AMSE JOURNALS –2014-Series: Advances B; Vol. 57; N° 1; pp 68-87
Submitted Feb. 2014; Revised May 17, 2014; Accepted June 1, 2014

Color Image Authentication based on Two-Dimensional Separable Discrete Hartley Transform (CIA2D-SDHT)

*S. K. Ghosal, **J. K. Mandal

*Department of Computer Science & Engineering
Greater Kolkata College of Engineering & Management
Baruipur, West Bengal, 743387, India
** Department of Computer Science & Engineering, University of Kalyani
Kalyani, West Bengal, 741235, India
(sudipta.ghosal@gmail.com; jkm.cse@gmail.com)

Abstract

In this paper, a novel watermarking technique based on two-dimensional separable discrete Hartley transform (2D-SDHT) has been proposed for color image authentication (CIA2D-SDHT). Each 2 x 2 sub-image block of the carrier image is pre-adjusted, if necessary and then transformed using 2D-SDHT in row major order. Two bits of secret data are fabricated at second and third bit positions of each transformed component. An inverse two dimensional separable discrete Hartley transform (2D-ISDHT) has been applied on embedded block followed by a post-adjustment operation on the frequency components to re-generate watermarked image with minimum degradation in spatial domain. The recipient at the destination end perform reverse operation to extract the secret bits stream. A message digest is obtained from the extracted watermark which in turn is compared with the extracted message digest for authentication. Experimental results conforms that the proposed technique offer better payload and PSNR over existing techniques [17-22].

Keywords: 2D-SDHT, 2D-ISDHT, message digest, payload and PSNR.

1. Introduction

Watermarking is an information hiding technique which embeds secret information in a digital cover medium, such as image, audio or video. Watermarking is applied on three different domains, i.e., the spatial domain, the compression domain, and the frequency domain. In the spatial domain, the cover image is altered directly and undetectably to conceal the secret message. Lee and Chen [1] proposed an information embedding algorithm in spatial domain where the least significant bit (LSB) of each pixel in the cover image was replaced by secret data.

Chang et al. [2] devised optimal LSB substitution for embedding secret data by using a dynamic programming strategy. Applying both run-length encoding and modular computation, Chang et al. [3] designed two efficient information embedding methods for bitmap files and grayscale files. Gutub [4] suggested an efficient way of embedding secret data into two least significant bits of a pixel in spatial domain. All of the techniques discussed are reversible information embedding techniques in the spatial domain. In the compression domain, the secret data are embedded through alteration of the compression code. In such techniques, the size of the data can be reduced significantly. Many researchers have taken interest in hiding information in the compression domain. Among the compression based schemes JPEG, JPEG2000, VQ, and block truncation coding (BTC), VQ is a simple and efficient method widely used for embedding. Chang et al. [5] proposed a reversible embedding technique based on SMVQ. In the same year Yang et. al [6] proposed an MFCVQ based, reversible embedding scheme using four adjacent blocks to encode the current block. However, the visual quality and payload of Yang et al.'s scheme were not good enough. In 2009, Chang et al. [7] used the concept of joint neighboring coding (JNC) in the VQ index table for embedding secrets with reversibility. Here, a novel information embedding technique based on the VQ codebook has been explored. The method used a codebook that has been resorted by PCA (principle component analysis) and exploited the distance of two code-words, which are similar to one image block, to embed the secret data. Based on the secret data to be embedded and the difference between those two code-words, the original image block is transformed into a difference number table which is compressed through entropy coding before sending to the receiver. At the receiving end, on decoding the compressed code, the secret data can be extracted, and the image can be recovered as a VQ compressed image.

In frequency domain, the cover image is preprocessed by Quaternion Fourier Transformation (QFT) [8], discrete cosine transformation (DCT) [9], discrete Wavelet transform (DWT) [10] , discrete Fourier transform (DFT) [11] or using other similar transformation to obtain frequency coefficients. Frequency coefficients are modified slightly to embed the secret data. Watermarked images are obtained through reverse transformation of the modified frequency coefficients. Frequency domain methods are widely used than spatial domain techniques. To avoid severe distortion of the original image the midrange frequencies are best suitable for embedding to obtain a balance between imperceptibility and robustness. In 2001, Fridrich et al. [12] proposed an invertible information embedding technique to modify the quantization table using a second-order function. In 2008, Maity, proposed a digital watermarking technique that selects region based on discrete Hadamard transform [13]. Two valued kernels of Hadamard transformation

cause smaller image information change during embedding compared to other transform domains such as DCT(discrete cosine transform), DFT(discrete Fourier transform), Fourier Mellin and wavelet-based embedding. Moreover, the usage of Hadamard transform as signal decomposition tool offers advantages in terms of simpler implementation, low computation cost and high resiliency considering both JPEG and JPEG 2000 framework. Varsaki et al. proposed a novel watermarking technique [14] based on Pascal transform where the embedding procedure is based on dividing each color image component into even-sized blocks. Information embedding is determined by monitoring the lower-right corner of the DPT coefficient matrix. This particular coefficient suffers the highest change with minimum pixel modifications. The embedding affects the sign of coefficients. If the sign is not desired one, i.e. negative for a message bit value of 0 and positive for a message bit value of 1, it is changed by repeatedly adding to the block or subtracting from the block. This process is based on the DPT properties and on the sensitivity of the lower-right coefficient. The embedding algorithm takes care of the underflows or overflows that may occur during the consecutive additions or subtractions. In 2011, Manoochehri M. et al. proposed a novel watermarking technique [20] based on the sub-bands of discrete Wavelet Transform and Fourier-Mellin Transform. The robustness of watermarked image against most of attacks like rotation has increased tremendously just because of incorporation of FMT specifications with DWT. R. O., El.Sofy and H.H.Zayed [21] proposed a high capacity data hiding technique where up to 48% of the cover image size has been embedded. In this paper, an adaptive hiding capacity function is used to hide secret data in the integer wavelet coefficients of the cover image with the optimum pixel adjustment (OPA) algorithm. Elham Ghasemi et al. [22] proposed a novel steganography technique based on Integer Wavelet Transform and Genetic Algorithm. Experimental results show that the technique offers better peak signal to noise ratio and capacity i.e. 35.17 dB and 50% respectively.

In the year 2012, Mandal and Ghosal proposed a fragile watermarking technique [17] where the separable discrete Hartley transform [15] has been used to convert the image from spatial domain to frequency domain. The watermark text/image is embedded into the frequency components of each transformed image block. Inverse separable discrete Hartley transformation is applied to produce the watermarked image in spatial domain as post-embedding operation. The pixel values in spatial domain act as wrapper to the hidden authenticating bits but, if we apply SDHT again, the hidden authenticating bits will be retrieved from the frequency component values by the application of the algorithm. Unlike the Discrete Fourier Transform (DFT), the SDHT produces real output for a real input which can be designated as its own inverse. Moreover, the SDHT can be defined as the difference of even and odd parts of the DFT.

The two dimensional separable discrete Hartley transform (2D-SDHT) over M x N carrier image is given in equation (1).

$$P_S(u,v) = \sum_{x=0}^{N-1}\sum_{y=0}^{M-1} p(x,y)cas(2\pi ux/N)cas(2\pi vy/M) \quad (1)$$

where, u varies from 0 to M-1 and v varies from 0 to N-1.

The variable u and v are the frequency variables corresponding to the spatial domain variables x and y where p(x,y) represents the intensity values of the pixel components in spatial domain. The sequence *cas* is defined in equation (2) and (3).

$$cas(2\pi ux/N) = cos(2\pi ux/N) + sin(2\pi ux/N) \quad (2)$$

$$cas(2\pi vy/M) = cos(2\pi vy/M) + sin(2\pi vy/M) \quad (3)$$

Similarly, the inverse transformation is used to convert the M x N block of frequency components into the spatial domain using the equation (4).

$$p(x,y) = \frac{1}{NM}\sum_{x=0}^{N-1}\sum_{v=0}^{M-1} P_S(u,v)cas(2\pi ux/N)cas(2\pi vy/M) \quad (4)$$

where, u varies from 0 to M-1 and v from 0 to N-1.

The proposed CIA2D-SDHT scheme exploits image authentication by fabricating the watermark data along with the message digest MD (which is generated from the watermark) into the carrier image with a minimal loss of quality and improved security. Problem motivation and formulation of transformation technique is given in section 2. Section 3 of the paper dealt with the proposed technique. Results, comparison and analysis are given in section 4.

Conclusions are drawn in section 5. References are given at end.

2. Separable Discrete Hartley Transform

The formulations of image sub block of size 2 x 2 can be expressed in 2D-SDHT as follows:

$$P_S(u,v) = \sum_{i=0}^{1}\sum_{j=0}^{1}(-1)^{ui}(-1)^{vj}p(i,j) = f_{u,v}(say) \quad (5)$$

where, i and j varies from 0 to 1 and the variable u and v are the frequency variables corresponding to the frequency components $f_{u,v}$. In each frequency component, two bits are fabricated at second and third bit position of the LSB part.

Similarly, by applying the inverse 2D-SDHT, the 2 x 2 masks in spatial domain can be obtained using equation 6.

$$p(i,j) = \frac{1}{4}\sum_{u=0}^{1}\sum_{v=0}^{1}(-1)^{ui}(-1)^{vj}P_S(u,v) = p_{i,j}(say) \quad (6)$$

where, u and v varies from 0 to 1 and the variable i and j are the spatial domain variables corresponding to the pixel intensity values $p_{i,j}$ in spatial domain.

Initial adjustment on the pixel values ensured non-generation of fractional values, overflow and underflow in terms of range of pixel values in two-dimensional inverse SDHT.

3. The Technique

In this paper, two dimensional separable discrete Hartley transform (2D-SDHT) has been used to generate a novel fragile watermarking technique in frequency domain for the purpose of color image authentication (CIA2D-SDHT). The message digests (MD) obtained from the watermark, the size of the watermark and the content of the watermark are embedded using the proposed CIA2D-SDHT. Two dimensional SDHT converts each 2 x 2 sub-image block of the carrier image into 2 x 2 transformed blocks of coefficients in row major order. Bits are embedded in each transformed coefficients of 2 x 2 sub-image block. In each component, two bits of the secret bits are embedded at the second and third bit positions of the co-efficient. An initial adjustment on the pixel components are applied to keep the pixel components within the valid range i.e., $0 \leq p \leq 255$. In the proposed technique, the pixel components are non-fractional as two least significant bits are not altered. A frequency adjustment has been incorporated as post-embedding operation on each embedded component to re-generate component value closest to the original without hampering the fabricated bits. An inverse two dimensional separable discrete Hartley transform (2D-ISDHT) is applied to re-generate the watermarked image in spatial domain. The reverse operation is performed to extract the message digests, size as well as the content of the watermark from the watermarked image. A new message digests MD' is calculated from the extracted watermark bits and the same is compared with the extracted message digests MD for authentication.

Consider a subset of "Baboon" image as the cover/carrier image. 2D-SDHT is applied on each sub-matrices viz. red, green and blue channels of a 2 x 2 sub-image block to convert it from spatial domain into the frequency domain. Let four pixels of a 2 x 2 sub-image block P1=[164,150,71], P2=[63,57,31], P3=[120,125,62], P4=[135,97,33]

From these four pixels, three matrices for red, green and blue channels are formed as R1=[164,63,120,135], G1=[150,57,125,97], B1=[71,31,62,33]

Frequency components are obtained through 2D-SDHT as, F(R1)=[482,86,-28,116], F(G1)=[429,121,-15,65], F(B1)=[197,69,7,11]

Let, the string "skg" is to be embedded which is represented using the binary stream as 01110011 01101011 01100111 corresponding to the ASCII values of each character. Subsequently, the authenticating bits are embedded at the second and third bit positions from LSB of each frequency component. Thus modified frequency components obtained are E(F(R1))=[486,94,-16,124], E(F(G1))=[421, 121, -11, 77], E(F(B1))=[197,73,7,15]

A post-embedding frequency adjustment ensured the enhancement of quality without tampering fabricated bits which generates the embedded coefficients A(E(F(R1))) = [486, 94, -32, 124], A(E(F(G1)))=[421, 121, -11, 61], A(E(F(B1)))= [197,73,7,15]

Inverse 2D-SDHT is applied to re-generate pixel components in spatial domain as $F^{-1}(A(E(F(R1))))$=[168,59,122,137],$F^{-1}(A(E(F(G1))))$ =[148,57,123,93], $F^{-1}(A(E(F(B1))))$ = [73,27,58,39]

It is observed that the modified pixel components are non-fractional as the two bits from the LSB position of each frequency component is kept unaltered.

Section 3.1 described the insertion technique in details that of extraction is given in section 3.2. Detailed algorithms for insertion as well as extraction are described in these sections.

3.1 Insertion

An initial adjustment on each pixel component is applied to restrict its value within range even after insertion of the watermark. Size of watermark, content and the message digest are embedded into each transformed co-efficient of 2 x 2 block obtained through two dimensional separable discrete Hartley transform. Two bits of authenticating watermark are embedded at the second and third bit position from the least significant part in each frequency co-efficient. The least two bits in each frequency components are kept unaltered to prevent generation of fractional values during inverse transform. An adjustment has also been incorporated to reduce the quality degradation.

Algorithm 1: Insertion (*Cover*; *Watermark*)

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 two dimensional separable discrete Hartley transform (2D-SDHT) 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:

Step 1: Generate r bits message digest (MD) from the authenticating watermark.

Step 2: Generate the size of the authenticating message/image ((L=W+H) bits, where W bits for width and H bits for height). The authenticating message/image bits size is

$$WKsize = 2 \text{ x } (3 \text{ x } (M \text{ x } N)) - (MD + L) \tag{7}$$

where, MD and L are the message digest and dimension of the authenticating watermark for the carrier image of dimension M x N. In proposed technique, the MD and L consist of 128 and 32 bits.

Step 3: The cover image is partitioned into 2 x 2 non-overlapping blocks in row major order consists of four pixels, $p_{i,\ j}$, $p_{i,\ j+1}$, $p_{i+1,\ j}$ and $p_{i+1,\ j+1}$, where the values of i and j lies in the range $0 \leq i \leq 1$ and $0 \leq j \leq 1$. If the chosen carrier/cover image is a color image, then for each 2 x 2 non-overlapping block (b^c), there exists three different 2 x 2 sub-matrices of red (R), green (G) and blue (B) channels which is expressed in equation (8).

$$b^c = \begin{cases} (p^R_{i,j}, p^R_{i,j+1}, p^R_{i+1,j}, p^R_{i+1,j+1}) : c = R \\ (p^G_{i,j}, p^G_{i,j+1}, p^G_{i+1,j}, p^G_{i+1,j+1}) : c = G \\ (p^B_{i,j}, p^B_{i,j+1}, p^B_{i+1,j}, p^B_{i+1,j+1}) : c = B \end{cases} \tag{8}$$

Step 4: Call procedure 3.1.3 for initial adjustment of pixel components.

Step 5: Call procedure 3.1.1 to apply the separable discrete Hartley transform (2D-SDHT) on each adjusted 2 x 2 pixel blocks of the cover image.

Step 6: Two bits of the authenticating message/image are fabricated at the second and third bit positions in each frequency component (f^c). Least two bits (0^{th} and 1^{st}) of the embedded components are kept unaltered to avoid fractional pixel component during inverse transform phase at step 8. It is assumed that the frequency component values after embedding watermark bits are $e_{i,\ j}$, $e_{i,\ j+1}$, $e_{i+1,\ j}$ and $e_{i+1,\ j+1}$ whereas the 2 x 2 embedded blocks b''^c is given in equation (9).

$$b''^c = \begin{cases} (e^R_{i,j}, e^R_{i,j+1}, e^R_{i+1,j}, e^R_{i+1,j+1}) : c = R \\ (e^G_{i,j}, e^G_{i,j+1}, e^G_{i+1,j}, e^G_{i+1,j+1}) : c = G \\ (e^B_{i,j}, e^B_{i,j+1}, e^B_{i+1,j}, e^B_{i+1,j+1}) : c = B \end{cases} \tag{9}$$

The embedded components e^c are obtained as given in equation (10).

$$e^c = \begin{cases} (f^c \& N | WK) \text{ where,} \\ N = X^9 + X^8 + X^7 + X^6 + X^5 + X^4 + X + 1 \\ WK = 0 | X^2 | X^3 | (X^3 + X^2) \end{cases} \quad (10)$$

Here, N and WK are two decimal numbers. The corresponding polynomial representation is given in equation (10). The bitwise-AND operation between f^c and N is performed to reset the second and third bits of f^c to '0'. The bitwise-OR operation is used to fabricate the watermark bits (WK) into the second and third bit positions of the same.

Step 7: Call procedure 3.1.4 to adjust the embedded component closest to the original.

Step 8: Call procedure 3.1.2 to apply the inverse separable discrete Hartley transform (2D-ISDHT) on each adjusted 2 x 2 transformed block to re-generate the watermarked image.

Step 9: Repeat step 3 to step 8 for the whole authenticating watermark size, content and for message digest MD.

Step 10: Stop.

Procedure 3.1.1: 2D-SDHT (*Pixel Block*)

Input: 2 x 2 sub-image block consisting of pixel components ($p_{i,j}$, $p_{i,j+1}$, $p_{i+1,j}$ and $p_{i+1,j+1}$).

Output: 2 x 2 transformed block consisting of frequency components ($f_{i,j}$, $f_{i,j+1}$, $f_{i+1,j}$ and $f_{i+1,j+1}$).

Method: Two-dimensional separable discrete Hartley transform (2D-SDHT) has been applied to convert each 2 x 2 pixel blocks consisting of $p_{i,j}$, $p_{i,j+1}$, $p_{i+1,j}$ and $p_{i+1,j+1}$ into transform domain using equation (5). Each 2 x 2 transformed block b'^c is consisting of frequency components $f_{i,j}$, $f_{i,j+1}$, $f_{i+1,j}$ and $f_{i+1,j+1}$, where the values of i and j lies in the range $0 \le i \le 1$ and $0 \le j \le 1$. The obtained transformed blocks b'^c is given in equation (11).

$$b'^c = \begin{cases} (f^R_{i,j}, f^R_{i,j+1}, f^R_{i+1,j}, f^R_{i+1,j+1}) : c = R \\ (f^G_{i,j}, f^G_{i,j+1}, f^G_{i+1,j}, f^G_{i+1,j+1}) : c = G \\ (f^B_{i,j}, f^B_{i,j+1}, f^B_{i+1,j}, f^B_{i+1,j+1}) : c = B \end{cases} \quad (11)$$

Procedure 3.1.2: 2D-ISDHT (*Frequency Component Block*)

Input: 2 x 2 transformed block consisting of frequency components ($f_{i,j}, f_{i,j+1}, f_{i+1,j}$ and $f_{i+1,j+1}$).

Output: 2 x 2 sub-image block consisting of pixel components ($p_{i,j}$, $p_{i,j+1}$, $p_{i+1,j}$ and $p_{i+1,j+1}$).

Method: The two-dimensional inverse separable discrete Hartley transform (2D-ISDHT) has been applied on each transformed block to convert it into the spatial domain using equation (6). Thus, each 2 x 2 block of pixel components b^c is consisting of pixel components ($p_{i,j}$, $p_{i,j+1}$, $p_{i+1,j}$ and $p_{i+1,j+1}$), where the values of i and j lies in the range $0 \leq i \leq 1$ and $0 \leq j \leq 1$.The obtained block of pixel components b^c is given in equation (12).

$$b^c = \begin{cases} (p^R_{i,j}, p^R_{i,j+1}, p^R_{i+1,j}, p^R_{i+1,j+1}) : c = R \\ (p^G_{i,j}, p^G_{i,j+1}, p^G_{i+1,j}, p^G_{i+1,j+1}) : c = G \\ (p^B_{i,j}, p^B_{i,j+1}, p^B_{i+1,j}, p^B_{i+1,j+1}) : c = B \end{cases} \quad (12)$$

where, $f_{i,j}, f_{i,j+1}, f_{i+1,j}$ and $f_{i+1,j+1}$ are the frequency components of each 2 x 2 transformed block (b^c).

Procedure 3.1.3: Initial Pixel Adjustment (*Pixel Value*)

Input: Original pixel component (p^c).

Output: Adjusted pixel component (p'^c).

Method: For each channel, set the upper limit value of a pixel component (p^c) to 243 and lower limit value to 12. It retains the values of each pixel component positive and less than, or equal to 255 during the inverse transformation at step 8. The adjustment has been done in such a way that all the pixel components lies in a valid range even after embedding watermark bits in transform domain. The adjustment is mathematically expressed in equation (13).

$$p'^c = \begin{cases} 243 : p^c \geq 243 \\ 12 : p^c \leq 12 \end{cases} \quad (13)$$

Procedure 3.1.4: Component Adjustment (*Embedded Component*; *Original Component*)

Input: Embedded component (e^c) and frequency component (f^c).

Output: Adjusted frequency component (e''^c).

Method: The adjusted component (e''^c) can be selected from the set of 2^k possibilities without hampering the least significant four bits. The adjusted component (e''^c) can be derived as follows:

1: begin

2: do

3: $s \leftarrow (e^c \ mod \ 2^4)$ and $i \leftarrow 0$.

4: while ($i < 4$)

5: $e'^c \leftarrow 2^4 \text{ x } i + s$

6: $e''^c \leftarrow c\mathit{losest}\ (e'^c, f^c)$

7: end while

8: Return

3.2. Extraction

The embedded image is taken as the input at the destination. The watermark size, content and message digest are extracted from it. A new message digest MD′ is obtained from the extracted watermark which in turn is compared with the extracted message digest MD for authentication. The extraction procedure is described in algorithm 2.

Algorithm 2: Extraction (*Watermarked Image*)

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

Output: The authenticating watermark image (W) in spatial domain and the message digest.

Methods: The two dimensional separable discrete Hartley transform (2D-SDHT) 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:

Step 1: The watermarked image is partitioned into 2 x 2 non-overlapping blocks in row major order. Each 2 x 2 block consists of four pixels, $p_{i,j}$, $p_{i,j+1}$, $p_{i+1,j}$ and $p_{i+1,j+1}$, where the values of i and j lies in the range $0 \leq i \leq 1$ and $0 \leq j \leq 1$. If the chosen watermarked image is a color image, then for each 2 x 2 non-overlapping block (b^c), there exists three different 2 x 2 sub-matrices of red (R), green (G) and blue (B) channels which is expressed in equation (14).

$$b^c = \begin{cases} (p^R_{i,j}, p^R_{i,j+1}, p^R_{i+1,j}, p^R_{i+1,j+1}) : c = R \\ (p^G_{i,j}, p^G_{i,j+1}, p^G_{i+1,j}, p^G_{i+1,j+1}) : c = G \\ (p^B_{i,j}, p^B_{i,j+1}, p^B_{i+1,j}, p^B_{i+1,j+1}) : c = B \end{cases} \quad (14)$$

Step 2: Call procedure 3.1.1 to apply the separable discrete Hartley transform (2D-SDHT) on each 2 x 2 sub-blocks of pixel components of the watermarked image.

Step 3: From each frequency component (f^c) of all three 2 x 2 sub-blocks, two bits of authenticating watermark are extracted from the second and third bit positions of the least significant part i.e., 8 bits are extracted from each 2 x 2 sub-block of a specific channel.

Step 4: For each 8 (eight) bits extraction, construct one alphabet/one primary (R/G/B) color component.

Step 5: Call procedure 3.1.2 to apply the inverse separable discrete Hartley transform (2D-ISDHT) on each 2 x 2 extracted frequency component block.

Step 6: Repeat step 1 to step 5 to complete decoding.

Step 7: Obtain 128 bits message digest MD' from the extracted authenticating message/image.

Step 8: Compare MD' with the extracted MD. If both are matches then the image is authorized, else unauthorized.

Step 9: Stop.

4. Results, Comparison and Analysis

This section represents the results, discussion and a comparative study of the CIA2D-SDHT technique over DCT, QFT and Spatio-Chromatic DFT based embedding [8–11] in terms of payload and visual interpretation with reference to peak signal to noise ratio (PSNR) analysis, bits per byte (bpB) and histogram analysis. Benchmark (PPM) images [16] are taken to formulate results as shown in fig- 1. All cover images are 512 x 512 in dimension whereas the gold coin (i.e. the secret data) of 254 x 256 is embedded into the cover images. The experiment has been carried out with eight different color images (i-viii), where each pixel is represented by three intensity values RGB (Red, Green and Blue). Images are labeled as: (i) Lena, (ii) Baboon, (iii) Airplane, (iv) Earth, (v) Sailboat, (vi) Foster City, (vii) San Diego, (viii) Oakland. A high fidelity watermarked image is obtained by embedding the “Gold Coin” image of dimension 254 x 256 into the carrier images.

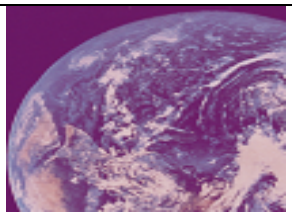
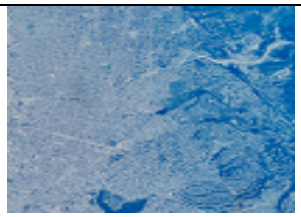
 (i) Lena	 (ii) Baboon	 (iii) Airplane
 (iv) Earth	 (v) Sailboat	 (vi) Foster City
 (vii) San Diego	 (viii) Oakland	 (ix) Gold Coin

Fig. 1 Cover images (i-viii) of dimension 512 x 512 along with the watermark (ix) of dimension 254 x 256

Fig. 1 shows the cover images (i to viii) and the authenticating image (ix). Fig- 2 shows visual state of the images before and after embedding the authenticating “Gold Coin” into the three different carrier images viz. ’Lena’, ’Baboon’ and ’Airplane’.

 Original Lena	 Embedded Lena	 Extracted Lena	 Authenticating Gold Coin
 Original Baboon	 Embedded Baboon	 Extracted Baboon	 Authenticating Gold Coin

Original Airplane

Embedded Airplane

Extracted Airplane

Authenticating Gold Coin

Fig. 2 Cover, embedded and the authenticating images using proposed CIA2D-SDHT technique

It is seen from table 1 that the average payload for carrier images of dimension 512 x 512 is 196608 bytes. In average case, the watermarked images produced a peak to signal noise ratio (PSNR) of around 38 dB which is considered as a sustainable quality. The number of bits embedded per byte (bpB) in each carrier image is 2. The image fidelity (IF) is used to identify the similarities between watermarked and original images. The average value for IF is 0.9994 which ensured that the quality degradation at the watermarked image is minimal.

Table 1. Results of embedding of 195894 bytes of information in each image of dimension 512 x 512

Carrier Image	**Max. Payload (bytes)**	**PSNR (dB)**	**IF**	**bpB**
Lena	196608	36.97	0.9992	2
Baboon	196608	38.75	0.9995	2
Airplane	196608	36.35	0.9996	2
Earth	196608	37.60	0.9993	2
Sailboat	196608	37.85	0.9995	2
Foster City	196608	37.44	0.9996	2
Oakland	196608	37.53	0.9994	2
San Diego	196608	38.73	0.9997	2
AVG	**196608**	**37.65**	**0.9994**	**2**

A comparative study has also been made among Discrete Cosine Transform (DCT), Quaternion Fourier Transform (QFT) and Spatio-Chromatic DFT (SCDFT) based embedding techniques [8–11] with the proposed CIA2D-SDHT, based on payload and the PSNR. It is seen from table 2 that the proposed technique offers a significant enhancement of payload by retaining a good visual clarity watermarked images over QFT, DCT, FFT and SCDFT [8–11, 19]. The payload is more than 192768 bytes and PSNR enhancement is around 7 dB for the 'Lena' image. On comparing the proposed CIA2D-SDHT technique with the SDHTIWCIA technique [17], it is seen that enhancement of the payload along with a minor compromising on PSNR values in average cases are ensured. In the proposed technique, the PSNR and Payload has also been

improved as compared to R.O., E. Sofy and H.H.Zayed's method [21] and Ghasemi et Al.'s method [22].

Table 2. Comparison of payload and PSNR for "Lena" image in the existing technique namely SCDFT, QFT and DCT based techniques [19], SDHTECIA [18], SDHTIWCIA [17], R.O, E. Sofy and H.H.Zayed's method [21] and Ghasemi et Al.'s method [22]

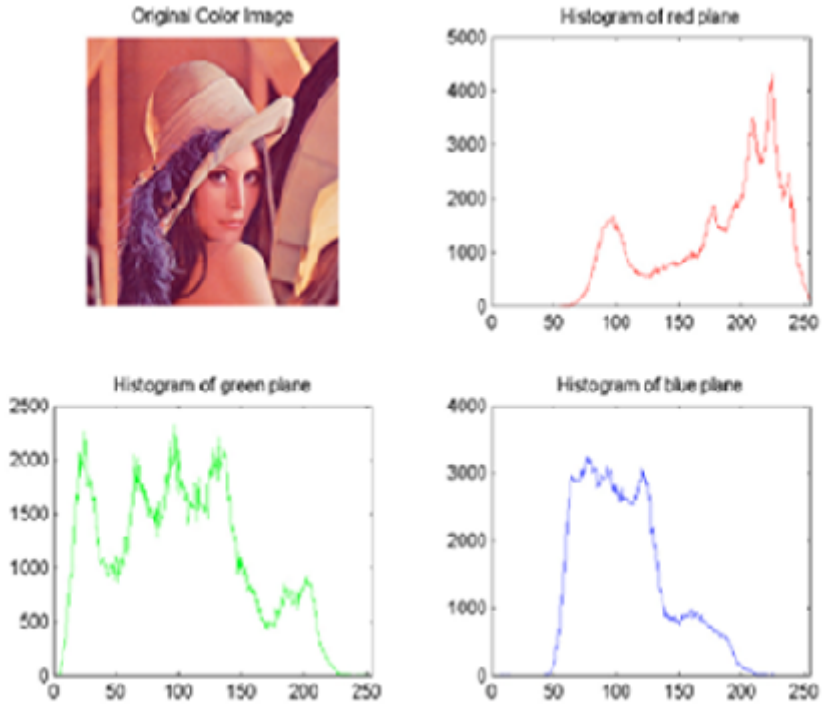
Technique	**Payload(bytes)**	**PSNR(dB)**
SCDFT	3840	30.10
QFT	3840	30.92
DCT	3840	30.40
SDHTECIA [18]	97794	44.87
SDHTIWCIA [17]	147456	37.95
Sofy R.O. and H.H.Zayed's method [21]	123301	31.8
Ghasemi et Al.'s method [22]	131072	35.17
CIA2D-SDHT	**196608**	**36.97**

The histogram analysis is done by comparing the results of the statistical parameters namely the mean, standard deviation and median with respect to the original and the watermarked image. The experimental results for "Lena" image is given in table 3 where the comparison of histogram has been done in channel-wise manner. The experimental results in table 3 also ensured that the differences between two images are minimal and hard to detect.

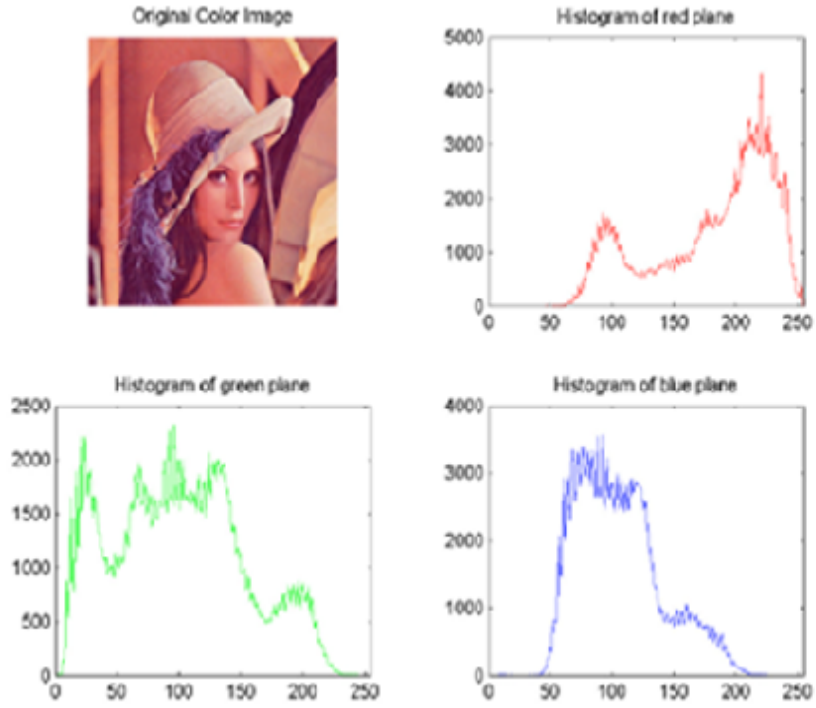
Table 3 Comparison of mean, median and standard deviation of original and watermarked "Lena" of dimension 512 x 512

Image	**Channel**	**Mean**	**Median**	**Standard Deviation**
Original Lena	R	180.22	197	49.05
	G	99.05	97	52.88
	B	105.41	100	34.06
Embedded Lena	R	179.64	196	49.11
	G	98.58	97	52.94
	B	104.90	100	34.20

The histogram of three different channels for original and watermarked "Lena" is depicted in fig 3.



(a) Histogram of original "Lena"



(b) Histogram of watermarked "Lena"

Fig. 3 Comparison of histogram between original and watermarked "Lena" image

The standard deviation analysis for varying sizes over the “Lena” image is shown in fig 4. It ensured that the change made into the watermarked image using our proposed technique is minimal and almost identical to the original image.

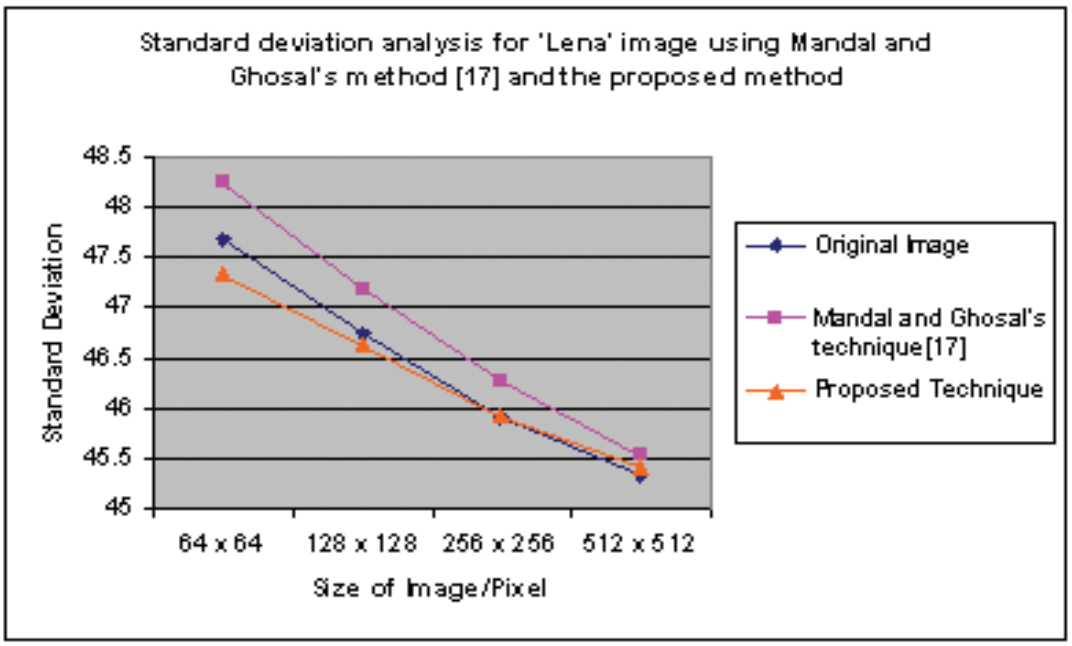


Fig. 4 Comparison of standard deviation between source and watermarked ’Lena’ image using Mandal and Ghosal’s method [17] and the proposed technique

Watermarked image may be altered during transmission. These alterations may be a result of intentional attacks such as filtering, blurring etc. or unintentional distortions such as lossy-compression, channel noise addition etc. Due to various kinds of attacks, an altered version of the watermarked image is available to the decoder. In a given authentication system, the role of the attacker is to alter the image in such a way that visually the image is not considerably degraded, however, the frequency distribution is transformed in such a manner that the decoder fails to extract the hidden data. But, in CIA2D-SDHT scheme, 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. 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. If the authentication process fails, the recipient sends a negative acknowledgement to the sender. The sender can realize about the attack and resends the watermarked image to the recipient. Thus, any kind of visual/geometrical attacks on the watermarked image are easily detectable. Fig 5, shows the six different states of the images, namely, (i) without any visual attack, (ii) Gaussian white noise attack with variance 0.01, (iii) Poisson noise attack, (iv) speckle noise attack with the variance 0.005, (v) salt and pepper

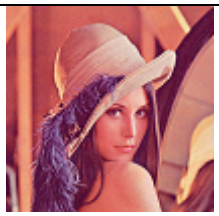
noise attack with noise density 0.005 and (vi) image blurring attack for 2 x 2 neighborhood pixel blocks.

(a) Watermarked "Lena" before attack

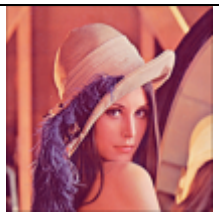
(b) Watermarked "Lena" with Gaussian White Noise Mean(μ)=0, Variance(σ)=0.01

(c) Watermarked "Lena" with Poisson Noise

(d) Watermarked "Lena" with Speckle Noise Mean(μ)=0, Variance(σ)=0.005



(e) Watermarked "Lena" with Salt & Pepper Noise Noise Density(η)=0.005



(f) Watermarked "Lena" with Image Blurring

Fig. 5 Watermarked "Lena" image on different kinds of visual attacks

It is seen from table 4 that the PSNR values obtained from the watermarked images (after different kinds of visual attacks) are still high and the attacked images are well perceptible as well. Also, the attacked images preserved a significant amount of watermark data. But, if a single bit is modified in the watermarked image then it is considered as unauthentic and the recipient can easily understand about the tampering. Thus, any kind of attack cannot hamper the principle of authentication in our proposed scheme.

Table 4 Comparison of PSNR values under different kinds of visual attacks on watermarked images

Images	**PSNR before attack**	**PSNR after Gaussian White Noise**	**PSNR after Poisson Noise**	**PSNR after Salt & Pepper Noise**	**PSNR after Speckle Noise**	**PSNR after Blurring Effect**
Lena	36.97	20.11	26.73	27.68	27.74	27.94
Baboon	38.75	20.09	26.92	27.79	28.06	20.73
Airplane	36.35	20.09	25.22	27.30	25.36	26.35
Earth	37.60	20.04	26.75	27.92	28.07	28.42
Sailboat	37.85	20.20	26.89	27.62	27.73	24.79

5. Conclusion

The CIA2D-SDHT technique is an image authentication process in frequency domain to enhance the security compared to the existing algorithms. Authentication is done by embedding secret data in a carrier image. Using the technique, two bits can be embedded in each frequency component of a 2 x 2 image sub-block. Experimental results conform that the proposed algorithm performs better than the Discrete Cosine Transform (DCT), Quaternion Fourier Transformation (QFT) and Spatio-Chromatic DFT (SCDFT) based scheme and robustness is achieved by hiding data in both positive and negative frequency components.

Acknowledgements

Authors expressed deep sense of gratitude to the PURSE scheme of DST, Govt. of India under which the research has been carried out at department of Computer Science and Engineering, University of Kalyani, India.

References

1. Lee Y. K., Chen L. H. (2000) "High capacity image steganographic model", IEEE Proceedings-Vision, Image, and Signal Processing, Vol.147, No.3, pp.288-294.
2. Chang, C. C., Hsiao J. Y. and Chan C. S. (2003), "Finding optimal least-significant-bit substitution in image hiding by dynamic programming strategy", Journal of Pattern Recognition, Vol.36, No.7, pp.1583-1595.
3. Chang, C. C., Lin C. C., Tseng C. S. and Tai W. L. (2007), "Reversible hiding in DCT-based compressed images", Journal of Information Sciences, Vol.177, No.13, pp.2768-2786.
4. Gutub A.A.A (2010), "Pixel Indicator Technique for RGB Image Steganography", Journal of Emerging Technologies in Web Intelligence, Vol. 2, No. 1, pp.56-64.
5. Chang C. C., Lin C. Y. and Wang Y. Z. (2006), "New image steganographic methods using run-length approach", Journal of Information Sciences, Vol.176, No.22, pp.3393-3408.
6. Yang B., Lu Z. M. and Sun S. H. (2005), "Reversible watermarking in the VQ-compressed domain", Proc. of Fifth IASTED International Conference on Visualization, Imaging, and Image Processing (VIIP2005), January 2005, Benidorm, Spain, pp.298–303.
7. Chang C. C., Kieu T. D. andWuW. C. (2009), "A lossless data embedding technique by joint neighboring coding", Pattern Recognition, Vol.42, No.7, pp.1597-1603.
8. Pei S.C., Ding J.J. and Chang J.H. (2001), "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.

9. Ahmed N., Natarajan T. and Rao K. R. (1974), “Discrete cosine transform, IEEE Transactions on Computers”, Vol.C-23, pp.90-93.
10. Rioul and Duhamel P. (1992), “Fast algorithms for wavelet transforms”, IEEE Transaction on Information Theory, Vol.38, No.2, pp.569-586.
11. Brigham E. O. (1974), “The fast Fourier transform”, Englewood Cliffs, NJ: Prentice-Hall.
12. Du W. C. and Hsu W. J. (2003), “Adaptive data hiding based on VQ compressed images”, Proc. of IEEE International conference on Vision, Image, and Signal Processing, Vol.150, No.4, pp.233-238.
13. Maity S.P. and Kundu M.K. (2009), “DHT domain digital watermarking with low loss in image information”, International Journal of Electronics and Communication, doi: 10.1016/j.aeue.2008.10.004, pp.1-15.
14. Varsaki et al. (2010), “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, May, 2010, Brussels, Belgium, pp.1-11.
15. Watson A.B., Poirson A. (1986), “Separable two dimensional discrete Hartley transform”, J.Opt.Soc. Am. A., Vol 3, NO. 12.
16. Weber Allan G., 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).
17. Mandal J.K, Ghosal, S.K (2012) “Separable Discrete Hartley Transform based Invisible Watermarking for Color Image Authentication (SDHTIWCIA)”, Proc. of Springer Second International Conference on Advances in Computing and Information Technology (ACITY-2012), July, 2012 , Chennai, India, pp. 767-776.
18. Mandal J.K., Ghosal S.K (2012) “Separable Discrete Hartley Transform based Embedding for Color Image Authentication (SDHTECIA)”, Second National Conference on Computing and Systems (NACCS-2012), March, 2012, Burdwan, India, pp. 178-183.
19. T. T. Tsui, X. -P. Zhang, and D. Androutsos (2008) “Color Image Watermarking Using Multidimensional Fourier Transformations”, IEEE Trans. on Info. Forensics and Security, vol. 3, no. 1, pp. 16-28.
20. M. Manoochehri et al (2011) “A Novel Synthetic Image Watermarking Algorithm Based on Discrete Wavelet Transform and Fourier-Mellin Transform”, Proc. of IEEE 3rd International Conference on Communication Software and Networks (ICCSN), May 2011, Xi'an, China, pp. 265-269.

21. R.O., El.Sofy, H.H.Zayed (2009) “An adaptive Steganographic technique based on the integer wavelet transforms”, Proc. of IEEE International Conference on Networking and Media Convergence (ICNM 2009), March 2009, Cairo, Egypt, pp. 111-117.
22. Elham Ghasemi, Jamshid Shanbehzadeh and Bahram ZahirAzami (2011) “A Steganographic method based on Integer Wavelet Transform and Genetic Algorithm”, Proc. of IEEE International Conference on Communications and Signal Processing (ICCSP), February 2011, Calicut, India, pp. 42-45.