A FRAGILE WATERMARKING BASED ON BINOMIAL TRANSFORM IN COLOR IMAGES

J. K. Mandal and S. K.Ghosal

Department of Computer Science and Engineering,
Kalyani University, Kalyani,
West Bengal, India, 741235.
{jkm.cse@gmail.com, sudipta.ghosal@gmail.com}
http://www.klyuniv.ac.in;http://www.jkmandal.com/

ABSTRACT

In this paper, a novel Binomial Transform based fragile image watermarking technique has been proposed for color image authentication. The Binomial Transform (BT) is used to convert each 2 × 2 sub-image block of the carrier image into transformed block corresponding to red, green and blue channels in sliding window manner. One/two/three watermark bits are embedded in second/third/fourth transformed components starting from the least significant bit's position (LSB-0). An adjustment has been incorporated to adjust embedded component closer to the actual value without hampering the fabricated bits. The inverse Binomial transform (IBT) is used to convert the transformed components back into the spatial domain. A delicate re-adjustment method is applied on the first transformed component to remain the pixel components in a valid range. The embedding operation in succession generates the final watermarked image. At the receiving end, whole watermark is extracted based on the reverse procedure and authentication is done through computed message digest and extracted bits. Experimental results conform that the proposed technique produces high payload and Peak Signal to Noise Ratio (PSNR) as compared to existing transformation based techniques[1, 5].

KEYWORDS

BT, IBT, LSB-0, Payload, PSNR, Authentication and Message digest.

1. INTRODUCTION

Digital watermarking is a technique of incorporating useful information into various digital media like image, audio and video etc. for ownership evidence, fingerprinting, authentication and integrity verification. The objective of this paper is to verify the integrity of a carrier image based on a novel fragile watermarking technique in transform domain.

Various transformations are applied to convert the carrier image from spatial domain to transform domain in a block wise manner. Each block contains a set of transformed components which can

Jan Zizka (Eds) : CCSIT, SIPP, AISC, PDCTA - 2013
pp. 281–288, 2013. © CS & IT-CSCP 2013 DOI : 10.5121/csit.2013.3632

be slightly modified to embed the watermark data. The watermarked image can be obtained by applying the respective inverse transformation. A separable discrete Hartley transform based invisible watermarking scheme[1] has been proposed by Mandal & Ghoshal. The SDHTIWCIA scheme exploits for image authenticating purpose by fabricating the authenticating watermark data along with the message digest (which is generated from authenticating data) into the carrier image with a minimal loss of quality and improved security.

The effectiveness of different watermarking methods can be measured in terms of payload, peak signal to noise ratio and image fidelity etc. In this regard, the Binomial transformation [2-3] has been applied for embedding watermark data into the cover image with a high payload and less degradation in quality. Moreover, a 128 bit message digest has been used for authentication purpose[4,5]. On embedding authenticating watermark (message/image) bits, inverse Binomial transformation is applied to re-generate the watermarked image in spatial domain.

The binomial transform (BT) is applied on pixel components $\{a_n\}$ to generate transformed components $\{s_n\}$ as per equation (1).

$$s_n = \sum_{k=0}^{n} (-1)^k \binom{n}{k} a_k. \tag{1}$$

Similarly, the inverse Binomial transform (IBT) is used to convert transformed components back into pixel domain as per equation (2).

$$a_n = \sum_{k=0}^{n} (-1)^k \binom{n}{k} s_k. \tag{2}$$

The main objective of proposed technique emphasizes on color image authentication by protecting secret watermark. The message digest MD (which is generated from watermark data) is used for authentication by verifying the integrity of the carrier image.

Section 2 of the paper deal with the proposed technique. Results, comparison and analysis are given in section 3. Conclusions are drawn in section 4. References are given at end.

2. THE TECHNIQUE

In this paper, a novel color image authentication technique has been proposed based on Binomial transform. The message digests (MD) is obtained from the authenticating watermark (message/image). The message digests and the size of the authenticating watermark is embedded using the proposed technique as an initial embedding. The Binomial transform (BT) has been applied on each 2 × 2 sub-image block of the carrier image to convert the pixel components into transformed components in row major order. One/two/three bits from the message digest, watermark size and the watermark are embedded on second/third/fourth transformed components starting from the least significant bits position (LSB-0). An adjustment method has been applied into each embedded component to reduce the changes made due to embedding. An inverse Binomial transform (IBT) has been applied on each adjusted component to get back the pixel components. During the IBT, if the pixel component becomes negative or greater than 255, a re-

adjustment operation is to be performed on the first transformed component repeatedly, till the pixel component become greater than or equal to 0 and less than or equal to 255. The procedure is applied for red, green and blue channel separately and the process continues till the final watermarked image is produced. The recipient of the watermarked image is instructed to perform the reverse operation to extract the watermark bits stream. The new message digest MD' can be calculated from the extracted watermark bits and the same is compared with extracted MD for authentication.

Section 2.1 depicts the insertion technique.The re-adjustment of first transformed component has been described in section 2.2 and the algorithm for extraction is given in section 2.3.

2.1 Insertion

Each 2 x 2 sub-matrices of the carrier image is converted into transformed components by applying Binomial transform (BT) in a channel wise manner. One/two/three watermark bits are embedded in second/third/fourth transformed components. An adjustment has been used to reduce quality degradation by adjusting the embedded components without affecting the fabricated bits. The inverse Binomial transform (IBT) is used to convert back the adjusted components into pixel components.

Algorithm:

Input: The *128* bits message digest *MD*, derived from the authenticating watermark, the carrier/cover image (I) and an authenticating watermark (message/image).

Output: The watermarked image (I′) in spatial domain.

Methods: The watermark (along with a message digest) is inserted into the carrier images by converting the image from spatial domain to transform domain using Binomial transform (BT). The detailed steps of embedding are as follows:

Steps:

1. Obtain *128* bits message digest *MD* from the authenticating watermark which may be a textual message or an image.

2. Calculate the size of the authenticating watermark ((*L* = *w* + *h*), where *w* bits for width and *h* bits for height). The authenticating watermark (W) bits size is:

$$W_{size}=[B \times \{3 \times (M \times N)\} - (MD + L)]$$

   Where, the bits per byte (*B)* is *1.5*; *MD* and *L* are the message digest and dimension of the authenticating watermark respectively for the carrier image of size *M* x *N* bytes. In our proposed technique, the *MD* and *L* consist of 128 and 32 bits.

3. Repeat step 3 until the message digests MD, the authenticating watermark size (W_{size}) and the authenticating watermark (W) is embedded.

   a. The cover image (I) is partitioned into 2 x 2 non-overlapping blocks in row major order. Each 2 x 2 sub-matrix (S_c) consists of four pixel components corresponding to each channel.

b. The Binomial transform (BT) of equation (1) has been applied to convert each pixel components into transformed components.

c. One/two/three bits from the message digest (MD), watermark size (W_{size}) and the watermark (W) are embedded on second/third/fourth transformed components starting from the least significant bits position (LSB-0). Generally, if a transformed component t consists of k bits and the number of bits inserted is r, then the embedded transformed component t' becomes:

$$t' = \{(t \,\&\, (2^k - 2^r)) \mid d$$

The decimal value d, corresponding to r bit authenticating watermark, can be expressed in binary form as, $d = (a_{r-1}a_{r-2}a_{r-3}\ldots\ldots\ldots a_{r-k})_2$, where for a positive integer i, the value of $(r-i)$ must be greater than or equal to 0, i.e., $(r-i) \geq 0$.

d. A quality adjustment has been applied to get transformed component closest to the original without hampering the fabricated bits. The adjustment has been done by altering left most $(k-r)$ bits and choosing the closest one of the original.

e. The adjusted components are converted back into the spatial domain using inverse Binomial transform (IBT) of equation (2). During the inverse Binomial transform (IBT), if any pixel component becomes negative or greater than 255, then a transformed component re-adjustment methodology is applied on the first transformed component discussed in section 2.2.

4. The successive bit embedding operations on each 2 x 2 sub-image block produces the watermarked image (I′).

5. Stop.

2.2 Re-Adjustment

The Binomial Transform (BT) is used to convert the pixel components into transformed components which can fabricate the authenticating watermark. The inverse Binomial transform (IBT) may generate two serious problematic situations:

- The pixel component value may by negative (-ve).
- The pixel component value may be greater than the maximum value (i.e. 255).

The first situation can be handled by incrementing the first transformed component with one while the second situation can be avoided by decrementing the first transformed component with two, repeatedly.

2.3 Extraction

The watermarked image (I') is received in spatial domain. During extraction, the watermarked image has been taken as the input and the authenticating watermark size, content and message digest MD are extracted. All extraction is done in transform domain from the transformed components through reverse operation.

Algorithm:

Input: The watermarked image (I′).

Output: The watermark image (W) and the message digest.

Methods: The Binomial transform (BT) is used to extract the watermark (along with a message digest) from the watermarked image by converting the image from spatial domain to transform domain. Successive extracted bits forms the watermark data and generate a message digest which can be used for authentication. The detailed steps of extraction are as follows:

Steps:

1. Repeat step 1, until and unless the 128 bits message digest (MD), watermark size(W_{size}) and the authenticating watermark is extracted.
   - **a.** The watermarked image *(I′)* is partitioned into 2 x 2 non-overlapping blocks in row major order. Each 2 x 2 sub-matrix (S_c) consists of four pixel components corresponding to each channel.
   - **b.** The Binomial Transform (BT) of equation (1) has been applied to transform each pixel components block (S_c) into transformed components.
   - **c.** One/two/three bits of the message digest (MD), watermark size (W_{size}) and the watermark(W) are extracted from second/third/fourth transformed components starting from the least significant bits position (LSB-0). Each 8 (eight) bits extraction ensures the construction of one alphabet/color component (R/G/B).
   - **d.** After extracting watermark bits, the transformed components are converted back into the spatial domain using inverse Binomial transform (IBT) of equation (2). Thus, the spatial domain sub-image block (S'_c) is consists of four pixel components while the bits are fabricated in transform domain.
2. Obtain *128* bits message digest *MD′* from the extracted watermark.
3. Compare *MD′* with extracted *MD*. If both are same then the image is authorized, else unauthorized.
4. Stop.

3. RESULTS, COMPARISON AND ANALYSIS

Benchmark (PPM) images [4] of dimension 512 × 512 are taken to embed the gold coin (i.e. the authenticating watermark image). Ten different color images (i-v) are taken. Images are labeled as: (i) Lena, (ii) Baboon, (iii) Pepper, (iv) Earth, (v) Sailboat. On embedding the watermark image i.e., the Gold-Coin image of (vi), the newly generated watermarked image produces a good visual clarity.

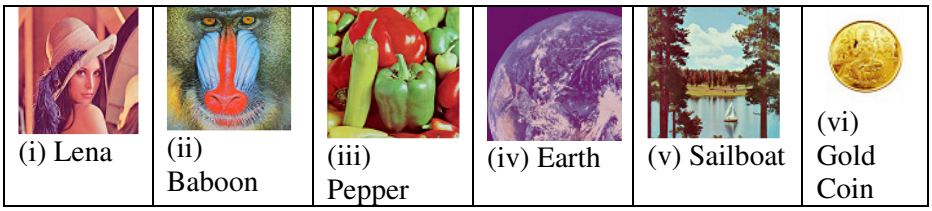

Figure 1. Different Cover images of dimension 512 × 512 along with the Authenticating Watermark Image

It is seen from table 1 that the watermarked images have a peak to signal noise ratio (PSNR) of around 42 dB in average case whereas the average bits per byte (bpb) for a given carrier image is 1.5.

Table 1. Results of embedding of 147234 bytes of information in each image of dimension 512 x 512

Carrier Image	**Max. Payload (byte)**	**PSNR**	**IF**	**BPB**
Lena	147456	41.40	0.9997	1.5
Baboon	147456	42.05	0.9998	1.5
Pepper	147456	41.28	0.9996	1.5
Earth	147456	41.61	0.9997	1.5
Sailboat	147456	41.67	0.9998	1.5
AVG	**147456**	**41.55**	**0.9997**	**1.5**

On comparing the proposed technique with the SDHTIWCIA technique [1] and Varsaki et. al's [5] method, one can easily identify the enhancement of the PSNR at the same and higher payload.

Table 3. Comparison of BPB and PSNR for proposed technique over SDHTIWCIA [1] and Varsaki et. Al's [5] method

Carrier Images	**Varsaki et. al's Method [5]**		**SDHTIWCIA [1]**		**Proposed Technique**	
	BPB (bits per byte)	**PSNR (dB)**	**BPB (bits per byte)**	**PSNR (dB)**	**BPB (bits per byte)**	**PSNR (dB)**
Lena	0.25	39.70	1.5	37.95	1.5	41.40
Baboon	0.25	30.69	1.5	38.57	1.5	41.28
Sailboat	0.25	35.28	1.5	38.23	1.5	41.67
AVG	***0.25***	***35.22***	***1.5***	***38.25***	**1.5**	**41.45**

The histogram analysis ensures the minimal changes in the watermarked images. Fig-3 depicts the histogram of 'Lena' image before and after embedding the 'Gold Coin' a separate channel wise manner.

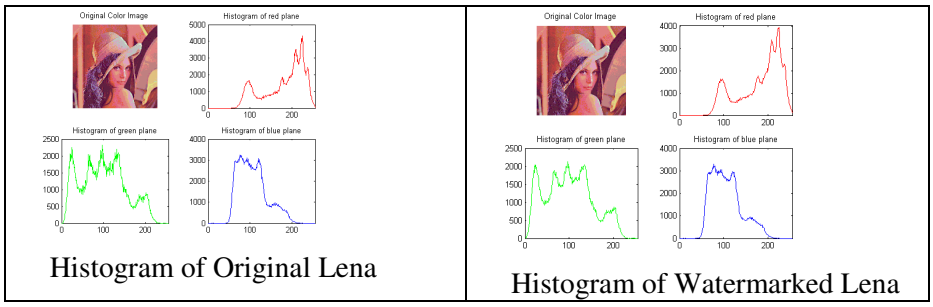

Figure 3: Comparisons results of histogram between of original and watermarked image

It is seen from table 4 that the differences of mean, standard deviation and median between original and watermarked images are very minimal.

Table 4. Comparison results of Mean, Median and Standard Deviation of original and watermarked images

Image	Channel	Mean	Standard Deviation	Median
Original Lena	R	180.22	49.05	197
	G	99.05	52.88	97
	B	105.41	34.06	100
Watermarked Lena	R	180.16	49.07	196
	G	99.01	52.90	98
	B	105.37	34.11	100

In this authentication system, the recipient operate the authentication process through matching of the extracted message digest MD with the generated message digest MD' at the destination, where MD' can be obtained from the extracted watermark image. If the extracted message digest MD matches with the generated message digest MD', then the authentication process is said to be successful, otherwise, it is said to be unsuccessful. That means any kind of attack on the watermarked image is easily detectable.

The PSNR (Peak Signal to Noise Ratio) and NCC (Normalized Cross-correlation) values are obtained from the watermarked images which are seen from table 5 by introducing attacks namely 'Median Filtering', 'Speckle Noise' and 'Salt & Pepper Noise'. It also ensures that the qualities of attacked watermarked images are still well perceptible but the message digest ensures that it is tampered.

Table 5. Comparison of PSNR and NCC values under different kinds of attacks for watermarked images

Images	PSNR	NCC	PSNR	NCC	PSNR	NCC	PSNR	NCC
	Before attack		After Median Filtering attack (3 x 3 neighborhood)		After Speckle Noise attack (Variance = 0.001)		After Salt & Pepper Noise attack (Noise Density=0.001)	
Lena	41.40	0.9996	33.64	0.9960	34.19	0.9996	34.52	0.9995
Pepper	41.28	0.9996	31.84	0.9937	34.74	0.9997	34.00	0.9996
Sailboat	41.67	0.9998	28.52	0.9936	34.20	0.9996	34.35	0.9996

4. CONCLUSION

The proposed technique can be used to authenticate a color image by embedding watermark in transformed components. Higher robustness is achieved by fabricating data in positive and negative transformed components. The technique emphasizes on the improvement over SDHTIWCIA [1] and Varsaki et. Al's method [5].

ACKNOWLEDGEMENT

The authors express deep sense of gratuity towards the Dept of CSE University of Kalyani where the computational resources are used for the work and the PURSE scheme of DST, Govt. of India
.

REFERENCES

[1] Mandal J.K, Ghosal, S.K "Separable Discrete Hartley Transform based Invisible Watermarking for Color Image Authentication (SDHTIWCIA)", Second International Conference on Advances in Computing and Information Technology (ACITY-2012), July 13-15, Vol. 2, ISBN-978-3-642-31551-0, pp. 767-776, Chennai, India, 2012.

[2] Borisov B. and Shkodrov V., Divergent Series in the Generalized Binomial Transform, Adv. Stud. Cont. Math., 14 (1): 77-82, 2007.

[3] S. Falcon and A. Plaza, "Binomial transforms of the k-Fibonacci sequence", International Journal of Nonlinear Sciences and Numerical Simulation 10(11-12): 1527-1538, 2009.

[4] Allan G. Weber, The USC-SIPI Image Database: Version 5, Original release: October 1997, Signal and Image Processing Institute, University of Southern California, Department of Electrical Engineering. http://sipi.usc.edu/database/ (accessed on 25th January, 2010).

[5] Varsaki et al, "On the use of the discrete Pascal transform in hiding data in images", "Optics, Photonics, and Digital Technologies for Multimedia Applications", Proc. of SPIE Vol. 7723, 77230L • © 2010 SPIE • CCC code: 0277-786X/10/$18 • doi: 10.1117/12.854220, 2010.