LEGENDRE TRANSFORM BASED COLOR IMAGE AUTHENTICATION (LTCIA)

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 fragile watermarking technique using Legendre transform (LT) has been proposed for color image authentication (LTCIA). An initial pixel adjustment is used to ensure that it never exceeds the range of a valid pixel component. The Legendre transform (LT) is applied on each pair of pixel components of the carrier image in row major order. The transformed components of each transformed pair are used to fabricate one/two/three watermark bits starting from the first bit position (LSB-1) based on the perceptibility of human eye on red, green and blue channel. An adjustment method has been incorporated to keep the embedded transformed components closer to the original without hampering the fabricated watermark bits. The inverse Legendre transform (ILT) is applied on each adjusted pair as post embedding operation to re-generate the watermarked image in spatial domain. At the receiving end the whole watermark can be extracted based on the reverse procedure thus authentication is done through message digest. Experimental results conform that the proposed algorithm has enhanced payload and PSNR over Varsaki et. al's Method [1] and SDHTIWCIA [2].

KEYWORDS

LT, ILT, LSB-1, Payload, PSNR, SDHTIWCIA and Message digest.

1. INTRODUCTION

Digital information sharing over the internet has enormous advantages for our modern world. But, due to the digital piracy in public domain, information security and assurance become an important issue. Several fragile/robust watermarking has been proposed based on the transformations like Quaternion Fourier Transformation (QFT), discrete cosine transformation (DCT), discrete wavelet transformation (DWT), or discrete Fourier transform (DFT) etc. to fabricate authenticating watermark bits in transformed components. Varsaki et. al. has proposed a discrete Pascal transform (DPT) [1] based technique which offers an efficient idea of hiding watermark bits into the real frequency components. In [2], a separable discrete Hartley transform based invisible watermarking scheme has been proposed which is exploited for image authenticating purpose by fabricating the authenticating watermark data along with the message

Jan Zizka (Eds) : CCSIT, SIPP, AISC, PDCTA - 2013
pp. 265–272, 2013. © CS & IT-CSCP 2013 DOI : 10.5121/csit.2013.3630

digest (which is generated from authenticating data) into the carrier image with a minimal loss of quality and improved security.

Legendre transform (LT) [3-6] can be applied to convert a color image into transform domain in row major order. Watermark bits are embedded in transformed components. After embedding watermark bits, inverse Legendre transformation (ILT) is applied to get back the watermarked image into spatial domain.

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,

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

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

The proposed technique exploits image authentication process by embedding the watermark data in both negative and positive transformed components along with the message digest MD (which is generated from watermark data) into the carrier image with a minimum change in visual properties with improved security.

Section 2 deals with the proposed technique. The results, comparison and analysis is given in section 3. Conclusion is drawn in section 4. References are given at end.

2. THE TECHNIQUE

In this paper, a novel watermarking technique based on the Legendre transform (LT) has been proposed for color image authentication (LTCIA). A message digests (MD), content of the watermark and the watermark size are embedded using the LTCIA technique. Each pair of pixel components of the carrier image is pre-processed for an initial adjustment, if necessary. This pre-

embedding pixel adjustment strategy ensures that the pixel values on embedding the watermark is not get out of range ($0 \leq p \leq 255$). The LT is applied on each pair of pixel components for converting the pixel components into transformed components. In the proposed LTCIA technique, due to the high sensitivity of human eye on green channel, only one bit of the watermark is embedded into each transformed component. Unlikely, due to the low perceptibility of human eye on blue channel, three bits from the watermark are fabricated into the components. Two bits are embedded in each red transformed component because the perceptibility of human eye in red channel as compared to the green and blue channel is neither high nor low. The bit embedding operation is started from the pre-LSB position of each transformed component (LSB-1) toward the higher order bits position. After embedding the authenticating watermark (message/image), a transformed components adjustment method has been incorporated to keep the embedded transformed component closer to the original without hampering the fabricated watermark bits. The inverse Legendre transform (ILT) is applied on each adjusted components pair as post embedding operation to re-generate the watermarked image in spatial domain. At the receiving end, the authorized person can extract the watermark from the watermarked image using reverse process and obtain a new message digest (MD') from the extracted watermark bits. The same is compared with extracted message digests (MD) for authentication.

2.1 Insertion

Initially, each pixel component pair are pre-adjusted, if necessary and then converted into transformed component pair corresponding to red, green and blue channels using Legendre transform (LT). Based on the varying sensitivity of human eye on (R/G/B) channel, watermark bits are embedded with varying proportions into the transformed components starting from the pre-LSB. A transformed components adjustment has been incorporated to adjust the transformed components without hampering the embedded bits. Inverse Legendre transform (ILT) converts each pair of adjusted components into pixel components pair to form the 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′) in spatial domain.

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 to 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).

$$W_{size}=[2 * \{3 * (m * n)\} - (MD + L)] \quad (8)$$

where, the average bits per byte is *2, MD* and *L* are the message digest and dimension of the authenticating watermark for the m x n, 24 bit host 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 (c), reset the upper and lower limit of pixel component (p_c) to retain the value positive and less than, or equal to *255* in spatial domain during embedding. The initial pixel adjustment has been made on the basis of the concept that human eye is less sensitive to blue channel and most sensitive to green channel. That means,

$$pc = \begin{cases} 251; \text{ if } (pc \geq 251); \\ 4; \text{ if } (pc \leq 4); \text{ If } (c=G) \\ 248; \text{ if } (pc \geq 240); \\ 8; \text{ if } (pc \leq 8); \text{ If } (c=B) \end{cases}$$

$$= \begin{cases} 240; \text{ if } (pc \geq 240); \\ 8; \text{ if } (pc \leq 8); \text{ If } (c=B) \end{cases} \quad (9)$$

- For each channel, apply Legendre transform (LT) on a pair of pixel components to generate a transformed components pair consisting of components f_i and f_{i+1}.
- Consequently, N bits of the authenticating watermark size, content and the message digests are embedded in each transformed component of every transformed pair starting from the first bit position (i.e., LSB-1) based on the chosen channel (R/G/B). The mathematical expression can be written as per equation (10).

$$N = \begin{cases} 1; \text{ if } (c=G) \\ 2; \text{ if } (c=R) \\ 3; \text{ if } (c=B) \end{cases} \quad (10)$$

[Embed authenticating watermark bits as per the above rules.]

- A transformed components adjustment has been incorporated to get transformed components values closest to the original without hampering the embedded bits. The transformed adjustment has been made by choosing the embedded transformed component value closest to the original one with the help of left most *(T-N-1)* bits alteration.
- Apply inverse Legendre transform (ILT) on each pair of adjusted components to re-produce 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. The successive pair embedding operation produces the watermarked image (I′).

5) Stop.

3.2 Extraction

The authenticated watermarked image is received in spatial domain. The Legendre transform (LT) converts each pair of pixel components into transformed components. The watermark size, contents and the embedded message digests (MD) are extracted from the specified positions of each transformed component. The watermark data and 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) in spatial domain 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 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) 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:

   - For each individual channel (*c*), apply Legendre transform (LT) on a pair of pixel components to generate a transformed components pair consisting of transformed components f_i and f_{i+1}.
   - Based on the chosen channel (R/G/B), N 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-1. The mathematical expression is written in equation (11).

$$N = \begin{cases} 1; \text{ if } (c=G) \\ 2; \text{ if } (c=R) \\ 3; \text{ if } (c=B) \end{cases} \quad (11)$$

   [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 into pixel components pair in spatial domain after extracting authenticating watermark bits.

3) Repeat step 1 and 2 to complete decoding as per the size of the authenticating watermark.

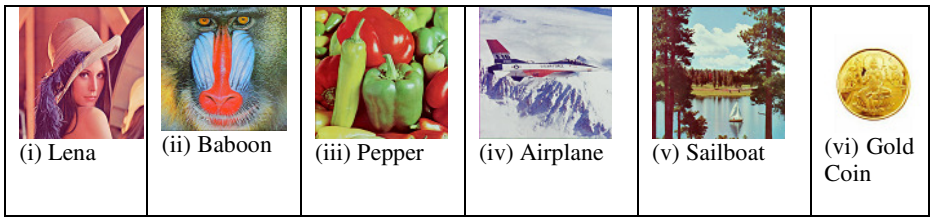
4) Obtain 128 bits message digest MD′ from the extracted authenticating message/image. Compare MD′ with extracted MD. If both are same then the image is authorized, else unauthorized.

5) Stop.

4. RESULTS, COMPARISON AND ANALYSIS

This section represents the results, comparison and analysis of the proposed LTCIA technique. Benchmark (PPM) images [7] of dimension 512 × 512 are taken to incorporate the gold coin (i.e. the authenticating watermark image). The experiment deals with five different color images (i-v) labeled as: (i) Lena, (ii) Baboon, (iii) Pepper, (iv) Airplane and (v) Sailboat. On embedding the

authenticating watermark image that is the Gold-Coin image of (vi), the newly generated watermarked image produces a good visual clarity.



(i) Lena (ii) Baboon (iii) Pepper (iv) Airplane (v) Sailboat (vi) Gold Coin

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 with a peak to signal noise ratio (PSNR) values of more than 38 dB. In the proposed technique, the average bits per byte (bpB) for a given carrier image is 2. Fig-2 shows the different states of three different images viz. Lena, baboon and Sailboat.

Table 1. Results of embedding of 196608 bytes of information in each Image of dimension 512 x 512

Carrier Image	**Payload (byte)**	**PSNR**	**IF**	**BPB**
Lena	196608	38.89	0.9995	2
Baboon	196608	38.77	0.9995	2
Pepper	196608	36.68	0.9982	2
Airplane	196608	38.91	0.9998	2
Sailboat	196608	38.73	0.9995	2
AVG	196608	*38.39*	*0.9993*	2

A comparative study has also been made among Varsaki et. al's method [1], SDHTIWCIA [2] and the proposed LTCIA technique in terms of payload and the PSNR. In contrast to Varsaki et. al's method, the payload is more than 172032 bytes and PSNR enhancement is around 3 dB while in comparison with the SDHTIWCIA technique, the payload enhancement is 49164 bytes along with a PSNR improvement of 0.57 dB.

Table 2. Enhancement of payload and PSNR in LTCIA over Varsaki et. al's method [1] and SDHTIWCIA [2]

Carrier Image	**Varsaki et. al's Method [1]**		**SDHTIWCIA [2]**		**LTCIA**	
	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	2	38.89
Baboon	0.25	30.69	1.5	38.57	2	38.77
Sailboat	0.25	35.28	1.5	38.23	2	38.73
AVG	***0.25***	***35.22***	***1.5***	***38.25***	***2***	***38.79***

The standard deviation analysis of 'Lena' image is shown in figure 3 which ensure that the changes made between the original and watermarked image in the propsed LTCIA technique is really very less as compared to the SDHTIWCIA [2] technique.

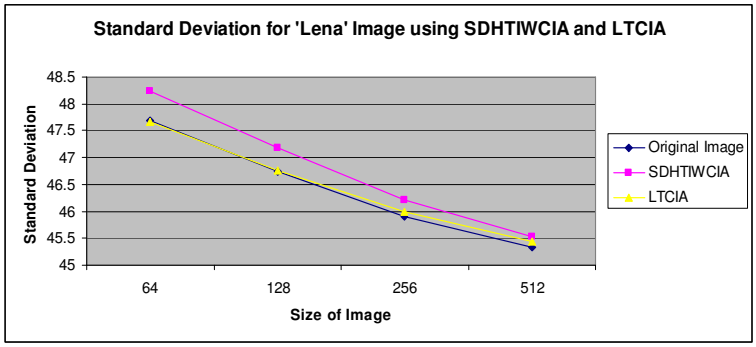


Figure 3: Comparisons of standard deviation between source and watermarked 'Lena' image using LTCIA and SDHTIWCIA

In the proposed LTCIA technique, 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. Moreover, if the authentication process fails, then the recipient resends a negative acknowledgement to the sender.

It is seen from table 3 that the PSNR (Peak Signal to Noise Ratio) values obtained from the watermarked images before and after different kinds of attacks has been altered.

Table 3. Comparison of PSNR values under different kinds of attacks on watermarked images

Images	**Before Attack (PSNR)**	**After 2 x 2 Blur attack (PSNR)**	**After Speckle Noise attack (PSNR)**	**After Poisson Noise attack (PSNR)**	**After Gaussian Noise attack (PSNR)**
Lena	38.89	29.35	33.60	26.85	20.14
Baboon	38.77	22.87	33.70	26.91	20.07
Sailboat	38.73	26.44	33.56	26.94	20.15

5. CONCLUSION

The LTCIA can be used for image authentication in transform domain to verify whether an image is tampered or not. Authentication is done by embedding watermark data in a carrier image and high robustness is achieved by hiding data in both positive and negative transformed components.

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] 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.

[2] 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), Vol. 2, ISBN-978-3-642-31551-0, pp. 767-776, July 13-15, 2012.

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

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

[5] Strehl, V. "Binomial Identities--Combinatorial and Algorithmic Aspects. Trends in Discrete Mathematics." Disc. Math. 136, pp. 309-346, 1994.

[6] Zudilin, W. "On a Combinatorial Problem of Asmus Schmidt." Elec. J. Combin. 11, R22, 1-8, 2004, http://www.combinatorics.org/Volume_11/Abstracts/v11i1r22.html.

[7] 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).