A FRAGILE WATERMARKING BASED ON SEPARABLE DISCRETE HARTLEY TRANSFORM FOR COLOR IMAGE AUTHENTICATION (FWSDHTCIA)

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

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

ABSTRACT

In this paper, a fragile watermarking based on two-dimensional Separable Discrete Hartley Transform has been proposed for color image authentication (FWSDHTCIA). Two dimensional SDHT is applied on each 2 × 2 sub-image block of the carrier image in row major order and produces four frequency components in transform domain. Due to the high sensitivity of human eye on green channel, only one authenticating message/image bit is fabricated at the second bit position of each frequency component for every 2 × 2 green sub-matrix. Unlikely, in every 2 × 2 red and blue sub-matrices, two bits from the authenticating message/image are fabricated at the second and third bit position of each frequency component as the human eye is less sensitive on red and blue channels as compared to green. After fabricating the authenticating watermark (message/image), a frequency adjustment strategy has been applied to get back the less distorted watermarked image in spatial domain. A delicate re-adjustment has been incorporated in the first frequency component of each 2 × 2 mask, to keep the quantum value positive in spatial domain without hampering the authenticating watermark bits. Two dimensional inverse SDHT (ISDHT) is applied on each 2 × 2 sub-mask as post embedding operation to produce the watermarked image. At the receiving end reverse operation is performed to extract the stream which is compared to the original stream for authentication. Experimental results conform that the proposed algorithm has improvised the payload and PSNR values over SDHTIWCIA [7] scheme which is previously proposed by us. Also, the proposed FWSDHTCIA scheme produces much better result than the Discrete Cosine Transform (DCT), Quaternion Fourier Transformation (QFT) and Spatio-Chromatic DFT (SCDFT) based techniques.

KEYWORDS

FWSDHTCIA, SDHT, ISDHT, DCT, QFT, SCDFT and Watermarked image.

1. INTRODUCTION

Due to the rapid advancement of internet technology, the protection of digital information is an important issue. Watermarking is such an idea by which one can incorporate useful information into various digital media like image, audio and video etc. for ownership evidence, fingerprinting, authentication and integrity verification, content labeling and protection, and usage control. In our proposed scheme, we shall focus on separable discrete Hartley transform based fragile watermarking scheme for color image authentication.

The watermark data can be incorporated in both spatial and frequency domain whereas the frequency domain techniques provides better security and robustness. Few frequency transformation approaches previously used us for embedding watermark message/image are discrete cosine transform (DCT), discrete wavelet transform (DWT), discrete Fourier transform (DFT) etc. In this paper, we have introduced a new kind of transformation technique for watermarking purpose, which is separable discrete Hartley transform (SDHT). In frequency domain, the watermark bits are embedded into the frequency component of the transformed image pixels in a block wise manner. In 1996-97, I. J. Cox et al. [1, 2] developed an algorithm to inserts watermarks into the frequency components and spread over all the pixels. DCT-based image authentication is developed by N. Ahmidi et al. [3] using just noticeable difference profile [4] to determine maximum amount of watermark signal that can be tolerated at each region in the image without degrading visual quality. But, the problem with the DCT based technique is that the payload capacity is very less. In general, robust image watermarking techniques are used to protect ownership of the digital image. In contrast, the purpose of fragile image watermarking techniques is image authentication, that is, to ensure the integrity of the digital image. Many image authentication methods through fragile watermarking have been proposed so far. The algorithms perform by determining whether or not the digital image has been tampered with.

Consequently, to enhance the payload capacity and to use the proposed technique for authentication purpose, the concept of two dimensional separable discrete Hartley transform and a 128 bit message digest has been introduced. The Discrete Hartley Transformation [5] is used to transform each 2 × 2 sub-image block of the cover image from spatial domain to frequency domain. The frequency components values are used for embedding authenticating message/image bits. After embedding authenticating watermark data, inverse Separable Discrete Hartley Transformation is applied to get back the watermarked image into spatial domain. If carefully observe the pixel values are not preserved though embedded bits are intact, but, if we apply 2D-SDHT again, the frequency component values are not changed. The Hartley transform produces real output for a real input which can be designated as its own inverse. Thus it has computational advantages over the discrete Fourier transform, although analytic expressions are usually more complicated for the Hartley transform. The definition of SDHT is the difference of even and odd parts of the DFT.

The two dimensional Separable Discrete Hartley Transform (2D-SDHT) of spatial value f(x,y) for the image of size M x N is given in equation (1).

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

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 *x, y* and f(x,y) is intensity value of pixels in spatial domain. The sequence *cas* defined by:

$$cas(2\prod ux/N) = cos(2\prod ux/N) + sin(2\prod ux/N) \qquad (2)$$

$$cas(2\prod vy/M) = cos(2\prod vy/M) + sin(2\prod vy/M) \qquad (3)$$

Similarly, the inverse transformation to convert frequency component to the spatial domain value is defined in equation (4).

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

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

The aim of FWSDHTCIA emphasizes on protection of secret information against unauthorized access. The proposed scheme exploits image authentication process by embedding the watermark data in both negative and positive frequency components along with the message digest MD (which is generated from watermark data) into the carrier image with a minimum change in visual pattern and improved security.

Problem motivation and formulation of transformation technique is given in section 2. Section 3 of the paper, deal 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. TRANSFORMATION TECHNIQUES

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

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

Where, u and v varies from 0 to 1 and $p(i,j)$ represents the spatial domain carrier image bytes of each 2 x 2 sub-mask, whereas $P_s(u,v)$ represents the frequency components respectively. In each 2 x 2 red and blue sub-masks, two bits are fabricated at second and third bit positions of the LSB part in each frequency component. Unlikely, only one bit is embedded at the second bit position in each frequency component of a 2 x 2 green sub-mask as the human eye is most sensitive for green channel.

Similarly, by applying the inverse 2D-SDHT, the 2 x 2 transformed masks can be formulated as:

$$p(i,j) = \sum_{u=0}^{1} \sum_{v=0}^{1} (-1)^{ui} (-1)^{vj} P_s(u,v) = p_{i,j} \text{ (say)}, \tag{6}$$

Where, i and j varies from 0 to 1 and the variable u and v are the frequency variables corresponding to the pixel intensity value $p_{i,j}$ in spatial domain. The last two untouched bits in each frequency component value ensures that, after applying inverse 2D-SDHT, all frequency component values are still non-fractional. Moreover, the re-adjustment phase ensures that all the inverse 2D-SDHT values are non negative and less than or equal to the maximum and greater than or equal to minimum possible value of a byte.

3. PROPOSED TECHNIQUE

In this paper a fragile watermarking scheme has been proposed for color image authentication (FWSDHTCIA) in frequency domain based on the two dimensional Separable Discrete Hartley Transform (SDHT). Initially, a 128 bit message digests (MD) and size of the watermark data is embedded using the proposed FWSDHTCIA scheme for authentication purpose. The 2D-SDHT is applied on 2 × 2 sub-image block for converting the spatial domain values to frequency components. This process is continued till the last sub-image block of the carrier/cover image in a row major order. Due to the high sensitivity of human eye on green channel, only one authenticating message/image bit is fabricated at the second bit position (LSB-2) of each frequency component for every 2 × 2 green sub-matrix. Unlikely, in every 2 × 2 red and blue sub-matrices, two bits from the authenticating message/image are fabricated at the second and third bit position (LSB-2 and LSB-3) of each frequency component as the human eye is less sensitive on red and blue channels as compared to green. The frequency adjustment procedure followed by the embedding has been applied on each embedded frequency component to select the component value closest to the original before embedding by the varying combination of 0's and 1's without hampering the fabricated bits. The first frequency component (except the last two consecutive bit positions and the embedded bit positions) may be used for re-adjustment of frequency components whenever it violates the basic principles of pixel representation in spatial domain like non-negative pixel value or a value less than or equal to 255 for eight bit representation. After re-adjustment, the 2D-ISDHT is applied again to get back valid pixel component value in spatial domain. In the proposed technique, the value of the frequency components does not become fractional as we are not altering the least two significant bits i.e. LSB-0 and LSB-1. The re-adjustment method works by adding multiples of eight for 2 × 2 green sub-matrix and multiples of sixteen for 2 × 2 red and blue sub-matrices whenever a frequency component value becomes negative. If any frequency component value becomes greater than 255, an even multiple of eight is deducted from the first frequency component of each 2 × 2 green sub-matrix and an even multiple of sixteen is deducted from the first frequency component of each 2 × 2 red and blue sub-matrices. Inverse Transform is applied on each 2 x 2 mask as post embedding to transformed watermarked image (sometimes, re-adjusted as well) in frequency domain to convert back into spatial domain. By performing the reverse operation, authenticating message\image can be extracted from the embedded image and new message digest MD' can be calculated from the extracted authenticating bits and the same is compared with extracted MD for authentication.

Consider, a 2 x 2 color image block of a cover/carrier image which consists of three sub-matrices namely R, G and B. Two dimensional separable discrete Hartley transform is applied to convert it from spatial domain pixel value to frequency components value in transform domain.

R_1={164,63,120,135}, G_1={150,57,125,97}, B_1={71,31,62,33)

Applying 2D-SDHT the transformed frequency component values obtained as given below:

$F(R_1)$={482,86,-28,116}, $F(G_1)$={429,121,-15,65}, $F(B_1)$={197,69,7,11}

The authenticating watermark message/image bit stream *10100001011000001100* is embedded based on the proposed embedding strategy. Hence, the embedded frequency components are:

$E(F(R_1))$={490,90,-16,116}, $E(F(G_1))$={425, 125, -15, 65}, $E(F(B_1))$={193,65,11,7}

Now, we have applied a frequency adjustment methodology by which we can ensure the enhancement of quality without losing the embedded authenticating bits. It is applied for each embedded frequency component by taking the closest value of that component without hampering the least four significant bits. So, the new sub-matrices after frequency adjustment become:

$A(E(F(R_1)))$={490,90,-32,116}, $A(E(F(G_1)))$={ 425, 125, -15, 65}, $A(E(F(B_1)))$= {193,65,11,7}

Again, if we apply inverse 2D-SDHT, then the regenerated pixel component values in spatial domain are:

$F^{-1}(A(E(F(R_1))))$={166,63,124,137}, $F^{-1}(A(E(F(G_1))))$={150,55,125,95},
$F^{-1}(A(E(F(B_1))))$ = {69,33,60,31}

It is seen that the modified pixel values are non-fractional as, the last two bits of each frequency component are unaltered. Re-adjustment of the first frequency component value is not needed in this example as all the spatial domain values are non-negative and not greater than 255.

The proposed scheme is described in the following sections namely, the Insertion, Re-adjustment and the Extraction. These are described in sec. 1, 2 and 3 respectively.

3.1. Insertion

Insertion is made at each transformed blocks of size 2 x 2 using two dimensional separable Discrete Hartley Transform. All the three channels of 2 x 2 masks in a 24 bit color image have been chosen for embedding based on their perceptibility. Since green color is most sensitive for human eye than red and blue channels, two bits from the authenticating message are fabricated in every frequency component of each 2 x 2 green sub-matrix whereas the bit embedding locations are second and third bit position. Unlikely, the second bit position is chosen for embedding one bit in each frequency component of every 2 x 2 red and blue sub-matrices. The authenticating message/image bits size is [B * {3 * (m * n)} – (MD + L)] where MD and L are the message digest and dimension of the authenticating image respectively for the source image size of m x n bytes. The L and MD are used in extraction phase to extract the whole authenticating message\image and to authorize authenticating message/image.

Steps:

1) Obtain 128 bits message digest *MD* from the authenticating message/image.

2) Obtain the size of the authenticating message/image (($L=w+h$) bits, where w bits for width and h bits for height). The authenticating watermark message/image (W) bits size is:

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

Where, average bits per byte is *B, MD* and *L* are the message digest and dimension of the authenticating message/image respectively for the source image size of *M* x *N* bytes. In our proposed scheme, for ten different benchmark images which are shown in Fig. 1, the avg. bit per byte is 1.66, whereas the dimension *L* consists of 128 and 32 bits.

3) Read authenticating message/image data do:

- The cover image *(I)* is partitioned into 2 x 2 non-overlapping blocks in row major order. Each 2 x 2 block is 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 $0 \le i \le 1$and $0 \le j \le 1$.
- Apply two dimensional SDHT on each sub-matrices corresponding to the red, green and blue channels separately which produces four frequency components $f_{i,j}$, $f_{i,j+1}$, $f_{i+1,j}$ and $f_{i+1,j+1}$ with respect to each sub-matrix.
- N number of bits is embedded in each frequency component of every 2 x 2 sub-matrix starting from the LSB-2 based on the channel (R/G/B) we have chosen. The mathematical expression can be written as follows:

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

[Embed authenticating message/image bit as per the above rules.]

4) A frequency adjustment method has been applied to get frequency components values closest to the original without hampering the hidden bits. The frequency adjustment has been made by altering left most *(T-N-2)* number of bits followed by choosing the specific frequency component value closest to the original one where *T* is the total number of bits in a frequency component.

5) Apply two dimensional inverse SDHT using identical masks. During the 2D-ISDHT phase, if the pixel value in spatial domain becomes negative or greater than 255; then the re-adjustment of

first frequency component at step 6 is applied repeatedly until and unless the pixel value becomes non-negative and not less than or equal to 255. Then, 2D-ISDHT is applied again to get back pixel component values in spatial domain.

6) Apply the re-adjustment phase on the first frequency component of each 2 x 2 sub-matrix (optionally).

7) Repeat step 2 to step 6 for the whole authenticating message/image size, content and for message digest *MD*. The successive block embedding operation produces the watermarked image *(I')*.

8) Stop.

3.2 Re-Adjustment

In the proposed algorithm after embedding we have used inverse transformation (ISDHT) to obtain the embedded image in spatial domain. Applying inverse transform on identical mask with embedded data of the frequency component value which may change and can generate the following situation:

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

The concept of re-adjust phase is to handle the above two serious problems by using the first frequency component of each 2 × 2 mask. In this phase if the converted value is negative (-ve) i.e. for case (i), the operation applied for each 2 x 2 sub-matrix is as follows:

$$f(0,0) = f(0,0) + i * 8;\ if(c=G)$$
$$= \mid f(0,0) + i * 16;\ if(c=G\ or\ B) \qquad (5)$$

Here, *f(0,0)* is the first frequency component of a 2 x 2 sub-matrix and *i* is a counter which is multiplied by the multiple of eight/sixteen, takes values in the range, i = 1, 2, 3, …, n. That means, *i* is multiplied and incremented in each step, till all the converted value in spatial domain i.e., pixel value becomes positive.

For case (ii), if the converted value exceeds the maximum value of a byte (i.e., 255) in spatial domain, then the operation applied for each 2 x 2 sub-matrix is as follows:

$$f(0,0) = f(0,0) - j * 8;\ if(c=G)$$
$$= \mid f(0,0) -j * 16;\ if(c=G\ or\ B) \qquad (6)$$

Here, *j* is a counter which is multiplied by the even multiple of eight/sixteen, takes values in the range, j = 2, 4, 6,…, n whereas, *n* is the positive even integer. That means *j* is multiplied and incremented in each step till all the converted value in spatial domain value becomes less than or equal to 255.

3.3. Extraction

The authenticated watermarked image is received in spatial domain. During extraction, the watermarked image has been taken as the input and the authenticating message/image size, image content and message digest *MD* are extracted from it. All extraction is done in frequency domain from frequency component.

Steps:

1) The watermarked image (I') is partitioned into 2 x 2 non-overlapping blocks in row major order. Each 2 x 2 image block is 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 $0 \le i \le 1$ and $0 \le j \le 1$.

2) For each 2 x 2 sub-matrix, do the following operations:

- To transform every 2 x 2 pixel blocks consisting of $p_{i,j}$, $p_{i,j+1}$, $p_{i+1,j}$ and $p_{i+1,j+1}$ from spatial domain to frequency domain, two-dimensional separable discrete Hartley Transform (2D-SDHT) has been applied on each sub-matrices corresponding to the red, green and blue channels separately which produces four 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 $0 \le j \le 1$.

- N number of bits is extracted from each frequency component of every 2 x 2 sub-matrix, starting from the LSB-2 based on the channel (R/G/B) we have chosen. The mathematical expression can be written as follows:

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

  [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 value.

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

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) Apply two dimensional inverse SDHT (2D-ISDHT) using identical sub-matrices.

6) Stop.

4. Results, Comparison and Analysis

This section represents the results, discussion and a comparative study of the proposed FWSDHTCIA scheme with the DCT, QFT based and Spatio-Chromatic DFT based watermarking methods in terms of payload capacity and visual interpretation, on the basis of peak signal to noise ratio (PSNR) analysis, bits per byte (BPB) and histogram analysis. Benchmark (PPM) images [6] are taken to formulate results and are shown in Fig-1. All cover images are 512 x 512 in dimension whereas the gold coin (i.e. the secret data) is embedded into the various source benchmark images. The experiment deals with ten different color images (i-x), where each pixel is represented by three intensity values RGB (Red, Green and Blue). Images are labeled as: (i) Lena, (ii) Baboon, (iii) Pepper, (iv) Airplane, (v) Splash, (vi) Earth, (vii) Sailboat, (viii) Foster City, (ix) San Diego, (x) Oakland. On embedding the watermark image that is the Gold-Coin image, the newly generated watermarked image produces a good visual clarity with high payload.

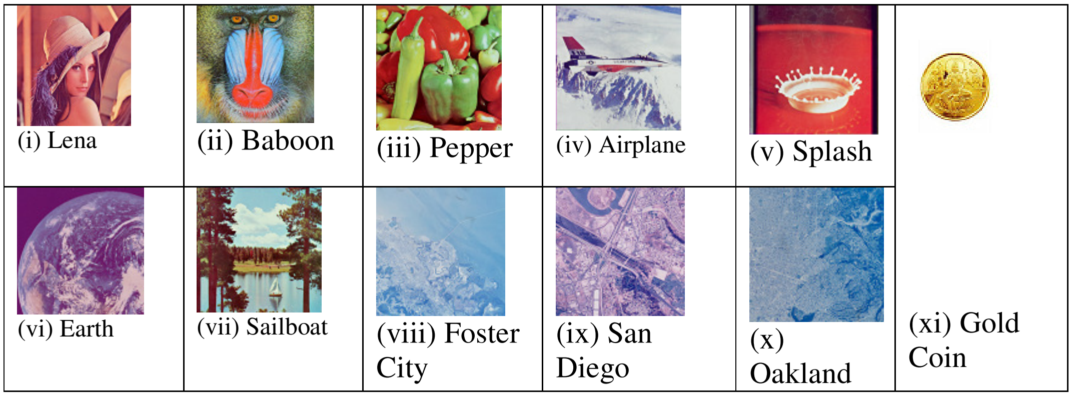


Figure 1. Different Cover images (512 x 512) and that of common authenticating image (232 x 234)

In order to test the security of the watermark data, it is quite difficult for the observer to detect the difference between the original and embedded image. From Table 1, we can identify the payload for carrier images which is 163840 bytes where the dimension of each original image is 512 x 512. After embedding the watermark data, the watermarked image is also retain a good visual clarity and produces value of 39 dB for peak to signal noise ratio in average cases. Moreover, the histogram analysis shows the changes made in the three images are more stable after embedding hidden bits. The table also shows that the bits embedded per byte (bpb) for each carrier image is 1.66. Fig-2 shows different states of modifications (before and after) of three different images viz. Lena, Baboon and Peppers.

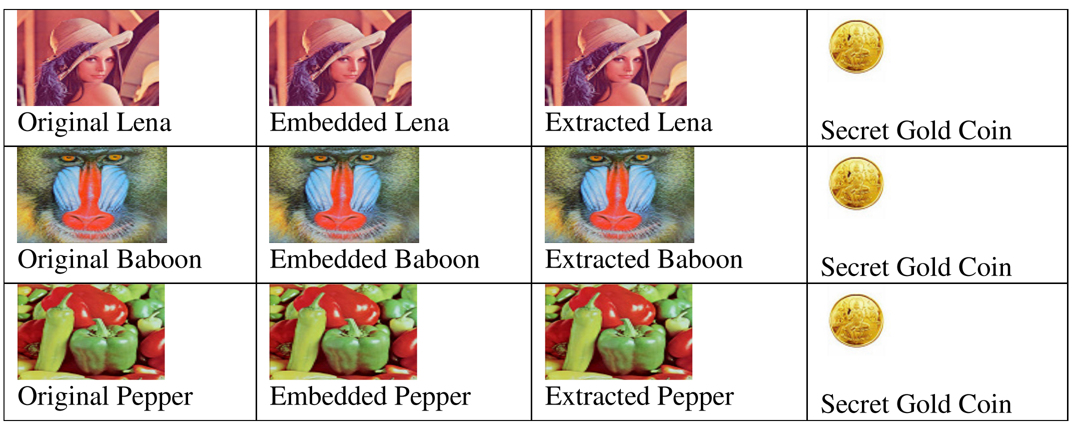


Figure 2. Cover, Watermarked, Extracted and Watermark Images using proposed FWSDHTCIA scheme

Also, a comparative study has been made among Discrete Cosine Transform (DCT), Quaternion Fourier Transformation (QFT) and Spatio-Chromatic DFT (SCDFT) based information embedding schemes [8] and our proposed FWSDHTCIA scheme based on the payload and the PSNR values. In the proposed scheme, the payload and PSNR is much more as compared to the SCDFT, QFT and SCDFT based techniques, besides pertaining good visual clarity watermarked images. For the Lena image, the payload is more than 160000 bytes and PSNR enhancement is around 9 dB. The image fidelity (IF) of 0.9995 in average case specifies that the distortion of the image is very minor.

Table 1. Results of embedding of 162918 bytes of information in each Image of dimension 512 x 512

Carrier Image	**Max. Payload (byte)**	**PSNR (dB)**	**IF**	**BPB**
Lena	163840	38.69	0.9995	1.66
Baboon	163840	40.11	0.9997	1.66
Pepper	163840	38.77	0.9991	1.66
Earth	163840	39.15	0.9996	1.66
Sailboat	163840	39.36	0.9996	1.66
Airplane	163840	38.13	0.9997	1.66
Foster City	163840	38.91	0.9997	1.66
Oakland	163840	39.45	0.9996	1.66
San Diego	163840	40.05	0.9998	1.66
Splash	163840	37.58	0.9992	1.66
AVG	163840	*39.02*	*0.9995*	1.66

Table 2. Comparison results of Payload Capacities and PSNR for Lena image in the existing technique namely SCDFT, QFT, DCT based schemes [8] and SDHTIWCIA [7]

Technique	**Payload(bytes)**	**PSNR(dB)**
SCDFT	3840	30.1024
QFT	3840	30.9283
DCT	3840	30.4046
SDHTIWCIA	147456	37.82
FWSDHTCIA	*163840*	*38.69*

In Fig. 3 and Fig. 4, the comparison result of the bpb and PSNR values for embedded 'Lena' image is shown in the form of a chart with varying sizes of carrier images viz. 64 x 64, 128 x 128, 256 x 256 and 512 x 512, where the comparison has been made between proposed FWSDHTCIA and previously proposed SDHTIWCIA [7] scheme mentioned by us. So, by comparing the proposed FWSDHTCIA scheme with the previously proposed SDHTEIWCIA scheme [7], one can easily identify the enhancement of the payload capacity along with the PSNR values in average cases. Also, the chart explains how efficiently we have enhanced the payload capacities and PSNR values along with the sizes of the cover images.

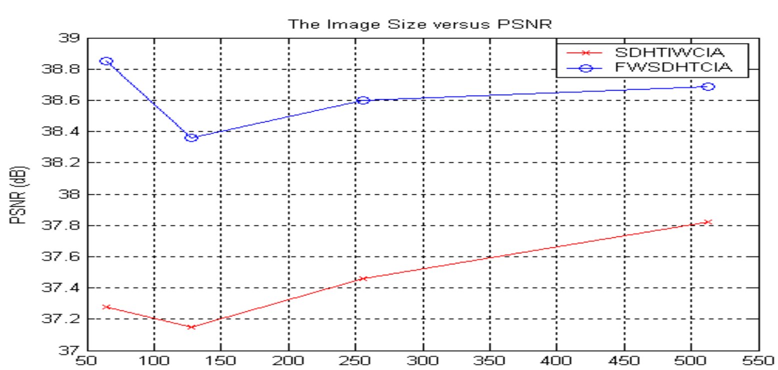
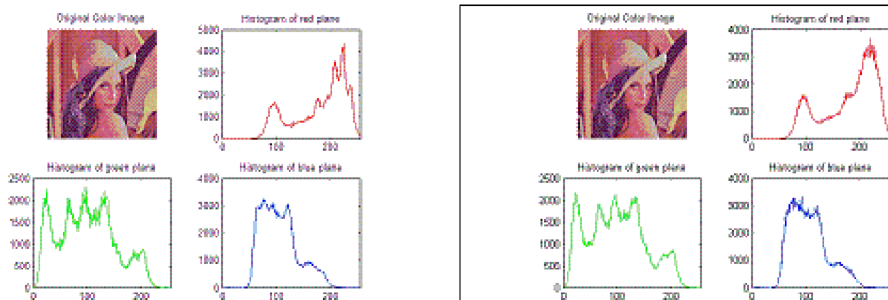


Figure 3. Comparisons Results of Size of Image/Pixel and PSNR among Varying Sizes of Embedded Lena Image with schemes SDHTIWCIA [7] and FWSDHTCIA

Figure 4. Comparisons Results of Size of Image/Pixel and Capacity (bits) among Varying Sizes of Embedded Lena Image with schemes SDHTIWCIA [7] and FWSDHTCIA

In Fig-3, the histogram analysis of Lena image is shown before and after embedding watermark data in an individual channel wise manner.



Histogram of Original Lena

Histogram of Watermarked Lena

Fig-3: Comparisons Results of Histogram between of Original and Watermarked Lena Image

The histogram analysis shows the comparison results in terms of mean, standard deviation and median between original and watermarked 'Lena' image in a channelwise manner. Moreover, The experimental results in Table 3 ensures that the differences between two images is very minimal and tough to detect for the attacker. Also, from Table 3, one can easily identify that the changes made in the standard deviation for green channel after embedding watermark message/image is less as compared to the standard deviation of other two channels due to the less number of bit embedding in green channel.

Table 3. Comparison results of Mean, Median and Standard Deviation of Original and Watermarked Lena Image

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
Watermarked Lena	R	179.68	196	49.15
	G	98.55	97	52.84
	B	104.92	100	34.19

5. CONCLUSION

The FWSDHTCIA scheme is an image authentication process in frequency domain to enhance the security compared to the existing algorithm. Authentication is done by embedding watermark data in a carrier image. Using the technique a total of twenty bits can be embedded in 2 x 2 image block. Experimental results conform that the proposed algorithm performs better than existing techniques.

REFERENCES

[1] J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, Secure spread spectrum watermarking for images, audio and video, in Proc. IEEE Int. Conf. Image Processing, Lausanne, Switzerland, Sep. 16-19, vol. 111, pp. 243-246, 1996.

[2] J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, Secure spread spectrum watermarking for multimedia, IEEE Trans. Image Processing, vol. 6, no. 12, pp. 1673-1687, 1997.

[3] N. Ahmidi, R. Safabkhsh, A novel DCT-based approach for secure color image watermarking, in Proc. Int. Conf. Information technology: Coding and Computing, vol. 2, pp. 709-713, Apr. 2004.

[4] H. Chou, Y. C. Li, A perceptually tuned sub-band image coder based on the measure of just-noticeable distortion profile, IEEE Trans. Circuits Syst. Video Technology vol. 5, no. 6, pp. 467-476, Dec. 1995.

[5] Watson A.B., Poirson A., Separable two dimensional discrete Hartley transform, Vol 3.NO. 12/December 1986/J.Opt.Soc. Am. A.

[6] 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).

[7] 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 Infromation Technology (ACITY-2012), July 13-15, 2012, Vol. 2,ISBN-978-3-642-31551-0, pp. 767-776, Chennai, India.

[8] T. T. Tsui, X. –P. Zhang, and D. Androutsos, Color ImageWatermarking Usimg Multidimensional Fourier Transfomation, IEEE Trans. on Info. Forensics and Security, vol. 3, no. 1, pp. 16-28, 2008.

Authors

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. Dean Faculty of Engineering, Teachnology & Management, working in the field of Network Security, Steganography, Remote Sensing & GIS Application, Image Processing. 25 years of teaching and research experiences. Eight Scholars awarded Ph.D. one submitted and eight are pursuing. Total number of publications is more than two hundred thirty in addition of publication of five books from LAP Lambert, Germany.

Sudipta Kr Ghosal, is an 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 research for PhD in Color Image Authentication from University of Kalyani, India under the supervision of Prof. J.K.Mandal. Mr. Ghosal has around three years of experience in teaching and industry. He has ten publications in the national and international conference proceedings.