BINOMIAL TRANSFORM BASED IMAGE AUTHENTICATION (BTIA)

S. K.Ghosal[1] and J. K. Mandal[2]

[1] Department of Computer Science and Engineering, Greater Kolkata College of Engineering & Management, Baruipur, West Bengal, India
sudipta.ghosal@gmail.com
[2]Department of Computer Science and Engineering, Kalyani University, Kalyani, West Bengal, India
jkm.cse@gmail.com

ABSTRACT

In this paper, a fragile watermarking technique based on Binomial transform (BT) has been proposed for color image authentication (BTIA). An initial adjustment is applied to adjust the pixel values. The Binomial transform (BT) is applied to convert each pair of pixel components into transform domain in row major order. Two bits of the authenticating watermarks, starting from the least significant bit position are embedded into each component of transformed pair. A post-embedding adjustment has also been incorporated to keep the embedded component values closest to the original without hampering the embedded watermark bits. The inverse Binomial transform (IBT) is applied on each adjusted pair to re-generate the pixel components which successively produce the watermarked image. At the receiving end, the whole watermark can be extracted by the reverse procedure which can be verified for authentication by obtaining a message digest. Experimental results conform that the proposed technique offers a higher payload and PSNR over existing techniques [7, 9].

KEYWORDS

BTIA, BT, IBT, Payload, PSNR and Watermarked image.

1. INTRODUCTION

Security of digital information in the form of text, audio, video etc. is become an important issue for today's world. Digital media can be protected through different schemes like cryptography, steganography, watermarking etc. Digital watermarking is an idea of fabricating secret information into the carrier/cover media such as image, audio and video etc. for ownership evidence, fingerprinting, authentication and integrity verification. The objective of this paper is to authenticate a carrier image through a fragile watermarking technique where Binomial transform has been introduced for embedding purpose.

Various transformations are applied on the carrier image to convert it from spatial domain into transform domain for authentication. Some popular transform domain technique includes Quaternion Fourier Transformation (QFT) [1], discrete cosine transformation (DCT) [2], discrete wavelet transformation (DWT) [3], or discrete Fourier transform (DFT) [4] based watermarking where the transformed components are used to fabricate the secret data. Transformed components are modified slightly to embed the secret data while the watermarked image can be obtained by applying the respective inverse transformation on the modified components.

DOI : 10.5121/ijma.2013.5405

The effectiveness of various watermarking techniques can be measured in terms of payload, peak signal to noise ratio and image fidelity etc. In this regard, the Binomial transform [5-6] is an excellent choice for embedding watermark information. In [7], a Binomial transform based fragile watermarking technique is applied on each 2 x 2 image block where a 128 bit message digest is used for authentication purpose. The existing method [7] can be improvised by applying the Binomial transform on a pair of pixel components instead over a 2 x 2 pixel block. As a result, the payload can be enhanced significantly and the quality degradation becomes minimal. 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 $\{s_n\}$ using 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 back the transformed components into pixel domain using 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 and 3 of the paper discussed the formulation of the Binomial transform for a pair of pixel components and the proposed technique. Results, comparison and analysis are given in section 4. Conclusions are drawn in section 5. References are given at end.

2. TRANSFORMATION TECHNIQUES

The formulation can be derived by transforming each pair of pixel components (a_i, a_{i+1}) into a pair of transformed components (s_i, s_{i+1}) using the Binomial transform (BT) given in equation (3).

$$\begin{aligned} s_i &= a_i \\ s_{i+1} &= a_i - a_{i+1} \end{aligned} \tag{3}$$

where s_i and s_{i+1} represents the pair of transformed components corresponding to the pixel components a_i and a_{i+1}.

Similarly, by applying the inverse Binomial transform (IBT), each pair of transformed components (s_i, s_{i+1}) are converted back into the spatial domain which consists of pixel components a_i and a_{i+1} as per equation (4).

$$\begin{aligned} a_i &= s_i \\ a_{i+1} &= s_i - s_{i+1} \end{aligned} \tag{4}$$

3. PROPOSED TECHNIQUE

In this paper, a novel watermarking technique has been proposed based on the Binomial transform (BT) for color images. A message digests (MD), content of the watermark and the watermark size are embedded using the proposed technique. Each pair of pixel components of the carrier image is pre-processed for an initial adjustment, if necessary. The initial adjustment sets a new upper limit (i.e., 248) and a lower limit (i.e., 8) for a pixel component. This pre-embedding pixel adjustment strategy ensures that the pixel values on embedding the watermark must lie within the valid range ($0 \leq p \leq 255$). The Binomial transform (BT) is used to convert each pair of pixel components into transformed components in row major order. Each component of a transformed pair is capable of hiding two bits of the authenticating watermark starting from the least significant bit position (LSB-0). A post-embedding adjustment has been incorporated to keep the embedded transformed components closest to the original without hampering the fabricated watermark bits. The inverse Binomial transform (IBT) is applied on each adjusted components to produce the watermarked image in spatial domain. This process is continued till the last pixel pair of the carrier/cover image in a row major order. The authorized recipient extracts the watermark from the watermarked image through reverse process and new message digest (MD') are obtained from the extracted watermark bits. The same is compared with extracted message digests (MD) at the destination end for authentication.

Consider three pairs of pixel components corresponding to red, green and blue channels from a given cover/carrier image. Binomial transform (BT) is applied on each pair of pixel components to convert it into transformed components. Let, the three pair of pixel components are R_1, G_1 and B_1. The steps are as follows:

$R_1=\{164,63\}, G_1=\{253,57\}, B_1=\{71,5\}$

On initial adjustment, the pairs of pixel components become:

$R_1=\{164,63\}, G_1=\{248,57\}, B_1=\{71,8\}$

Applying Binomial transforms (BT) on each pair of pixel components, the obtained pairs of transformed components are as here under:

$TR_1=\{164,101\}, TG_1=\{248,191\}, TB_1=\{71,63\}$

Now, if we embed the binary stream of *010001110100* using the proposed technique, the embedded components pairs becomes:

$ETR_1=\{165,100\}, ETG_1=\{249,191\}, ETB_1=\{69,60\}$

The transformed adjustment method ensures that the bits which are not taking part in embedding can form a set of patterns of 0's and 1's followed by the fabricated bits. Consequently, the value closest to the original transformed component is chosen from all the possible combinations. So, after adjusted components are as here under:

$AETR_1=\{165,100\}, AETG_1=\{249,191\}, AETB_1=\{69,64\}$

Again, by applying inverse Binomial transform (IBT) on each pair of transformed components, the obtained pairs of pixel components are as shown below:

$F^{-1}AETR_1=\{165,65\}, F^{-1}AETG_1=\{249,58\}, F^{-1}AETB_1=\{69,5\}$

The process of embedding is repeated for each pair of pixel components and continued till the end of authenticating watermark bits. This section has been categorized into two parts namely the algorithm for insertion and the algorithm for extraction.

3.1. Insertion

Initially, each pixel component pair are pre-adjusted, if necessary and then converted into the pair of transformed components corresponding to red, green and blue channels based on Binomial transforms (BT). Each transformed component (R/G/B) can fabricate two bits at the least two significant bit positions (LSB-0 and LSB-1). A post-embedded processing has been incorporated to adjust the transformed components without hampering the embedded bits. Inverse Binomial transform (IBT) converts each pair of embedded as well as adjusted components into the pair of pixel components which in succession produces the final watermarked image.

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′).

Methods: The Binomial transform (BT) is used to fabricate the watermark (along with a message digest) into the carrier images by converting the image from spatial domain into transform domain. Embedding bits in transform domain offers high robustness and improved security. The detailed steps of embedding are as follows:

Steps:

1) A 128 bits message digest (*MD)* is obtained from the watermark to authenticate a color image.
2) The size of the authenticating watermark (L) can be expressed by equation (5).

$$W_{size}=[2 \times \{3 \times (m \times n)\} - (MD + L)] \quad (5)$$

where, the number of bits embedded per byte is *2, MD* and *L* are the message digest and dimension of the authenticating watermark for the m x n color image. The dimension *L* consists of 32 bits of which 16 bits for width and remaining 16 bits for height.

3) Read authenticating watermark message/image and perform the operations given below:
   - The carrier/host image *(I)* is partitioned into pair of pixel components namely p_j, p_{i+1} in row major order.
   - For each channel (Red/Green/Blue), reset the upper and lower limit of pixel component (p_c) to retain the value positive and less than, or equal to *255* before embedding watermark bits. That means,

$$p_c = \begin{cases} 248: p_c \geq 248 \\ = \\ 8: p_c \leq 8 \end{cases} \quad (6)$$

   - Apply Binomial transform (BT) on each pair of pixel components to generate transformed components pair consisting of components f_i and f_{i+1}.

- Two bits of the authenticating watermark size, content and the message digests are embedded in each transformed component of every transformed pair starting from the least significant bit position (i.e., LSB-0).
  [Embed authenticating watermark bits as per the above rules.]
- An adjustment has been incorporated to get transformed components closest to the original without hampering the embedded bits. The adjustment has been done by altering left most *(T-3)* bits followed by choosing the embedded component value closest to the original one where T is the total number of bits used to represent an embedded component.
- Apply inverse Binomial transform (IBT) on each pair of adjusted components to re-generate the pixel components pair in spatial domain.

4) Repeat step 3 until and unless the whole authenticating watermark size, content and the message digest MD is embedded. Successive pair of fabricated pixel pair produces the watermarked image (I′).
5) Stop.

3.2. Extraction

The authenticated watermarked image is received in spatial domain. The Binomial transform (BT) converts each pair of pixel components into transformed components. The watermark size, contents and the embedded message digests (MD) are extracted from each transformed component. A new message digest (MD') has been obtained from the extracted watermark which in turn compared with the extracted message digests (MD) for authentication.

Algorithm:

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

Output: The authenticating 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 in turn used for authentication. The detailed steps of extraction are as follows:

Steps:

1) The watermarked image (I') is partitioned into pair of pixel components namely p_j, p_{i+1} in row major order.
2) Read each pair of transformed components and do the following operations:
   - Apply Binomial transform (BT) on a pair of pixel components corresponding of Red/Green/Blue channel, to generate transformed components pair consisting of transformed components f_i and f_{i+1}.
   - Two bits of the authenticating watermark size, content and the message digests are extracted from each transformed component of every transformed pair starting from the LSB-0.
     [Extract authenticating message/image bit as per the above rules.]
   - For each 8 (eight) bits extraction, it constructs one alphabet/one primary (R/G/B) color component.
   - Apply inverse Binomial transform (IBT) on each pair of transformed components to convert back it into the spatial domain.
3) Repeat step 1 and 2 to complete decoding as per the size of the authenticating watermark.

4) Obtain 128 bits message digest MD′ from the extracted watermark. Compare MD′ with extracted MD. If both are same then the image is authorized, else unauthorized.
5) Stop.

4. RESULTS, COMPARISON AND ANALYSIS

Five different carrier/cover images [8] of dimension 512 × 512 are taken to incorporate the gold coin (i.e. the authenticating watermark image). Images are labelled as: (i) Lena, (ii) Baboon, (iii) Pepper, (iv) Earth and (v) Sailboat. On embedding the Gold-Coin image of (vi), the newly generated watermarked image produces a good visual clarity and huge payload.

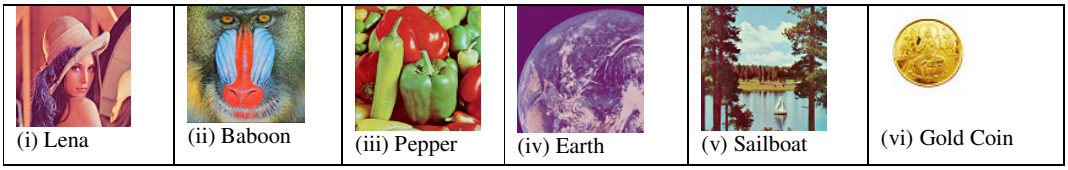

Figure 1. Different cover/carrier images of dimension 512 × 512 along with the watermark

It is seen from table 1 that the watermarked image has a peak to signal noise ratio (PSNR) of around 42 dB in average case whereas the bits per byte (bpB) for a given carrier image is 2.
Table 1. Results of embedding of 195638 bytes of information into each carrier image of dimension 512 x 512

Carrier Image	**Max. Payload (byte)**	**PSNR**	**IF**	**bpB**
Lena	196608	42.46	0.9998	2
Baboon	196608	42.46	0.9998	2
Pepper	196608	40.18	0.9995	2
Earth	196608	42.49	0.9998	2
Sailboat	196608	42.14	0.9998	2
AVG	*196608*	*41.94*	*0.9997*	*2*

Again, it is seen from table 2 that the PSNR and payload has been significantly improved in our proposed technique over the Mandal and Ghosal's existing technique [7] and Varsaki et al.'s [9] method.

Table 2. Comparison of bpB and PSNR for proposed technique over Mandal and Ghosal's [7] method and Varsaki et. Al's [9] method

Carrier Images	**Varsaki et al.'s Method [9]**		**Mandal and Ghosal's technique [7]**		**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	41.40	2	42.46
Baboon	0.25	30.69	1.5	42.05	2	42.46
Sailboat	0.25	35.28	1.5	41.67	2	42.14
AVG	*0.25*	*35.22*	*1.5*	*41.70*	*2*	*42.35*

The standard deviation analysis for varying sizes over the 'Lena' image is shown in figure 2. It ensures that the change made into the watermarked image using our proposed technique is really very minimal and almost identical to the original image.

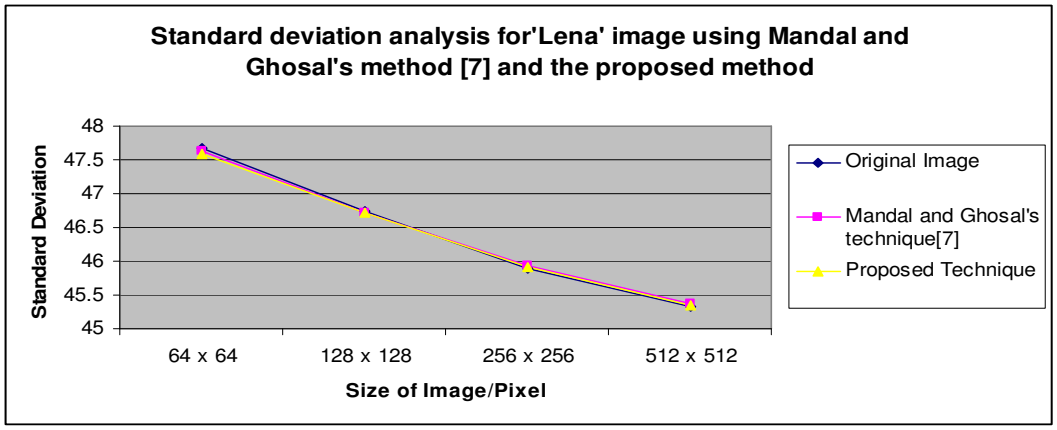

Figure 2: Comparison of standard deviation between source and watermarked 'Lena' image using Mandal and Ghosal's method [7] and the proposed technique

In this authentication system, the recipient operate the authentication process by matching the extracted message digest MD with the newly generated message digest MD', where MD' can be obtained from the extracted watermark image. If the extracted message digest MD matches with the newly generated message digest MD', then the authentication process is said to be successful, otherwise, it is unauthorized.

The PSNR (Peak Signal to Noise Ratio) and NCC (Normalized Cross-correlation) values are obtained from the watermarked images which is seen from table 3 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 3. Comparison of PSNR and NCC values of the watermarked images under different kind of attacks

Water-marked Images	**PSNR**	**NCC**	**PSNR**	**NCC**	**PSNR**	**NCC**	**PSNR**	**NCC**
	Before attack		**After Median Filtering attack (3 x 3 neighbourhood)**		**After Speckle Noise attack (Variance = 0.001)**		**After Salt & Pepper Noise attack (Noise Density=0.001)**	
Lena	42.46	0.9998	33.56	0.9968	34.38	0.9988	34.75	0.9987
Pepper	40.18	0.9995	31.56	0.9941	34.50	0.9985	33.82	0.9978
Sailboat	42.14	0.9998	28.49	0.9948	34.33	0.9988	34.49	0.9988

5. CONCLUSION

The proposed technique is an image authentication process in transform domain to enhance the security compared to the existing algorithm. Authentication is done by embedding watermark data in a carrier image. Using the technique two bits can be embedded in transformed components. Experimental results conform that the proposed algorithm performs better than existing techniques [7, 9].

ACKNOWLEDGEMENT

The author expressed deep sense of gratitude to the PVRSE scheme of DST, Govt. of India through which the experimental setup has been used for the research at the department of computer science and engineering, University of Kalyani.

REFERENCES

[1] Pei S.C., Ding J.J., Chang J.H., "Efficient Implementation of Quaternion Fourier Transform, Convolution, and Correlation by 2-D Complex FFT", IEEE TRANSACTIONS ON SIGNAL PROCESSING, VOL. 49, NO. 11, pp 27-83, 2001.

[2] N. Ahmed, T. Natarajan and K. R. Rao, "Discrete cosine transform," IEEE Transactions on Computers, Vol.C-23, pp.90-93, 1974.

[3] Rioul and P. Duhamel, "Fast algorithms for wavelet transforms," IEEE Transaction on Information Theory, Vol.38, No.2, pp.569-586, 1992.

[4] E. O. Brigham, "The fast Fourier transform," Englewood Cliffs, NJ: Prentice-Hall, 1974.

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

[6] 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.

[7] Mandal, J. K., Ghosal S. K., "A Fragile Watermarking based on Binomial Transform in Color Images", Proceedings of Third International Conference on Computer Science & Information Technology (CCSIT 2013), ISBN : 978-1-921987-00-7, Feb.18-20, 2013, Bangalore, India., DOI : 10.5121/csit.2013.3632, Volume 3, Number 6, 2013, pp. 281–288, 2013.

[8] 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).

[9] 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.

Authors

Sudipta Kr Ghosal, Assistant Professor and Teacher in-charge of Computer Science & Engineering department at Greater Kolkata College of Engineering & Management, Kolkata. He received his bachelor of technology in Computer science and Engineering in 2007. He received his master of technology in IT (Courseware Engineering) from Jadavpur University, Kolkata, India in 2010. He is pursuing PhD in Color Image Authentication from University of Kalyani, India under the supervision of Prof. J. K. Mandal. Mr. Ghosal has around four years of experience in teaching and industry. He has fifteen publications in the national and international conferences/journals.

Jyotsna Kumar Mandal, M. Tech.(Computer Science, University of Calcutta), Ph.D.(Engg., Jadavpur University) in the field of Data Compression and Error Correction Techniques, Professor in Computer Science and Engineering, University of Kalyani, India. Life Member of Computer Society of India since 1992 and life member of cryptology Research Society of India. Ex-Dean Faculty of Engineering, Teachnology & Management, working in the field of Network Security, Steganography, Remote Sensing & GIS Application, Image Processing. 26 years of teaching and research experiences. Nine Scholars awarded Ph.D. one submitted and eight are pursuing. Total number of publications is more than two hundred seventy seven in addition of publication of five books from LAP Lambert, Germany.