A FRAGILE WATERMARKING BASED ON LEGENDRE TRANSFORM FOR COLOR IMAGES (FWLTCI)

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 Legendre transformation (LT) based fragile watermarking technique has been proposed for color image authentication. The authentication is done by inserting the watermark into the carrier images in transform domain. An initial pixel adjustment has been applied on each pixel component to keep the pixel value positive and less than or equal to the maximum. The Legendre transformation (LT) is applied on each pair of pixel components of the carrier image in row major order. The first transformed component can fabricate two bits whereas the second component fabricates three bits of authenticating watermark starting from the least significant bit position (LSB-0). A post adjustment is also applied to keep the embedded components closer to the original without affecting the least three significant bits. The inverse Legendre transform (ILT) is applied on each adjusted pair to re-generate the watermarked image. During inverse transform, at if the second pixel component of the adjusted pair become fractional, then the LSB-2 of the first component is set to one; otherwise is set to zero. The reverse procedure is applied at the destination to retrieve back the watermark which in turn is verified for authentication through a message digest. Experimental results conform that the proposed algorithm has improvised the payload and PSNR over Varsaki et. al's Method [6] and LTCIA technique [7].

KEYWORDS

LT, ILT, LTCIA, Payload, PSNR and Watermarked image.

1. INTRODUCTION

Digital information protection through watermarking scheme is an important area of research to resist digital piracy over internet. Watermark information can be incorporated into the carrier/cover media such as image, audio and video etc. for ownership evidence, fingerprinting, authentication and integrity verification.

Over the years, different transformation has been applied on the carrier image to fabricate the watermark in transform domain. Few popular techniques include Quaternion Fourier Transformation (QFT)[1], discrete cosine transformation (DCT)[2], discrete wavelet transformation (DWT)[3], or discrete Fourier transform (DFT)[4] based watermarking. The watermark bits are embedded into the carrier images by altering the transformed components unlike the modification of pixel values in spatial domain. Again, by applying the respective inverse transformation, the watermarked image is produced in spatial domain.

The effectiveness of different watermarking techniques can be measured in terms of payload, peak signal to noise ratio and image fidelity etc. With reference to this Legendre transform [5-6] is an excellent choice for embedding watermark because it offers high payload, less distortion and improved security. A Legendre transform based fragile watermarking technique (LTCIA) is applied by Mandal & Ghosal [7]on each 2 x 2 image block where a 128 bit message digest is used for authentication. The technique proposed by Mandal & Ghosal [7] can be improvised by applying the Legendre transform on a pair of pixel components followed by inserting the watermark bits starting from the LSB-0. As a consequence, the payload can be enhanced significantly and the quality degradation becomes minimal. On embedding authenticating watermark (message/image) bits, inverse Legendre transformation is applied to re-generate the watermarked image.

The Legendre transform (LT) is applied on pixel components $\{c_k\}$ to generate transformed components $\{a_k\}$ as per equation (1).

$$a_n = \sum_{k=0}^{n} \binom{n}{k}\binom{n+k}{k} c_k \tag{1}$$

$$= \sum_{k=0}^{n} \binom{2k}{k}\binom{n+k}{n-k} c_k, \tag{2}$$

where $\binom{n}{k}$ is a binomial coefficient [4].

Similarly, the inverse Legendre transformation (ILT) is used to convert transformed components back into pixel domain as per equation (3).

$$\binom{2n}{n} c_n = \sum_{k=0}^{n} (-1)^{n-k} d_{n,k}\ a_k, \tag{3}$$

where,

$$d_{n,k} = \binom{2n}{n-k} - \binom{2n}{n-k-1} \tag{4}$$

$$= \frac{2k+1}{n+k+1}\binom{2n}{n-k} \tag{5}$$

This paper is emphasized to authenticate a carrier image through a fragile watermarking technique where Legendre transform has been introduced for embedding purpose. 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 dealt with the formulation of the Legendre 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 for a pair of components can be made by transforming each pair of pixel components (c_i, c_{i+1}) into a pair of transformed components (a_i, a_{i+1}) using the Legendre transform (LT) of equation (6).

$$a_i = c_i$$

$$a_{i+1} = c_i + 2 * c_{i+1} \quad (6)$$

where, a_i and a_{i+1} represents the pair of transformed components corresponding to the pixel components c_i and c_{i+1}. Two bits of the authenticating watermark are fabricated in the first component and three bits are embedded into the second component starting from the least significant bit (i.e., LSB-0).

Similarly, by applying the inverse Legendre transform (ILT), each pair of transformed components (a_i, a_{i+1}) is re-transformed back into the spatial domain which consists of pixel components c_i and c_{i+1} as shown in equation (7).

$$c_i = a_i$$
$$c_{i+1} = (a_{i+1} - a_i) \setminus 2 \quad (7)$$

3. PROPOSED TECHNIQUE

In this paper, a fragile watermarking technique based on the Legendre transform (LT) has been proposed for authentication of color images (FWLTCI). A message digests (MD), content of the watermark and the watermark size are embedded using the proposed technique. Initially, the pixel components are adjusted to set a new upper limit (i.e., 248) and a lower limit (i.e., 8) for a pixel component, if necessary. This pre-embedding adjustment ensures that all the pixel components after embedding watermark bits is positive and less than or equal to 255. The Legendre transform (LT) is used to convert each pair of pixel components into transformed components in row major order. The first component of a transformed pair is capable of hiding two bits and the second component is responsible for fabricating three bits of the authenticating watermark starting from the least significant bit position (LSB-0). After embedding the authenticating watermark (message/image), a post-embedding adjustment has been incorporated to keep the embedded components closest to the original without affecting the least three significant bits. The inverse Legendre transform (ILT) is applied on each adjusted pair to re-generate the watermarked image in spatial domain. During inverse transform, if the second pixel component of the adjusted pair become fractional, then the LSB-2 of the first component is set to one; otherwise is set to zero. The above procedure is repeated for each pair of pixel components of the carrier/cover image. The authorized person extracts the watermark from the watermarked image using the 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 recipient end for authentication.

Consider three pairs of pixel components corresponding to red, green and blue channels from a given cover/carrier image. Legendre transform (LT) 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 Legendre transforms (LT) on each pair of pixel components, the obtained pairs of transformed components are as here under:

TR_1={164,290}, TG_1={248,362}, TB_1={71,87}

Now, if we embed the binary stream of *010001110100110* using the proposed technique, the pairs of embedded components becomes:

$ETR_1=\{165,288\}, ETG_1=\{251,365\}, ETB_1=\{68,86\}$

The adjustment method ensured 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. In this example, the components are same as before after adjustment:

$A\ ETR_1=\{165,288\}, AETG_1=\{251,365\}, AETB_1=\{68,86\}$

By applying inverse Legendre transform (ILT) on each pair of transformed components, the obtained pairs of pixel components are as shown below:

$F^{-1}AETR_1=\{165,61.5\}, F^{-1}AETG_1=\{251,57\}, F^{-1}AETB_1=\{68,9\}$

During inverse transform (ILT), the pixel component can have a fractional value which is not possible in reality. Thus, if the second pixel component becomes fractional then the fractional part of the component is discarded and the LSB-2 of the first component is set to one. If there is no fractional value then the LSB-2 of the first component is set to zero.

$CF^{-1}AETR_1=\{165,61\}, CF^{-1}AETG_1=\{251,57\}, CF^{-1}AETB_1=\{64,9\}$

The process of embedding is repeated for each pair of pixel components and continued till the end of authenticating watermark bits. At the receiving end, the recipient takes the watermarked image and based on the value at LSB-2 of the first component for each pair, the specified number of watermark bits are extracted.

This section has been categorized into two parts namely the algorithm for insertion and the algorithm for Extraction.

3.1. Insertion

The pixel components are converted into transform domain in a pair-wise manner based on Legendre transforms (LT). The first transformed component (R/G/B) can fabricate two bits and the second component can hide three bits of the watermark staring from the least significant bit (i.e., LSB-0). An adjustment has been incorporated to adjust the transformed components without hampering the least three significant bits. Inverse Legendre transform (ILT) converts each pair of 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 Legendre transform (LT) 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)* has been obtained from the watermark to authenticate a color image.
2) The size of the authenticating watermark (L) can be expressed by equation (8).

$$W_{size}=[2.5 \times \{3 \times (m \times n)\} - (MD + L)] \quad (8)$$

where, the number of bits embedded per byte is *2.5, 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 do perform the operations shown 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), adjust the upper and lower limit of pixel component (p_c) as per equation (9), to retain the value positive and less than, or equal to *255* before embedding watermark bits. That means,

$$p_c = \begin{cases} 248: p_c \geq 248 \\ = \\ 8: p_c \leq 8 \end{cases} \quad (9)$$

- Apply Legendre transform (LT) on each pair of pixel components to generate transformed pair consisting of transformed components f_i and f_{i+1}.
- Consequently, two bits of the authenticating watermark size, content and the message digests are embedded into the first transformed component and three bits are embedded into the second component of each 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 obtain transformed components closest to the original without hampering the least three significant 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 Legendre transform (ILT) on each pair of adjusted components to re-generate the pixel components pair in spatial domain.
- During inverse transform, if the second pixel component of the adjusted pair become fractional, then the fractional part is discarded for computational flexibility and to keep track of the fractional information, the LSB-2 of the first component is set to one; otherwise is set to zero.

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

3.2. Extraction

The extraction of the hidden watermark can be accomplished by applying the Legendre transform (BT) on each pair of pixel components. In each transformed pair, the LSB-2 of the first transformed component is verified and then the watermark size, contents and the embedded message digests (MD) are extracted. 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 Legendre transform (LT) is used to extract the watermark (along with a message digest) from the watermarked image by converting the image from spatial domain into 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 Legendre transform (LT) on a pair of pixel components corresponding to Red/Green/Blue channel, to generate transformed pair consisting of components f_i and f_{i+1}.
   - For each transformed pair, if the LSB-2 of the first component is one, then the second transformed component is incremented by one.
   - Two bits of the authenticating watermark size, content and the message digests are extracted from the first transformed component and three bits of the same are extracted from the second component (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 Legendre transform (ILT) 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.

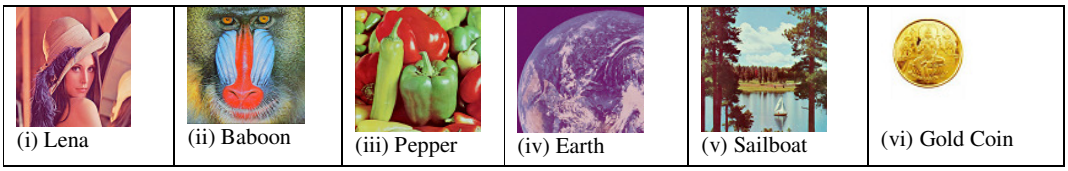

Figure 1. Different cover/carrier images of dimension 512 × 512 along with the 283 × 288 watermark image

It is seen from table 1 that the watermarked image has a peak to signal noise ratio (PSNR) of around 39 dB in average case whereas the bits per byte (bpB) for a given carrier image is 2.5.

Table 1. Results of embedding of 245430 bytes of information into each carrier image of dimension 512 x 512

Carrier Image	**Max. Payload (byte)**	**PSNR**	**IF**	**bpB**
Lena	245760	39.62	0.9996	2.5
Baboon	245760	39.62	0.9996	2.5
Pepper	245760	37.68	0.9990	2.5
Earth	245760	39.64	0.9996	2.5
Sailboat	245760	39.39	0.9996	2.5
AVG	245760	*39.19*	*0.9994*	2.5

Again, it is seen from table 2 that the PSNR and payload has been significantly improved in our proposed technique over the LTCIA technique [7] and Varsaki et al.'s [8] method. The comparison result has been depicted in table 2 for three different carrier images.

Table 2. Comparison of bpB and PSNR for proposed technique over LTCIA technique [7] and Varsaki et. Al's [8] method

Carrier Images	**Varsaki et al.'s Method [8]**		**LTCIA 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	2	38.89	2.5	39.62
Baboon	0.25	30.69	2	38.77	2.5	39.62
Sailboat	0.25	35.28	2	38.73	2.5	39.39
AVG	*0.25*	*35.22*	*2*	*38.79*	*2.5*	*39.54*

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.

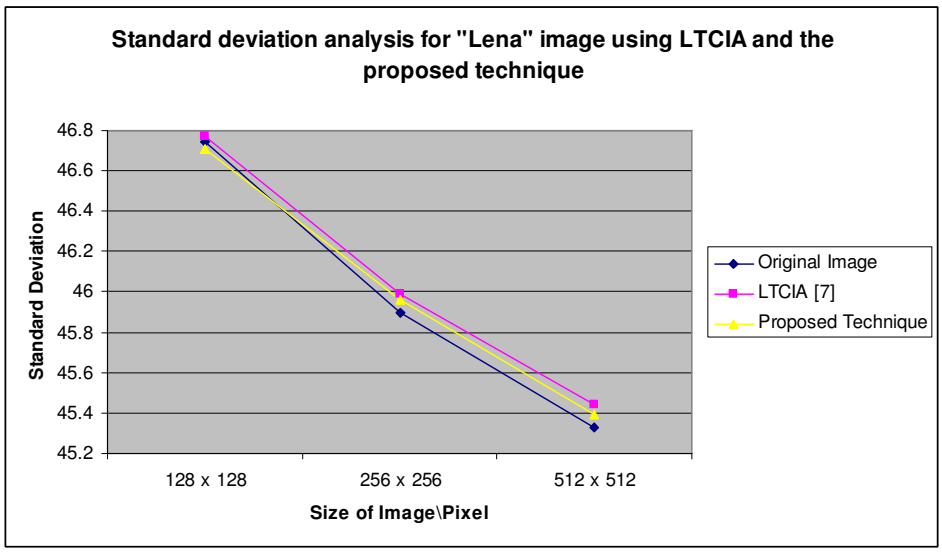

Figure 2: Comparison of standard deviation between source and watermarked 'Lena' image using LTCIA technique [7] and the proposed technique

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 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 IF (Image Fidelity) 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 IF values of the watermarked images under different kind of attacks

Water-marked Images	**PSNR**	**IF**	**PSNR**	**IF**	**PSNR**	**IF**	**PSNR**	**IF**
	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	39.62	0.9996	33.47	0.9968	33.80	0.9980	33.88	0.9983
Pepper	37.68	0.9990	31.39	0.9944	33.68	0.9980	33.10	0.9973
Sailboat	39.39	0.9996	28.47	0.9944	33.73	0.9986	33.50	0.9985

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, 8].

ACKNOWLEDGEMENT

Authors like to express deep sense of gratitude to the PURSE scheme of DST, Government of India under which this research work has been carried out in the department of Computer Science &Engineering, University of Kalyani, India.

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] Jin, Y. and Dickinson, H. "Apéry Sequences and Legendre Transforms." J. Austral. Math. Soc. Ser. A 68, pp. 349-356, 2000.

[6] Schmidt, A. L. "Legendre Transforms and Apéry's Sequences." J. Austral. Math. Soc. Ser. A 58, pp. 358-375, 1995.

[7] Mandal, J. K., Ghosal S. K., "Legendre Transformation based Color Image Authentication(LTCIA)", 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.2013.3630, Volume 3, Number 6, pp. 265–272, 2013.

[8] 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.

[9] 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).

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. and eight are pursuing. Total number of publications is two hundred seventy seven in addition of publication of five books from LAP Lambert, Germany.