy	Eye	Food	house
	PSNR(dB)				
Cropping (10%)	45.53	46.38	45.45	44.35	43.68
Rotation (30^0)	44.23	43.56	43.58	43.59	44.29
Resize (25%)	42.46	41.98	42.48	42.49	42.97
Noise addition (25%)	44.38	42.57	43.57	43.29	42.02
Filtering (7×7)	42.46	42.48	42.48	41.30	41.39
Blurring (15%)	39.12	38.58	40.10	39.75	40.02
Motion blurring (15%)	38.12	37.28	38.59	37.29	39.23

TABLE.III CORRECTION VALUES FOR DIFFERENENT ATTACKS

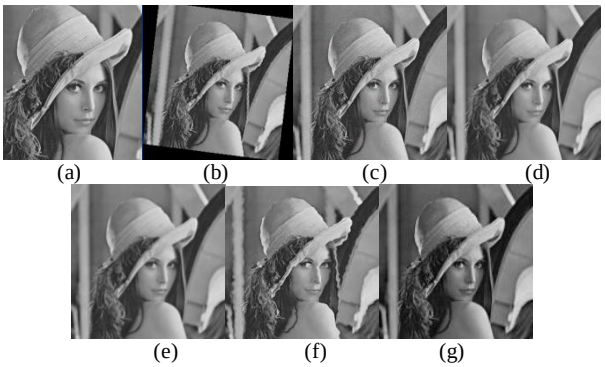
Attacks	Lena	Boy	Eye	Food	house
	NCC				
Cropping (10%)	0.91	0.95	0.93	0.91	0.87
Rotation (30^0)	0.89	0.89	0.88	0.89	0.89
Resize (25%)	0.89	0.88	0.89	0.89	0.86
Noise addition (25%)	0.85	0.86	0.87	0.84	0.84
Filtering (7×7)	0.79	0.79	0.83	0.81	0.81
Blurring (15%)	0.78	0.77	0.79	0.75	0.78
Motion blurring (15%)	0.85	0.85	0.87	0.87	0.85



(a) (b) (c)

(d) (e)

Figure. 4 Watermarked images (a) Lena (b) Boy (c) Eye (d) Food (e) House



(a) (b) (c) (d)

(e) (f) (g)

Figure. 5 Attacked gray level images (a) Cropping; (b) Rotation; (c) Noise; (d) Filtering; (e) Blurring; (f) Motion blurring; (g) Resizing

Table 1 list our experimental results and it indicates that the proposed PHBC method has a higher detection rate than the other methods. The test results are shown in Table 1 with associated PSNR dB (Peak Signal to Noise Ratio). It is observed that, average PSNR range for attacked watermark images is 40 to 50 dB. The quality watermarked images are shown in Figure 4.

The robustness of the proposed PHBC watermarking method is tested for the images and is given in Table 2 and Table 3 as PSNR and NCC under the attacks of various geometric transformations such as Cropping, Rotation, Noise addition, Filtering, Blurring, Motion blurring and Resizing which are presented in Figure 5. The experiments are carried out with such synchronization pattern, proving that the information contained in the images after geometric transformations are still sufficient to retrieve the watermark.

Watermarking techniques are usually tested against various robustness criteria. The proposed PHBC watermarking technique is tested by using the different geometric attacks and different watermarks are embedded in the standard test images "Lena", "Boy", "Eye", "Food" and "Lena". The watermarked images are cropped with percentage 30, Rotated with 30^0, adding 20% Gaussian noise, Filtered with a 7×7 median filter, Blurring and Motion blurring with 15% and Resizing ¼ of image are given in Figure 5 (a)–(g). The proposed PHBC method watermarking technique preserves robustness to all geometrical transformations.

The proposed PHBC algorithm is more robust to Cropping, Rotation, Addding Noise, median filtering, Blurring, Motion blurring, and Resizing. This indicates that an embedded watermark is still recoverable even

after the common image processing operations on the watermarked image and hence highly suitable for the copyright protection.

A. Image authentication

The proposed PHBC method is proficient for image authentication. In the experiment, the signature is extracted from the original image and inserted back into the image as watermark. Then a small area of the watermarked image is modified. In the receiver's side, the signature and watermark are extracted from the modified image. Then the modified area is detected if the signature and watermark are not the same in the corresponding blocks. Figure 6 shows the result. In Figure 6(b), a hair clip is put on the head of the watermarked Boy image. In authentication, the difference of signature and watermark indicate the modified area showing in Figure 6(c) marked with white.

(a) (b) (c)

Figure.6 Authentication Image (a) Original image (b) Tamper image (c) Tamper detection

V. CONCLUSION

The present paper describes a robust PHBC watermarking scheme with least deformation of the cover image and the algorithm requires squat computation cost. The use of both modified entropy model and watermarking is a very active research field with a lot of applications. Accompany with the development of digital watermarking, more and more attacks on digital watermarking are emerging. Some common attacks and novel attacks are shown in the paper. With the rapid development of digital technology, people use digital signal to communicate, share information and save data more frequently, digital watermarking can provide security protection for both individuals and companies, and will keep developing rapid and play an important role in the future network. Watermarking is a very active research field with a lot of applications. Although it is a relatively new field, it has produced important algorithms for hiding messages into digital signals. These can be described by many different models.

ACKNOWLEDGMENT

The authors would like to express their gratitude to Sri K.V.V. Satyanarayana Raju, Founder & Chairman and Sri K. Sasi Kiran Varma, Managing Director, Chaitanya group of Institutions for providing necessary Infrastructure. Authors would like to thank the anonymous reviewers for their valuable comments.

REFERENCES

[1] I.J. Cox, J. Killian, F.T. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia", IEEE Transactions on Image Processing, Vol.6, No. 12, 1997, pp. 1673-1678.

[2] Ruizhen Liu and Tieniu Tan, "Content-based watermarking model", in Proceedings of 15th International Conference on Pattern Recognition, Vol. 4, 2000, pp. 238-241.

[3] H. Huang, F. Wang, and J. Pan, Efficient and Robust Watermarking Algorithm with Vector Quantisation. Electron. Letter, June 2001 .

[4] T. Kalker and J. Haitsma, Efficient Detection of a Spatial Spread Spectrum Watermark in MPEG Video Streams. Proceeding of IEEE Int. Conf. Image Processing, 2000 .

[5] C. Lu, S. Huang, C. Sze, and H. Liao, Cocktail Watermarking for Digital Image Protection. IEEE Transaction on Multimedia,,4 , 2000.

[6] Alattar, A.M. (2004). Reversible watermark using the difference expansion of a generalized integer transform, IEEE Transactions on Image Processing, Vol.13, No.8, Pp.1147-1156.

[7] Tian, J. (2003) Reversible data embedding using a difference expansion, IEEE Transactions on Circuits and Systems for Video Technology, Vol.13, No.8, Pp.890-896.

[8] Qi, X. and Qi, J. (2007) A robust content-based digital image watermarking scheme, Signal Processing, Elsevier, Vol. 87, Issue 6, Pp. 1264-1280.

[9] Sachs, D., Anand, R. and Ramchandran, K. (2000) Wireless image transmission using multiple-description based concatenated codes,Proceedings Data Compression Conference DCC 2000, P. 569.

[10] Xie, L. and Arce, G.R. (2001) A class of authentication digital watermarks for secure multimedia communication IEEE Transactions on Image Processing, Vol.10, No.11, Pp.1754-1764.

[11] A Xie, Z., Wang, S., Gan, L., Zhang, L. and Shu, Z. (2008) Content Based Image Watermarking in the Ridgelet Domain, International Symposium on Electronic Commerce and Security, Pp.877-881.

[12] Kim, M. and Lee, W. (2004) A Content-Based Fragile Watermarking Scheme for Image Authentication, Lecture Notes in Computer Science, Content Computing, Springer Berlin / Heidelberg, Vol. 0302/2004, Pp. 258-265.

Dr. S.MaruthuPerumal received his B.E, in Computer Science and Engineering from Bharathidasan University and M.E. in Computer Science and Engineering from Sathyabama University Chennai. He received his Ph.D in the area of Digital watermarking. He is having Fourteen years of teaching experience. At present he is working as an Associate Professor and Head of the Department IT Godavari Institute of Engineering and Technology, Rajahmundry. He published Twenty three research publications in various Inter National, National Conferences and Journal. His research interest includes Image processing, Digital Watermarking, Steganography and Security. He is a life member of ISCA, IAENG and Institutional Member of CSI.

G RoslineNesaKumari received her M.E. Degree from Sathyabama University Chennai in 2005.She is Pursuing her Ph.D degree in Computer Science and Engineering at Dr MGR University Chennai. She is having Eleven years of teaching experience. At present she is working as an Associate Professor in Godavari Institute of Engineering and Technology, Rajahmundry. She published Twenty six research publications in various International, National Conferences and Journal. She is a life member of Indian Science Congress Association (ISCA), IAENG, Red Cross. Her research interest includes Image processing, Digital Watermarking and Security.

