International Journal of Soft Computing and Engineering (IJSCE)
ISSN: 2231-2307, Volume-2, Issue-4, September 2012

A Simple Block Based Content Watermarking Scheme for Image Authentication and Tamper Detection

L. Sumalatha, G. RoslineNesa Kumari, V.Vijaya Kumar

Abstract*— Digital watermarking techniques have been proposed for handling applications like Copy protection, Content authentication of digital images. Any tiny change to the content is not acceptable in images especially when they are used to store secret information in the form of an invisible digital watermark. To address this present paper proposes a simple block based content checksum watermarking (BCCW) method for image authentication and tamper localization. The proposed BCCW is a hierarchical and block based method. In BCCW the image is divided into sub blocks of size 4×4. Then a hierarchical relationship is established by dividing each 4×4 as a set of four 2×2 blocks. A Checksum of 8 bits is computed from pixels of 4×4 block and the checksum is placed intelligently on the selected 2×2 block pixels. In the proposed BCCW if any block or even a pixel is tampered then the block checksum does not match with the extracted bit sequence. The main advantage of the BCCW scheme is, it can identify effectively in which blocks the tampering has occurred. The experimental results show that the quality of the embedded image is very high, and the positions of the tampered parts are located correctly. The proposed BCCW method is compared with several other methods.

Index Terms*—Block Based, Content Checksum, Image Authentication

I. INTRODUCTION

The rapid progress in the digital multimedia technology offered many facilities in the transmission, reproduction and manipulation of data. As the internet is an open environment, the data sent on the internet is vulnerable to attacks such as interception, fabrication and modification. This advancement in the multimedia technology has also brought the challenge such as copyright protection, content authentication for content providers. Watermarking is a popular technique that is used for copyright protection and authentication. Depending on the objective of the application, watermarking schemes are simply classified into fragile watermarking and robust watermarking schemes. The robust watermarking schemes are developed for copyright protection of images, while the fragile watermarking scheme is designed for content authentication. Schyndel *etal.*[1] proposed an authentication technique that adds a maximal length linear shift register sequence (m-sequence) to the corresponding image block, the spatial cross correlation function of the sequence and the watermarked image is computed for authentication. An authentication technique that calculated checksum on an image block and embedded into the LSB's of the same block was presented in [2]. Wolfgang and Delp [3] authentication technique is an extension of Schyndel *etal.* work that improves the localization properties and robustness. P. Wong [4] described another fragile marking technique in which a digest using a hash function is obtained. The image, image dimensions, and marking key are hashed during embedding and used to modify the least-significant bit plane of the original image. This is done in such a way that when the correct detection side information and unaltered marked image are provided to the detector, a bi-level image chosen by the owner (such as a company logo), is observed. This technique has localization properties and can identify regions of modified pixels within a marked image. Roy *etal.* [5] found a tradeoff between the length of the hash and tamper localization and presented a robust image hashing method in which the hash is calculated from the features of the image. Besides authentication of the image, a variety of watermarking methods [1], [4], [6] are further developed to localize the tampered region. Image authentication methods, based on cryptography, use a hash function [7], [8] to compute the message authentication code (MAC) from images. The generated hash is further encrypted with a secrete key from the sender, and then appended to the image as an overhead, which is easy to be removed.

This paper proposed a new BCCW scheme for image authentication. The BCCW evaluates the checksum of the pixels of each block using simple method. The checksum is embedded into the selected pixels. The novelty of the proposed BCCW is the embedded image owns a very high embedding quality because of its hierarchical nature. The rest of this paper is organized as follows. In Section II, related works are illustrated briefly. In Section III, the proposed BCCW scheme is presented. Then, the experimental results are shown in section IV. Section V describes about tamper localization. Finally, conclusions of are given in Section VI.

II. RELATED WORK

Walton's [1] Authentication scheme was one of the first techniques used for image tampering detection based on inserting check-sums into the least significant bits (LSB) of the image data. The scheme computes an array of checksum as the authentication information out of the seven most significant bits (MSBs) of each pixel of the original image. The check-sum value is obtained by summing the numbers determined by the 7 most significant bits (MSB) of selected pixels. Then the check-sum bits are embedded in the LSB. The checking process is similar to the embedding process. It consists in comparing, for each block, the check-sum

Manuscript received on September, 2012.

L. Sumalatha, Associate Professor, Department of Computer Science and Engineering, University College of Engineering, JNTUK, Kakinada, AP, India.

G. Rosline Nesa Kumari, Associate Professor, Godavari Institute of Engineering and Technology, Rajahmundry, AP, India.

Dr. V.Vijaya Kumar, Dean of Computer Sciences, Godavari Institute of Engineering and Technology, Rajahmundry, AP, India.

determined by the MSB of the tested image with the original check-sum value recovered from the LSB. The main advantage of this method is that it does not produce visible changes in the image and provides a very high probability of tamper detection. After a careful study we found the following disadvantages of Walton's method.

However, there are several problems found in Walton's scheme:

i) An attack can exchange the pixels in a seal path that will not affect the checksum of the image. This form of tampering is not detected.
ii) The scheme cannot indicate the tampered location of the tampered image.
iii) The scheme cannot distinguish between an innocent adjustment and a malice replacement.

Chang *etal.* [6] proposed an authentication method based on fragile watermarking. At first the image is divided into 3x3 overlapping blocks. The center pixel of each block is embedded with the cryptographic hash of the features of the corresponding block. The feature of a block consists of the eight neighboring pixels, the index of the block, the height and width of the image and the user's secret key. A cryptographic hash of the feature of the block is calculated using MD5. Let X is the center pixel in which the data is embedded. The 8-neighbors of the center pixel are P1, P2,.., P8 as shown in Fig 1.

P_3	P_2	P_1
P_4	**X**	P_8
P_5	P_6	P_7

Figure. 1 The embedded pixel X and its eight neighbors.

The cryptographic hash of the block is given by,

$$H(B_i) = \left(P_1||P_2||\ldots.||P_8||i||ID||K_u\right) \quad (1)$$

Where $\|\cdot\|$ denotes concatenation, Bi is the i^{th} block of the image, 'i' is the block number, ID is the image identity and Ku is the user secret key. The hash of each block is obtained, and is embedded into r least significant bits (LSBs) of the pixel X, where $2 \le r \le 4$. The value of r is determined by the block variance (σ),

$$\sigma = \sum_{i=1}^{8}(P_i - P_{i+1 \bmod 8})^2 \quad (2)$$

$$r = \begin{cases} 2, & 0 \le \sigma < 8 \\ 3, & 8 \le \sigma < 16 \\ 4, & 16 \le \sigma < 255 \end{cases} \quad (3)$$

The present study found that this scheme is also not suitable for the purpose of image authentication because it suffers with the following disadvantages.

i) The content authentication of 9 pixels is placed in the form of one bit in the center pixel of a 3×3 block. This results a very poor content authentication.
ii) This method is using block variance which is a complex operation when compared to block average.
iii) It is complex in nature due to the use of MD5 for finding checksum.
iv) The block features calculated do not depend on the watermarked pixel.
v) The computation of the block variance (σ) does not depend on the watermarked pixel; hence it is the same for both the tampered watermarked pixel and the non-tampered watermarked pixel.

III. PROPOSED BCCW METHOD

To overcome the above drawbacks of Walton's scheme [1] scheme and Chang *et al.* [6], the present paper proposed a BCCW method which embeds the checksum computed on the block B_i into the 2x2 sub block that has the maximum average compared to other sub blocks of the block. By this any change in the watermarked block results in a wrong checksum. The present paper has not considered the variance of the block for finding the r value as it changes if the pixels in the block change.

The proposed BCCW method for authentication is shown in Fig 2. The shaded region is the watermarked pixels. Four bits of watermark is embedded into four pixels.

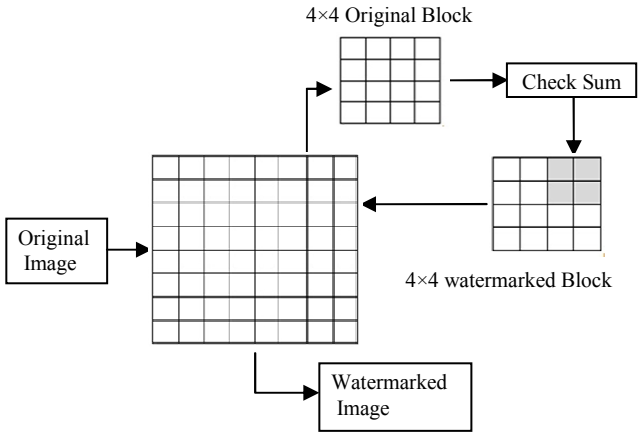

Figure. 2 Block Diagram of proposed BCCW watermarking method

The checksum computation of the proposed BCCW method is based on Walton's method [8]. The BCCW modifies the Walton's scheme by dividing the original image into 4x4 blocks. Then a hierarchical relation is established in the BCCW by dividing into 2×2 blocks, which is not there in Walton's method.

A. Embedding

The watermark embedding process of the proposed BCCW scheme consists of seven steps, which are given below.

Step 1: A grayscale image I of M × N pixels is divided into non- overlapping blocks of size 4×4.
Step 2: In each 4×4 block, the 7th bit plane of each pixel XORed with one bit of the 16 bit secret key and the result is stored in the 7th bit plane itself.
Step3: The check sum C(S) of BCCW for each watermarked block is calculated by the following algorithm:

Algorithm: Checksum Computation

(1) For each block B:
  (i) Denote the pixels in the block as $(P_1, P_2, \ldots\ldots, P_{16})$
  (ii) Generate a pseudorandom sequence of 16 integers $n_1, n_2, n_3 \ldots n_{16}$ in a range of [0, N] controlled by a secret key.
  (iii) The check-sum value CS is calculated as

$$CS = \sum_{i=1}^{16} n_i \cdot f(P_i) \bmod N \quad (4)$$

Where N is an odd number and should be chosen in such a way that CS should be of 8 bits, $f(P_i)$ is the grey-level of the pixel P_i (determined by the 7 MSB).

This binary sequence of the checksum (8 bits) is folded to form 4 bits of content watermark (CW). The folding operation involves the XOR of two consecutive bits into one bit.

Step 4: Divide each 4×4 block into four 2×2 non-overlapping sub blocks. Let the sub blocks of a block B_i be B_i^1, B_i^2, B_i^3 and B_i^4.

Step 5: The average intensity of each sub block is computed. Let the average intensities be A_i^1, A_i^2, A_i^3 and A_i^4.

Step 6: The sub block with the maximum average intensity is considered for embedding. If two or more sub blocks show the maximum average intensity then the first block from the top left is chosen.

Step 7: The sub block B_i^j selected for embedding consists of four pixels,P_1,P_2, P_3 and P_4. Into the LSB's of these pixels one bit of the content watermark is embedded by,

$$P_i' = 2 * \left\lfloor \frac{P_i}{2} \right\rfloor + CW_i \quad (5)$$

Each block results in a watermarked block B'.

B. Extraction

The extraction process of BCCW consists of six steps.

Step 1: The watermarked image (W) is divided into 4x4 non-overlapping blocks.

Step 2: Divide each block into 2×2 non-overlapping sub blocks. Let the sub blocks of a block be BW_i be BW_i^1, BW_i^2, BW_i^3 and BW_i^4.

Step 3: The average intensity of each sub block is computed. Let the average intensities be Aw_i^1, Aw_i^2, Aw_i^3 and Aw_i^4.

Step 4: The sub block with the maximum average intensity contains the content watermark. From the sub block Aw_i^j from the four pixels,Pw_1, Pw_2, Pw_3 and Pw_4 the content watermark is extracted by,

$$b_i = \mathrm{mod}(Pw_i, 2) \quad (6)$$

Step 5: The checksum can be recomputed on the image block using (4) and compared with content watermark. The similarity of the both indicates that the block is not modified maliciously.

Step 6: To recover the original pixels from the watermarked pixel the 7th bit of the watermarked pixel is XORed with the corresponding bit of the 16 bit secret key.

Experimental Results

The proposed BCCW method is applied on eight 8-bit gray scale images like Lena, Cameraman, Peppers, House, Living room, Baboon, Jet plane and Tiffany of size 256x256. The digital watermarking image quality parameters PSNR and NCC are applied on the proposed BCCW method. The PSNR value is defined by (7),

$$PSNR = 10 \log_{10} {}^{255^2}/_{MSE} \text{ dB} \quad (7)$$

Here, 255 represent the maximum value of each pixel and the mean square error (MSE) for an image is defined in (8).

$$MSE = \left(\frac{1}{H*W}\right) \sum_i^H \sum_j^W \left(X_{ij} - X'_{ij}\right)^2 \quad (8)$$

Here, notations H and W represent the height and width of an image, respectively, x_{ij} is the pixel value of the coordinate (x, y) of an original image and x'_{ij} is the pixel value after hiding processing. In general, the higher the PSNR value of a stego-image, the better the image quality. In contrast, once the image quality of a stego-image is worse, its PSNR value is small. Basically, with human vision alone, it is difficult to distinguish a stego-image from its original when the PSNR value is ≥ 30 dB.

To verify the robustness Normalized Correlation Coefficient (NCC) is used by the BCCW method which is defined in (9). Using NCC if the similarity value is nearer to 1 then it is considered as acceptable.

$$NCC = \frac{\sum_{i=0}^{N-1} W(i) \times W'(i)}{\sum_{i=0}^{N-1} (W(i))^2} \quad (9)$$

Where W(i) and W′(i) are the original and extracted watermarks. Table I Shows the PSNR and NCC values of the test images, and it is clear that the PSNR values are ≥ 50dB and the NCC is nearer to 1.

Figure. 3 Original images- Lena, Cameraman, Peppers, House, Living room, Baboon, Jet Plane, Tiffany.

Figure .4 Watermarked images- Lena, Cameraman, Peppers, House, Living room, Baboon, Jet Plane and Tiffany.

I. PSNR AND NCC VALUES OF THE IMAGES BY APPLYING THE PROPOSED (BCCW) SCHEME.

Image	PSNR(dB)	NCC
Lena	52.612	1
Cameraman	52.639	0.98
Peppers	52.648	0.98
House	53.259	0.97
Living room	52.646	1
Baboon	52.618	0.98
Jet plane	52.643	0.97
Tiffany	52.666	0.99

In Table II, a comparison of the proposed BCCW method with other existing methods like Chang *etal.* [6], P.L.Lin *et al.*[9] and S.Bravo-Solario *etal.*[10] is performed. The PSNR value of the proposed method is better than these methods even after embedding 4bits of the checksum into each 4×4 block. The tamper detection is almost 100% for all the methods. Chang's *etal.*[6] method detects the tamper 100% subjected to the probability of a tampered block which is embedded with r bits of watermark passing the detection test as correct block is $\left(\frac{1}{2}\right)^{r}$ where $2 \le r \le 4$. P.L.Lin *etal.* [9] method detects 100% of tampered blocks only if the block size is 12×12, for smaller block size like 4×4, the missing rate less than 0.37%. The proposed BCCW method uses 4×4 blocks and the detection rate is local to the corresponding block and hence localizes the tamper with 100% accuracy.

II. COMPARISON OF THE PROPOSED BCCW METHOD WITH CHANG ET AL. [6], P.L.LIN ET AL. [9], BRAVO-SOLARIO ET AL. [10] METHODS.

Quality Factors	Chang et al. method	P.L.Lin et al. method	S. Bravo-Solorio et al. method	Proposed BCCW method
PSNR(dB)	48.44	44.37	41	52.71
Tamper Localization	100%	100%	99%	100%

III. TAMPER LOCALIZATION

Figure 5 shows an example of the effectiveness of the proposed BCCW method in localizing image tampering. The proposed BCCW method detects any form of tampering, namely, insertions, deletions, exchange of patches in the image. The idea is that any intentional tampering leaves behind significant addition or deletion of content information, primarily edge boundary information. The resolution of the patch detection depends on the size of the image blocks considered for tampering and hence affects the check sum of the tampered blocks.

Figure.5 Tamper Localization –Baboon, Tampered Baboon, Tampered region of Baboon, Living Room, Tampered Living Room, Tampered region of Living Room.

The PSNR values of the four images namely Baboon, Lena, Jet plane and Living room after embedding and after recovering are given in Table 3. The PSNR values of the recovered image are a good indication of the efficiency of the proposed scheme. Table III also shows the number of blocks that are tampered and the detection rate of the tamper blocks. As the content watermark of a block embedded by proposed system is local to that block, the block that is tampered gives a wrong checksum. By this the tamper is identified very clearly. Hence, the detection rate is almost 100% for the proposed BCCW scheme.

IV. INFORMATION OBSERVED WHILE EMBEDDING AND DETECTION RATE OF TAMPER.

Image	PSNR (dB) (Embed-ding)	Tampered Blocks	Detection Rate	PSNR (dB) (Recovered)
Baboon	52.61	100	99%	39.13
Lena	52.61	225	99%	36.70
Jet Plane	52.64	155	99%	36.66
Living room	52.64	25	99%	40.69

V. CONCLUSIONS

In this paper, BCCW is proposed, in which the checksum is calculated on the pixels of the block using a secret key. This is defined by the person who owns a valid secret key and thus it provides the rightful ownership of others in this image authentication scheme. In other words, it is impossible for people to pass the ownership test without the secret key. In Walton's method [2] predefined seal paths are used for embedding data but any malicious replacement of the pixels in seal paths goes undetected. This is overcome by the BCCW method by a key based selection of pixel pairs for embedding. Also the proposed BCCW method does not perform complex computations like MD5 and variance as used in Chang etal. method [6]. The proposed scheme is simple and can easily detect the tampered locations in the size of 4×4 blocks. Unlike Walton's method and Chang et al. method, the BCCW method recovers the original pixels and checks the integrity of the corresponding block by re-computing the checksum and comparing with that of extracted content watermark. The proposed BCCW does not produce any visible changes in the image by content and digital watermark authentication and provides a very high probability of tamper detection. The PSNR, NCC values and detection rate of tamper of the proposed BCCW method is compared with various other methods. The results clearly indicate the efficacy of the proposed BCCW method when compared to the recent existing methods.

VI. ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their valuable comments. The authors express deep sense of gratitude to Dr. G.Tulasi Ram Das, Honorable Vice Chancellor, JNTUK for encouraging Research and Development. The authors express their gratitude to Dr.E.V.Prasad, Registrar, JNTUK and Dr.J.V.R. Murthy, Chairman, BOS, JNTUK for their sincere suggestions. Also 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.

REFERENCES

[1] Schyndel, R.G., Tirkel, A.Z., Osborne, C.F.,"A digital watermark", In Proceedings of the IEEE International Conference on Image Processing, Austin, Texas, 1994,vol. 2, pp. 86–90.
[2] Walton, S. "Information authentication for a slippery new age", Dr. Dobbs J. 1995, 20 (4), pp.18–26.
[3] Wolfgang, R.B., Delp, E.J., "A watermark for digital images", In Proceedings of IEEE International Conference on Image Processing, Lausanne, Switzerland, 1996, vol. 3, pp. 219–222.
[4] Wong, P.W., "A public key watermark for image verification and authentication." In Proceedings of IEEE International Conference on Image Processing, Chicago, IL, 1998. vol. 1, pp. 425–429.
[5] Sujoy Roy and Qibin Sun, "Robust hash for detecting and localizing image tampering", in Proc. IEEE International Conference on Image Processing, Sep 2007.
[6] C.-C. Chang, Y.-S. Hu, T.-C. Lu, "A watermarking-based image ownership and tampering authentication scheme", in Pattern Recognition Lett. 2006, 27 (5), pp.439--446.
[7] V. Skala and M. Kucha, "The hash function and the principle of duality" in Proceedings of Computer Graphics International 2001, pp. 167–174.
[8] S. Halevi and H. Krawczyk, Strengthening digital signatures via randomized hashing, Advances in Cryptology-CRYPTO 2006, pp. 41–59.
[9] P.L.Lin, C.H., Hsieh, W.S., "Applying projection and B-spline to image authentication and remedy" in IEEE Trans. Consumer Electron. 2003., 49 (4), pp.1234–1239.
[10] Sergio Bravo-Solorio and Asoke K. Nandi." Fragile watermarking with improved tampering localization and self-recovery capabilities". In EUSIPCO 2010, pp.820-824.

L.Sumalatha recieved her B.Tech from Acharya Nagarjuna University, Guntur in the year 2000 and M.Tech(CSE) from JNT University, Hyderabad in the year 2004. At present she is working as Associate Professor in Dept of Computer Science and Engineering, University College of Engineering, JNTUK, Kakinada. She is having teaching experience of about 12years and has taught many courses to UG and PG Students. She is pursuing her Ph. D from JNT University Kakinada. Her research areas includes Information Security and Digital image Processing.

G Rosline NesaKumari 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 Under the Guidance of Dr V VijayaKumar Professor & Dean of Computer Sciences – GIET. 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 Sixteen 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.

Dr. Vakulabharanam VijayaKumar received integrated M.S.Engg, degree from Tashkent Polytechnic Institute (USSR) in 1989. He received his Ph.D. degree in Computer Science from Jawaharlal Nehru Technological University (JNTU) in 1998. He has served the JNT University for 13 years as Assistant Professor and Associate Professor and taught courses for M.Tech students. He has been Dean for Dept of CSE and IT at Godavari Institute of Engineering and Technology since April, 2007.His research interests include Image Processing, Pattern Recognition, Network Security and Steganography, Digital Watermarking, and Image retrieval. He is a life member for CSI, ISTE, IE, IRS, ACS and CS. He has published more than 120 research publications in various National, Inter National conferences, proceedings and Journals.