Imperceptible Image Authentication Using Wavelets

Anirban Goswami[1] and Nabin Ghoshal[2]
(Corresponding author: Anirban Goswami)
Department of Information Technology, Techno India[1]
EM-4/1, Sector-V, Salt Lake, Kolkata, West Bengal 700091, India
Department of Engineering and Technological Studies, University of Kalyani[2]
Kalyani, Nadia-741235, India
(Email: angos.kol@gmail.com)
(Received May 25, 2015; revised and accepted Sept. 6 & Oct. 4, 2015)

Abstract

This paper introduces an enhanced image authentication technique providing greater security with uncompromising visual quality. To augment data security, the authenticating information is diffused into the transformed coefficients of both the levels after a two level Discrete Haar Wavelet Transform. In addition a bit level noise reduction algorithm increases the imperceptibility of the added noise. The extraction algorithm is completely blind and authenticity is verified by regenerating a message digest at the receiving end. The algorithm has been tested against some related attacks and is appropriate in smart card design. Performance comparisons exhibit significant growth over other similar techniques.

Keywords: Copy attack, DWT, image authentication, MD, SSIM

1 Introduction

In present scenario, extensive use of internet facility in daily activities has indulged in certain issues like ownership of digital images, authenticity of ownership claims, copyright, data integrity, fraud detection, self-correcting images etc. So, covert communication is gaining importance and data (Image/Text/Audio/Video) hiding within a cover image has become an important factor.

The issues that are involved in **data hiding** are: 1) Perceptibility: Embedding of secret information in a cover medium with visually acceptable distortion level, 2) Capacity: Change in the volume of secret data with respect to perceptibility and 3) Robustness: Resistance against effort to destroy, remove, or change the embedded data. Various data-hiding schemes are available which emphasize on hiding high amount of secret data within a cover image without destroying the aspect of imperceptibility.

The boom in the internet technology has resulted in more and more digital images getting transmitted over non-secure channels very quickly. So, military, medical and quality control images must be protected against unauthorized manipulation during transmission. Moreover, due to unavoidable interference during transmission original secret data may not reach an intended receiver. This run time problem is taken care of by the process of **image authentication**, i.e. the secret data is hidden within a cover image in an imperceptible manner which can only be deciphered by an intended receiver.

To protect the authenticity of the documents, several approaches including cryptography, watermarking, digital signatures and steganography based on the image content are proposed. The concept of cryptography (encryption and decryption algorithms) was used to protect the secrecy of the message and its communication. But slowly the concept of cryptography became very weak and the secrecy of the existence of the data became a point of concern. So, **watermarking** was introduced to hide digital information in a carrier signal without indulging any special curiosity for the attackers. Digital watermarking facilitates users to handle a secret document legally along with the necessary security. A further refinement, i.e. invisible watermarking confirms that an authorized person is only eligible to extract a watermark utilizing some mathematical calculations. This defines more security and robustness than visible watermarking in the domain of data privacy.

Moreover, digital image steganography [4] based image authentication plays a vital role in preserving and protecting secured documents by showing effective resilience against attempts to corrupt the hidden data. So, every algorithm in this domain must consider certain factors like 1) perceptual transparency, i.e. degradation in the quality of the cover image is insignificant and 2) the volume of payload data [20] and robustness of embedding, i.e. resistance against related attacks namely AWGN, filtering, lossy compression, scaling and cropping.

The key issue, i.e. effectiveness of robust embedding [19], being highly dependent on the pattern of concealment, appropriate domain (Spatial domain [11, 21, 36, 39] or Transform domain [8, 15, 17]) of the cover image and the position of embedding are major concerns. In contrast to spatial domain, choosing spectral domain of an image for embedding proves more credible. Amongst the available transform domain techniques viz. Discrete Cosine transforms (DCT), Discrete Fourier transforms (DFT) [18], Z transforms [16] etc., recently algorithms are focusing more on Discrete Wavelet transforms (DWT) [24, 31] for its two exclusive features namely Multi-resolution analysis (MRA) and rectification of the problem of time - frequency resolution as mentioned in the theoretical aspects of HVS [22].

Some of the existing algorithms are discussed in this context. Embedding of secret messages in high frequency coefficients and utilizing the unchanged low frequency coefficients for improving the image quality was proposed by Chen et al. in "A DWT Based Approach for Image Steganography" [7]. A lossy image compression using wavelet technique was implemented by Raviraj et al. in "The Modified 2D-Haar Wavelet Transformation in Image Compression" [29] where different compression thresholds for the wavelet coefficients was considered to improve the quality of the reconstructed image. Similarly, a lossy image compression method was also proposed by Tamboli et al. in "Image Compression using Haar Wavelet Transform" [32] where different related compression thresholds were applied to minimize the computational requirements. In "Robust Digital Image Steganography within Coefficient Difference on Integer Haar Wavelet Transform" [1], Abu et al. tried to embed the secret message in the difference values of two adjacent 1-level Integer Haar Wavelet transformed coefficients. 1 level of resolution using Discrete Haar Wavelet transform and embedding in all the four coefficients was also proposed by Bhattacharyya et al. in "Data Hiding in Images in Discrete Wavelet Domain Using PMM" [3]. In another algorithm "DWT Based Watermarking Algorithm using Haar Wavelet" [2], Anuradha et al. also suggested embedding into 1 level decomposed coefficients. Vanitha et al. in "A Review on Steganography - Least Significant Bit Algorithm and Discrete Wavelet Transform Algorithm" [34] considered only the LSB position of Discrete Haar Wavelet transformed coefficients to embed the message bits. In another algorithm "Implementation of Image Steganography using 2-Level DWT Technique" [35], Verma et al. tried to insert the secret data in the LL sub-band of the transformed coefficients.

From the above facts, it appears that some of the algorithms were developed using lossy wavelet based compression technique [30], whereas in others either there is a use of only 1- level Haar resolution or there is degradation in the image quality after the embedding of secret data. In the proposed algorithm, a high image compression ratio is maintained using lossless image compression [30] technique. Moreover, the cover image is decomposed to 2-level of resolution and both the levels are simultaneously used for embedding. In contrast to normal LSB position for embedding [33], the proposed algorithm uses the pseudo random nature of embedding position to firmly authenticate the resilience against attempt to corrupt the data by an intruder. Moreover a decent image quality is maintained by successfully decreasing the difference between the cover and stego image in spite of embedding at different dynamic LSB positions.

The theory of Discrete Haar Wavelet transform (DHWT) and Inverse Discrete Haar Wavelet Transform (IDHWT) are discussed in the next section.

2 Concept of DHWT and IDHWT

DHWT considers both low pass and high pass filters to extract the low frequency (approximation) coefficients and high frequency (detail) coefficients of a signal [10] respectively. In $n \times n$ matrix these filters are applied along the rows and then along the columns at every level of decomposition. In the first level the generated sub-bands are

1) LL (low-low frequency) representing approximation band;
2) LH (low - high frequency) representing vertical band;
3) HL (high - low frequency) representing horizontal band;
4) HH (high - high frequency) representing diagonal band.

Each successive decomposition level further, utilizes the LL sub-band of the previous level.

Mathematically, DHWT replaces a sequence of values by its pair wise average $x_{n-1,i}$ and difference $d_{n-1,i}$ values calculated as in Equation (1):

$$\left\{ \begin{array}{l} x_{n-1,i} = (x_{n,2i} + x_{n,2i+1})/2 \\ d_{n-1,i} = (x_{n,2i} - x_{n,2i+1})/2 \end{array} \right\} \quad (1)$$

For example,

1) As consecutive pairs of input sequences having the first element as even index are used for calculating the averages and differences, the total number of elements in each set, i.e. $(x_{n-1,i})$ and $(d_{n-1,i})$ is exactly equal to half the number of elements mentioned in the original sequence.
2) The two sequences $(x_{n-1,i})$ and $(d_{n-1,i})$ are concatenated to generate a new sequence of similar length as that of the input sequence. For example if the original sequence is (10, 13, 25, 26, 29, 21, 7, 15), then the resulting sequence will be $(11.5, 25.5, 25, 11, -1.5, -0.5, 4, -4)$. This sequence can be visualized as 2 halves:
    a. Averages from the original sequence, i.e. a coarser approximation to the original signal is considered as the first half;

$$M_0 = \begin{bmatrix} a(191) & b(187) \\ c(171) & d(151) \end{bmatrix} \xrightarrow{\text{After DHWT}} M_1 = \begin{bmatrix} a'(175) & b'(6) \\ c'(14) & d'(-4) \end{bmatrix} \xrightarrow{\text{After IDHWT}} M_2 = \begin{bmatrix} a(191) & b(187) \\ c(171) & d(151) \end{bmatrix}$$

Figure 1: An example

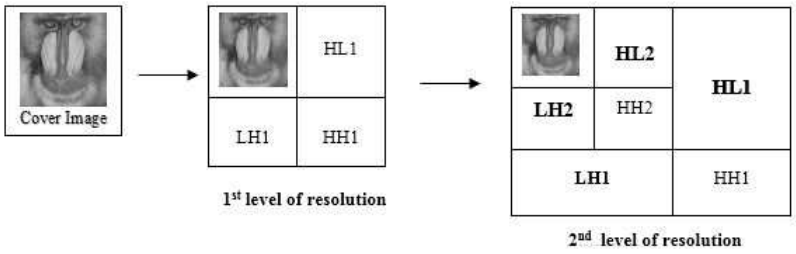

Figure 2: Two-level of resolution using discrete Haar wavelet transform

b. The second half contain the details or approximation errors of the first half.

These transformations do not increase the volume of data. In reverse process, Inverse Discrete Haar Wavelet Transform (IDWT) reconstructs the original sequence by using Equation (2):

$$\left\{ \begin{array}{l} x_{n,2i} = (x_{n-1,i} + d_{n-1,i}) \\ x_{n,2i+1} = (x_{n-1,i} - d_{n-1,i}) \end{array} \right\} \quad (2)$$

In both these equations n represents the total number of elements in a set and i denote a particular position within the set.

In practical application, the implementation of DHWT and IDHWT on a 2 x 2 matrix is explained in Figure 1.

Here M_0 is the original spatial matrix, M_1 is the transformed matrix and M_2 is the reformed spatial matrix.

The transformed coefficients are generated by using

$$\begin{aligned} a' &= ((a+b)+(c+d))/4, \\ b' &= ((a-b)+(c-d))/4, \\ c' &= ((a+b)-(c+d))/4 \\ d' &= ((a-b)-(c-d))/4. \end{aligned}$$

The spatial components are recalculated as

$$\begin{aligned} a &= ((a'+b')+(c'+d')), \\ b &= ((a'-b')+(c'-d')), \\ c &= ((a'+b')-(c'+d')) \\ d &= ((a'-b')-(c'-d')). \end{aligned}$$

Here a, b, c and d are spatial components and a', b', c' and d' are their frequency counterparts.

So, the effectiveness of DHWT refers to:

1) Creation of sub images at multiple resolutions which is similar to a process of HVS [13, 14, 38];

2) The averaging and differencing operations at multiple resolutions is similar to some important image analyzing methods namely Laplacian pyramid method of Burt et al. [5] and the Mumford-Shah theorem [26];

3) Decent correlation between fractal theory [9] and wavelet transforms. The procedures for effective hiding and proper extraction of the secret data are explained in the next section.

3 The Technique

In the embedding technique, the cover image is considered as a set of non-overlapping mask each of size 4×4. 2D DHWT is applied on each of these mask to obtain frequency coefficients and the decomposition is done up to 2 levels. The payload is embedded in the middle frequency bands and three areas of embedding viz.

1) The coefficients of HL2, LH2 and 4 coefficients of HL1;

2) The coefficients of HL2, LH2 and 4 coefficients of LH1;

3) 4 coefficients of LH1 and 4 coefficients of HL1 are proposed. The areas are highlighted in Figure 2.

The formation of stego coefficients can be mathematically expressed as: $s'(m,n) = s(m,n) + \alpha \times w(k)$, where $s(m,n)$ is the host signal, $s'(m,n)$ is the stego signal, $w(k)$ is the payload in form of a distributed sequence and α is the scaling factor to ascertain the strength of the payload signal. The value of α is controlled to maintain a coordination between the imperceptibility and robustness of embedding. The bitwise payload sequence is generated from 1) payload size of 32 bit which represents the combined size of image header and image data, 2) payload message digest (160 bit) and 3) payload data.

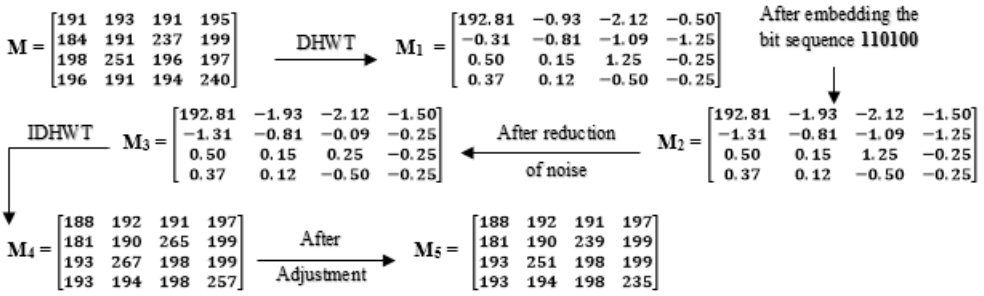

Figure 3: Embedding

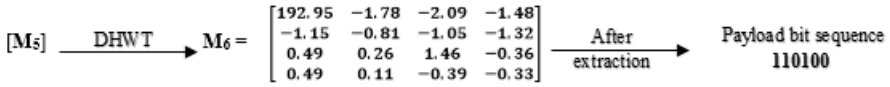

Figure 4: Extraction

An example of the embedding and extraction procedure are shown in Figure 3 and Figure 4 respectively.

In the embedding process, M represents a set of spatial values. On application of DHWT, M1 is generated which contains a set of corresponding frequency values. A bit sequence 110100 is fabricated at pseudo-random generated positions (Subsection 3.2) in some of the selected frequency components and M2 is obtained. The accrued noise due to embedding is minimized (Subsection 3.3) to obtain M3. The technique of IDHWT is applied on M3 to obtain stego values as shown in M4. But it is seen that some of the stego values contradict the image property. An adjustment technique (Subsection 3.4) is implemented to maintain the image property for all the stego values and the final set is M5.

In the extraction process, the embedding bit sequence is extracted from M6 which is obtained by applying DHWT on M5.

The algorithm for embedding is explained in Subsection 3.1. In order to enhance the effectiveness of hiding mechanism, a mathematical function is defined in Subsection 3.2 to generate the pseudo-random embedding positions. Subsection 3.3 defines an initiative taken to achieve high PSNR values in spite of embedding at dynamically variable LSB positions (0-3). Protective measures as explained in Subsection 3.4 are also taken to maintain proper image property of the stego image.

In case of extraction (Subsection 3.5), the embedded bit sequence is extracted by using the mathematical expression $w(k) = (s'(m,n) - s(m,n))/(\alpha \times s(m,n))$ to reconstruct the payload size, message digest and the payload data.

3.1 The Insertion Algorithm

This procedure for embedding is discussed in Algorithm 1.

Algorithm 1 Embedding Technique

Input: An image as cover and a payload (Image/Text/Audio/Encrypted Data).
Output: A stego image.
Steps:

1: A 160 bit (SHA-1) message digest is generated from the payload.
2: Steps 2.1 to 2.7 are repeated to fabricate the payload size (in bytes), generated message digest and the payload entirely into the cover image,

2.1 From the cover image, non-overlapping 4x4 blocks of pixels are read in row major sequence.

2.2 The transform technique is applied on the spatial blocks sequentially to obtain the corresponding frequency blocks.

2.3 Only the integer part of the target frequency coefficients of a block are chosen for embedding.

2.4 The payload bits are scanned one at a time and embedded in pseudo-random positions in each of the selected frequency components.

2.5 An adjustment technique is applied on some of the modified frequency components to reduce the degree of noise due to embedding.

2.6 The stego pixels are obtained by applying Inverse Discrete Wavelet Transform on the selected block.

2.7 Necessary readjustments are applied on an adverse stego block to maintain proper image property.

2.8 The correct spatial block is written back into the output image in the same location.

3: **End**.

3.2 Generation of Pseudo-random Location

This procedure for generating pseudo-random embedding positions is discussed in Algorithm 2.

3.3 Reduction of Embedded Noise

This procedure to reduce noise due to the embedding procedure is discussed in Algorithm 3.

3.4 The Extraction Algorithm

This procedure for extraction is discussed in Algorithm 4.

3.5 Procedure for Retention of Image Property

This procedure to preserve the image property after the embedding technique is discussed in Algorithm 5.

Algorithm 2 Pseudo-Random Position

As input we consider three parameters p, q and r respectively, where p is a 8 bit integer value representing the mean of the current block, q (i.e. 0/1) signifies the last embedded bit of the payload and r (i.e. 0-7) represents the position of q in the current payload data byte. The generated pseudo-random value is a 2 bit integer value.
Steps:

1: Starting from LSB, three bits of r are taken.
2: A sequence qr2r1r0 (e.g. 1011) is formed to generate pos1 = qr2 XOR r1r0.
3: pos1 is regenerated as pos1 = (p1p0 XOR p3p2) XOR ($pos1_1$ $pos1_0$).
4: Let, Q be a buffer to hold maximum N values and prevent successive repetitions of the same random values of pos1.
5: Execute the following statements to get the final value of pos1.
IF (there are empty spaces in Q) then
The present value of pos1 is inserted into Q.
ELSE
The present pos1 is compared with its existing values in Q.
IF (there is a difference at any position) then
The present value of pos1 is treated as the final value.
ELSE
The current value of pos1 is modified as,
IF (q = 0) then
pos1 = (complement of $pos1_0$) $pos1_1$
ELSE
pos1 = $pos1_0$ (complement of $pos1_1$)
This value of pos1 in inserted into Q and returned as the final position.
6: **End**.

Algorithm 3 Reduction of noise

The magnitude of the stego component may differ or remain same as the spatial value. If s = e (b, t) then the magnitude of the adjustment factor n is defined as n = |s - b|. The adjustment on s is done based on:
Steps:

1: If n = 0, no adjustment is done.
2: if n > 0, then adjustment is done with respect to the embedding position of the payload bit. The bits of the binary representation of s are altered (0 to 1 / 1 to 0) on the right (i.e. towards LSB) and/or left (i.e. towards MSB).
Note: s is the stego frequency component, e () is the embedding function, b is the bit to be embedded and t is the position of embedding.

Algorithm 4 Extraction Technique

Input: A stego image.
Output: The extracted payload (Image/ Text/ Audio/ Encrypted Data).
Steps:

1: The fabricated bits are to be extracted to reform the required information.
2: Steps 2.1 to 2.5 are repeated to reform the payload.
2.1 From the stego image, non- overlapping 4x4 blocks of pixels are read in row major sequence.
2.2 Two Dimensional Discrete Haar wavelet Transform is applied on the spatial blocks at a time to obtain the frequency blocks.
2.3 The integer part of the target frequency values is chosen and the pseudo-random positions are generated for extraction.
2.4 The embedded bits are extracted from the selected areas.
2.5 The extracted bits are properly arranged to form the payload size, message digest and the payload itself.
3: The 160 bit message digest (SHA-1) is generated from the extracted payload.
4: The generated and extracted message digests are compared to check the authenticity of the received payload.
5: **End**.

Algorithm 5 Preservation of image property

In a stego block, some pixel values may contradict the image property. For rectification, specific adjustments are made on the spatial pixel values and the embedding algorithm is repeated again on that block. By experimentation on a number of gray scale images a threshold value T has been derived for the proposed algorithm to control the adjustment procedure. The possible adjustments are:

1: When all the spatial values in a block are in the range [0, T] only and a negative stego pixel value generates, then the highest difference, i.e. [0- (highest -ve pixel value)] is added to all the spatial values.
2: When all the spatial values in a block are in the range [(255-T), 255] only and there is a generation of a stego pixel value above 255, then the highest difference [(highest + ve pixel value) - 255] is subtracted from all the spatial values.
3: When all the spatial values in a block are in the range [(0, T), ((255-T), 255)] and there is a generation of both negative stego pixel value and stego pixel value above 255. The two types of differences are calculated as 1) A = [0- (highest -ve pixel value)] and 2) B = [(highest + ve pixel value) - 255]. The actual difference is selected as diff = max (A, B). The value (2 x diff) is subtracted from all the spatial values in the range [((255-T), 255)] and diff is added to all the spatial values in the range [0, T].
4: When all the spatial values in a block are in the range [(0, T), ((255-T), 255)] and there is a generation of both negative stego pixel value and stego pixel value above 255. The differences are calculated as in case 3.The actual difference is selected as diff = A or B. The value (2 x diff) is subtracted from all the spatial values in the range [((255-T), 255)] and diff is added to all the spatial values in the range [0, T].
5: When all the spatial values in a block are in the range [0, 255] and there is a generation of both negative stego pixel value and stego pixel value above 255. The differences are calculated as in case 3.The actual difference is selected as diff = A or B. The value (2 x diff) is subtracted from all the spatial values in the range [((255-T), 255)], diff is added to all the spatial values in the range [0, T] and the mid-range, i.e. [(T+1), ((255-T) - 1)] values remain unchanged.

4 Experiment and Results

The algorithm has been experimented on a number of gray scale images in a system with the following hardware configuration: 4 GB of main memory, processor of at least 1 GHz clock speed, 1 GB of graphics memory and 4 GB of free disk space. Various fidelity tests are performed on a number of gray scale images to analyse the robustness of embedding, i.e. to check whether there is any perceptual distortion in the cover image after the embedding of secret data. The imperceptibility is measured in terms of Mean Squared Error (MSE) [28], Peak Signal to Noise Ratio (PSNR) [28], Image Fidelity (IF) and Structural Similarity Index Metric (SSIM) [37]. The quantifiers are defined as follows:

1) Mean Square Error (MSE): The average energy of the error difference between the test and the reference signal is computed using Equation (3)

$$MSE = \frac{1}{MN}\sum_{y=0}^{M-1}\sum_{x=0}^{N-1}[I(x,y) - I'(x,y)]^2 \quad (3)$$

Here I(x, y) and I'(x, y) are the pixel values in the cover and the stego image and M, N are the horizontal and vertical pixel dimensions of the cover image.

2) Peak Signal to Noise Ratio (PSNR):The ratio of the maximum intensity of a signal against the intensity of the corrupting noise that affects the fidelity aspect is calculated by using Equation (4)

$$PSNR = 20log_{10}\frac{255}{\sqrt{MSE}} \quad (4)$$

where the constant value 255 signifies the maximum intensity of a pixel having a colour depth of 8 bits.

3) Image Fidelity (IF): The measurement of the degradation level of a perceived image w.r.t a perfect image is done with the help of Equation (5)

$$IF = 1 - \frac{\sum_{y=0}^{M-1}\sum_{x=0}^{N-1}[I(x,y) - I'(x,y)]^2}{\sum_{y=0}^{M-1}\sum_{x=0}^{N-1}[I(x,y)]^2} \quad (5)$$

4) Structural Similarity Index Metric (SSIM): This procedure is sensitive to distortions that disintegrate the natural spatial correlation of an image and considered as the best possible method to evaluate image quality. It is evaluated as a product of luminance comparison function l (f, g), contrast comparison function c(f, g) and structural comparison function s(f, g) as shown in Equation (6).

$$SSIM(f,g) = l(f,g).c(f,g).s(f,g) \quad (6)$$

where,

$$\begin{cases} l(f,g) = \dfrac{2\mu_f\mu_g + C_1}{\mu_f^2 + \mu_g^2 + C_1} \\ c(f,g) = \dfrac{2\sigma_f\sigma_g + C_2}{\sigma_f^2 + \sigma_g^2 + C_2} \\ s(f,g) = \dfrac{\sigma_{fg} + C_3}{\sigma_f\sigma_g + C_3} \end{cases} \quad (7)$$

The first term, i.e. luminance comparison function used in Equation (7) measures the closeness of mean luminance (μ_f and μ_g) of the cover and stego images. The second term, i.e. contrast comparison function

measures the closeness of the contrast (measured by the standard deviation σ_f and σ_g) of the two images. The third term i.e. the structure comparison function measures the correlation coefficient between the two images f and g. Note that σ_{fg} is the covariance between f and g. The positive values of the SSIM index fall between [0,1] where 0 signifies no correlation between images and 1 means $f = g$. The positive constants C_1, C_2 and C_3 are used to avoid a null denominator.

The comparison between the three areas of embedding in terms of PSNR (in dB), IF and SSIM are shown in Table 1, Table 2 and Table 3 respectively. In case of area 1 and area 2 the size of the payload is 110x110 and in case of area 3 the size of the payload is 120x120. The size of each of the cover images is 512x512 for all the cases.

Table 1: Analysis of PSNR

Cover Images	Payload	PSNR(in dB)		
		Area I	Area II	Area III
Monalisa	Earth	37.19	37.16	37.22
Lenna		36.17	36.14	36.29
Baboon		37.40	37.42	37.49
Oakland		37.09	37.16	37.25
Woodlad		36.77	36.86	37.10
Peppers		36.10	36.12	36.40
Tiffany		34.15	34.10	34.63
Airplane		35.10	34.89	35.16
Sailboat		35.39	35.46	36.55
Average		**36.15**	**36.14**	**36.45**

Table 2: Analysis of IF

Cover Images	Payload	IF		
		Area I	Area II	Area III
Monalisa	Earth	0.9954	0.9958	0.9959
Lenna		0.9340	0.9334	0.9356
Baboon		0.9933	0.9938	0.9938
Oakland		0.9939	0.9947	0.9950
Woodlad		0.9984	0.9982	0.9983
Peppers		0.9859	0.9853	0.9864
Tiffany		0.9918	0.9921	0.9920
Airplane		0.9835	0.9836	0.9843
Sailboat		0.9959	0.9963	0.9964
Average		**0.9857**	**0.9859**	**0.9864**

It can be considered that the degradation level of a stego image is quite acceptable if the PSNR value is greater than 35 dB, i.e. the payload is almost invisible to HVS. Table 1 suggests that the proposed algorithm is quite successful in achieving a decent average PSNR value, i.e. 36.24 dB in spite of hiding quite a large volume of secret data simultaneously in both the levels of resolution. Moreover from Table 2 and Table 3 the average values of IF and SSIM, i.e. 0.9860 and 0.9948 respectively, proves that the stego image more or less resembles the cover image. Also, visual analysis of the testing images shows imperceptible distinction between the cover and the stego images as shown for the three areas of embedding in Figure 5, Figure 6 and Figure 7 respectively.

Table 3: Analysis of SSIM

Cover Images	Payload	SSIM		
		Area I	Area II	Area III
Monalisa	Earth	0.9990	0.9988	0.9988
Lenna		0.9963	0.9961	0.9959
Baboon		0.9959	0.9962	0.9964
Oakland		0.9913	0.9915	0.9915
Woodlad		0.9954	0.9960	0.9960
Peppers		0.9973	0.9972	0.9971
Tiffany		0.9851	0.9850	0.9844
Airplane		0.9949	0.9948	0.9948
Sailboat		0.9977	0.9985	0.9985
Average		**0.9947**	**0.9949**	**0.9948**

In addition to this, our proposed embedding algorithm can be implemented in all the middle frequency bands, irrespective of whether they are present in a combination of 1-level and 2-level of resolution or only in 2-level of resolution and the average value of PSNR suggest robust embedding. Moreover, performance comparison is also done with other similar existing algorithms as shown in Table 4.

Table 4: Comparative analysis of PSNR

No.	**Algorithm**	**Level of Resolution**	**Avg. PSNR (in dB)**
A	[3]	1	34.60
B	[27]	1	38.52
C	[2]	2	39.62
D	[12]	2	26.30
E	[6]	2	33.08
F	[23]	2	36.04
G	Proposed	2	36.44
H	Proposed	2	43.22
I	Proposed	2	45.73

From the above table it shows that as compared to 1-level resolution in A, with similar embedding capacity our proposed algorithm even with 2-level of resolution in G generates an enhanced PSNR value of 36.44 dB. Similarly, considering the same embedding capacity as in B, our algorithm with 2-level of resolution in I shows an increased PSNR value of 45.73 dB as compared to 38.52 dB

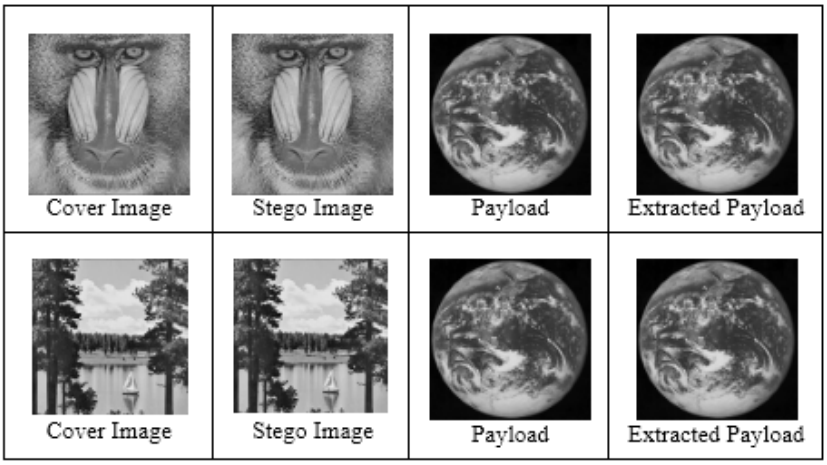

Figure 5: Embedding in Area I

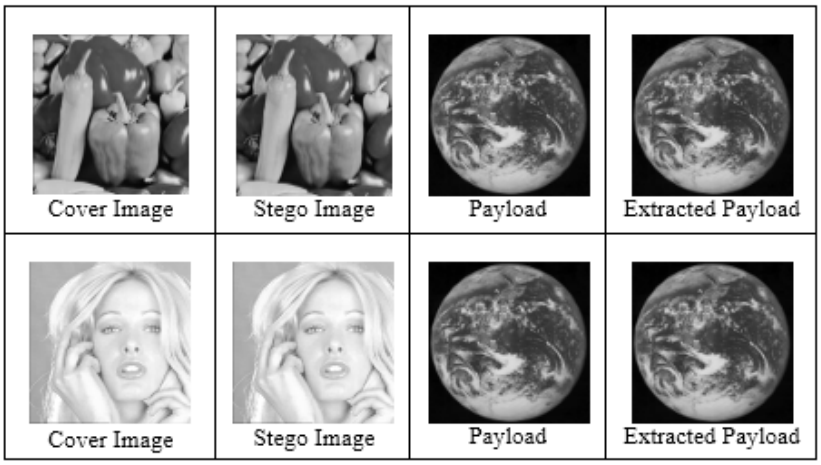

Figure 6: Embedding in Area II

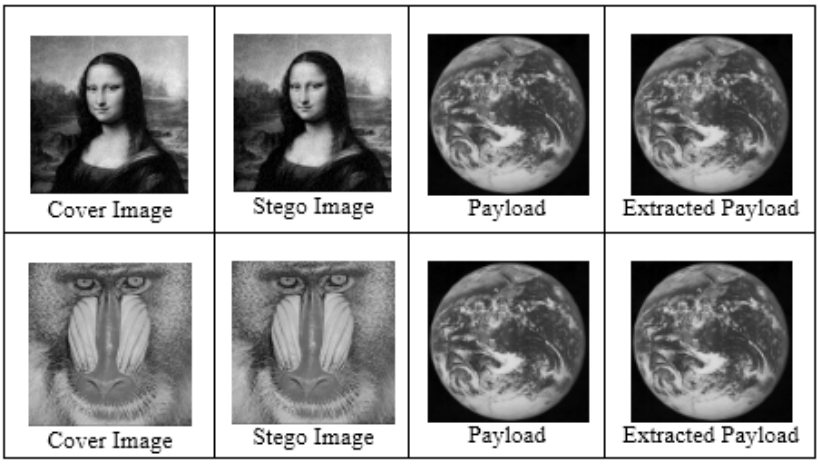

Figure 7: Embedding in Area III

Figure 8: Visual analysis of cover and stego images

in B even with 1-level of resolution. In addition to this, considering 2-level of resolution and similar embedding capacity our algorithm in H shows an escalation in PSNR value, i.e. 43.22 dB when compared with some similar algorithms like C, D, E and F having PSNR values of 39.62 dB, 26.30 dB, 33.08 dB and 36.04 dB respectively.

5 Resistance to Certain Attacks

5.1 Visual Attack

Initiative is imparted to resist visual attack by eliminating certain issues related to secret message like 1) embedding in a sequential order and 2) length is less than the maximum size of the bit plane. Figure 8 shows the visual interpretation of the magnified version of a source and the stego image of the three areas and it may be inferred that the algorithm can resist visual attack considerably.

5.2 Statistical Attack

This is similar to visual attack. The assumption is that the least significant bit of a cover image is random and may be replaced by a secret message is not necessarily correct. The basic concept is to compare between the frequency distribution and the theoretically expected distribution of a potential cover image. If the statistical profile of the new data does not with the standard data, then it probably contains a hidden message. In Figure 9 there is a detailed graphical comparison between the cover and stego signals with respect to the pixel intensity value vs. pixel number. It shows that the graph for stego image mostly overlaps the graph for cover image. Due to efficient adjustment of noise in the stego image, no noticeable changes occur after the concealment of the payload in the carrier image. So we may infer that the proposed algorithm is significantly robust in the domain of data authentication and different areas of comparison as shown in sub figures strongly establish the fact. Moreover as the cover and stego images are more or less identical and statistically similar, an unintended user will have confusion in implementing statistical attack.

5.3 Copy Attack

The objective is to copy a payload from one carrier signal to another. It is performed in two steps: 1) An estimation of the embedded payload is made from the stego image and 2) The estimated payload is copied from the stego image to a carrier signal to obtain a separate target stego image. Our proposed algorithm uses a self-defined mathematical pseudorandom function to establish a link between the payload and the cover image. As the function is only known to the authorized sender and receiver, the link can only be verified by an intended receiver during the extraction of the payload. In addition to this, the pseudorandom function also helps to make the payload a function of the original cover image which may cause a problem in terms of the marked target cover image. The elimination of copy attack also helps to resist protocol attack.

6 Conclusions

Social Implication: Personal identification and authentication demand the necessity of security, protection and access restriction which may be achieved using a biometric authentication system. The characteristic of biometric system is unique and cannot be lost or forgotten and the components used by biometric systems include fingerprints, hand geometry, iris, retina, facer, hand, vein etc.

To access sensitive and restricted areas in an office, we like to propose the facility of smart card for an individual's identity. A chip will be embossed on the identity card and the information content in the chip will be original template, entire biometric sensor, microprocessor and memory. This chip will function as per the operations of System-on-Card (SOC).

The card is prepared using two images namely: 1) Digital photo as cover image and 2) Image of his or hers retina as payload. These two images are fed as input to the proposed embedding algorithm to produce a stego image. The stego image is written into the memory of the chip and the identity card is prepared to be delivered to the individual. At the entry

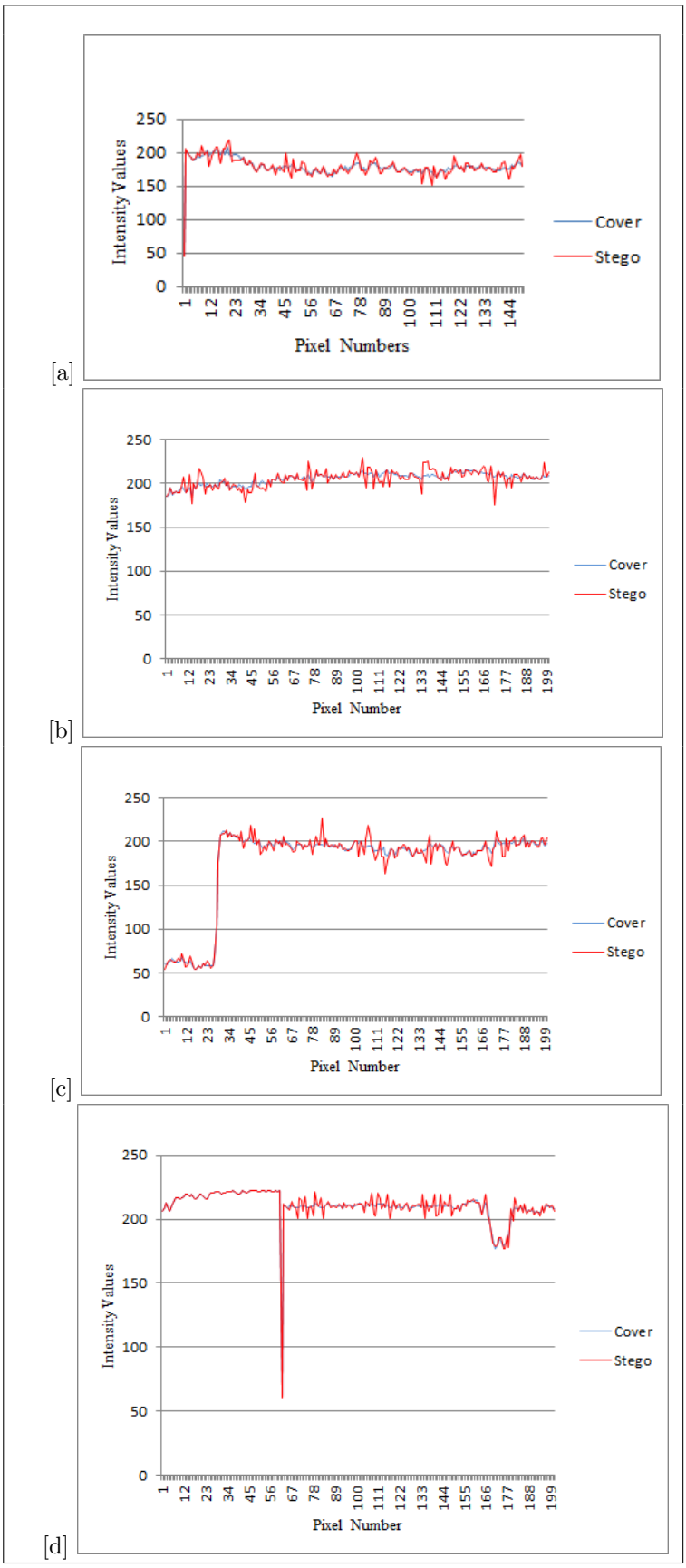

Figure 9: Statistical analysis of source and stego image pixels

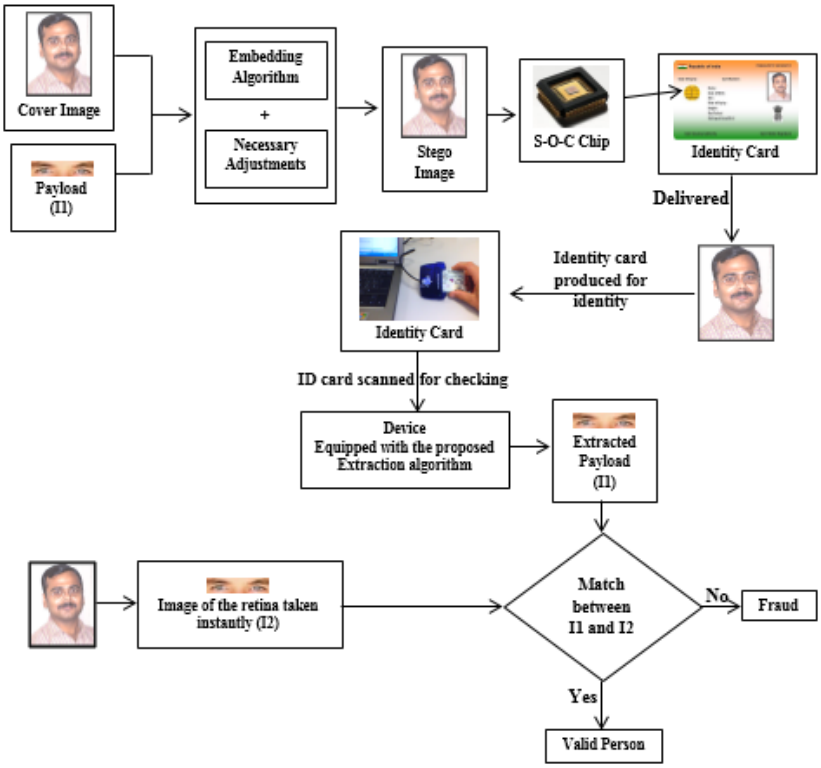

Figure 10: Authentication in smart card

point where the card is required to prove an individual's identity, the image of the retina of the individual is captured instantly. The embedded stego image is extracted by scanning the chip on the identity card. The payload i.e. original image of retina is extracted by using the extraction algorithm. The captured and the extracted images of the retina are matched to validate an individual's identity. It is pictorially represented in Figure 10 as.

Conclusions: This paper proposes a secured data authentication algorithm for the protection of copyright information. Embedding capacity, level of decomposition and the areas chosen for embedding are quite better than many existing methods. The PSNR values computed for the three proposed areas show effective results and the average values of IF and SSIM ensure the similarity between the cover image and the stego image. The extraction of the original payload bits is also difficult as they are not embedded directly into a fixed LSB position in the spatial domain of a cover image. In addition to this, the payload can be extracted [25] without the availability of the original cover image and the algorithm proves effective against some related attacks.

Future Studies and Recommendations: The proposed algorithm can be implemented using other wavelet frequency methods. Moreover color cover image can also be taken into consideration with embedding in other frequency bands.

Acknowledgments

The authors express their deep sense of gratitude to the faculty members of the Dept. of Engineering and Technological Studies, University of Kalyani, West Bengal, India, where the work has been carried out.The work has been financially supported by DST, PURSE.

References

[1] N. A. Abu, P. W. Adi, and O. Mohd, "Robust digital image steganography within coefficient difference on integer Haar wavelet transform," *International Journal of Video and Image Processing and Network Security*, vol. 14, no. 2, pp. 1–8, 2014.

[2] Anuradha and R. P. Singh, "Dwt based watermarking algorithm using Haar wavelet," *International Journal of Electronics and Computer Science Engineering*, vol. 1, no. 1, pp. 1–6, 2012.

[3] S. Bhattacharyya and G. Sanyal, "Data hiding in images in discrete wavelet domain using pmm," *Academic Journal, World Academy of Science, Engineering and Technology*, vol. 44, pp. 376–384, 2010.

[4] M. Borda and I. Nafornita, "Digital watermarking - principles and applications," in *Proceedings of*

The International Conference on Communications, pp. 41–54, 2004.

[5] P. A. Burt and E. H. Adelson, "The laplacian pyramid as a compact image code," *IEEE Transactions on Communications*, vol. 31, pp. 532–540, 1983.

[6] A. Chawla and P. Shukla, "A modified secure digital image steganography based on DWT using matrix rotation method," *International Journal of Computer Science and Communication Engineering*, vol. 2, no. 2, pp. 20–25, 2013.

[7] P. Y. Chen and H. J. Lin, "A DWT based approach for image steganography," *International Journal of Applied Science and Engineering*, vol. 4, no. 3, pp. 275–290, 2006.

[8] Q. Cheng and T. S. Huang, "Robust optimum detection of transform domain multiplicative watermarks," *IEEE Transactions on Signal Processing*, vol. 51, no. 4, pp. 906–923, 2003.

[9] G. M. Davis, "A wavelet-based analysis of fractal image compression," *IEEE Transactions on Image Processing*, vol. 7, pp. 213–245, 1998.

[10] G. M. Davis and A. Nosratinia, "Wavelet-based image coding: An overview," in *Applied and Computational Control, Signals, and Circuits*, pp. 369–434, 1999.

[11] S. Dey, A. Abraham, and S. Sanyal, "An LSB data hiding technique using prime numbers," in *Third IEEE International Symposium on Information Assurance and Security*, pp. 101–106, 2007.

[12] Y. Dinesh and A. P. Ramesh, "Efficient capacity image steganography by using wavelets," *International Journal of Engineering Research and Applications*, vol. 1, no. 1, pp. 251–259, 2012.

[13] D. J. Field, "Wavelets, vision and the statistics of natural scenes," *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, vol. 357, pp. 2527–2542, 1999.

[14] D. J. Field and N. Brady, "Wavelets, blur and the sources of variability in the amplitude spectra of natural scenes," *Vision Research*, vol. 37, pp. 3367–3383, 1997.

[15] V. Fotopoulos and A. N. Skodras, "A novel approach on transform domain watermarking against geometrical deformations," in *Proceedings of IEEE workshop on Signal Processing Systems Design and Implementation*, pp. 403–406, Nov. 2005.

[16] N. Ghoshal, S. Chowdhury, and J. K. Mandal., "A steganographic scheme for colour image authentication using z-transform (SSCIAZ)," in *Proceedings of The International Conference on Information System Design and Intelligent Applications*, pp. 209–216, Jan. 2012.

[17] N. Ghoshal and J. K. Mandal, "Controlled data hiding technique for color image authentication in frequency domain," in *Proceedings of The Second International Conference on Emerging Applications of Information Technology (EAIT'11)*, pp. 284–287, Feb. 2011.

[18] N. Ghoshal and J. K. Mandal, "Discrete fourier transform based multimedia color image authentication for wireless communication (dftmciawc)," in *Proceedings of The Second International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology*, pp. 1–5, 2011.

[19] N. Ghoshal, J. K. Mandal, and A. Khamrui, "A framework for block based image authentication," in *Proceedings of The Fourth IEEE International Conference on Industrial and Information Systems (ICIIS'09)*, pp. 343–348, Dec. 2009.

[20] N. Ghoshal, J. K. Mandal, A. Sarkar, and D. Chakrabarty, "Image authentication by hiding large volume of data and secure message transmission technique using mask," in *Proceedings of The IEEE International Advanced Computing Conference (IACC'09)*, pp. 3177–3182, Mar. 2009.

[21] M. Juneja and P. S. Sandhu, "Improved LSB based steganography techniques for color images in spatial domain," *International Journal of Network Security*, vol. 16, no. 6, pp. 452–462, 2014.

[22] S. A. Kasmani and A. R. Naghsh-Nilchi, "A new robust digital image watermarking technique based on joint DWT DCT transformation," in *Proceedings of The Third IEEE International Conference on Convergence and Hybrid Information Technology (ICCIT'08)*, pp. 539–544, Busan, Korea, 2008.

[23] L. Li, H. H. Xu, C. C. Chang, and Y. Y. Ma, "A novel image watermarking in redistributed invariant wavelet domain," *The Journal of Systems and Software*, vol. 84, no. 6, pp. 923–929, 2011.

[24] G. Manikandan, M. Kamarasan, and N. Sairam, "A new approach for secure data transfer based on wavelet transform," *International Journal of Network Security*, vol. 15, no. 2, pp. 106–112, 2013.

[25] Q. Mao, C. C. Chang, and T. F. Chung, "A reversible steganography suitable for embedding small amounts of data," *International Journal of Network Security*, vol. 16, no. 4, pp. 295–303, 2014.

[26] D. Mumford and J. Shah, "Boundary detection by minimizing functionals," in *Proceedings of The IEEE Conference on Computer Vision and Pattern Recognition (CVPR'88)*, pp. 19–43, 1988.

[27] P. Patil and D. S. Bormanel, "DWT based invisible watermarking technique for digital images," *International Journal of Engineering and Advanced Technology*, vol. 2, no. 4, pp. 603–605, 2013.

[28] S. Poobal and G. Ravindran, "The performance of fractal image compression on different imaging modalities using objective quality measures," *International Journal of Engineering Science and Technology*, vol. 2, no. 1, pp. 239–246, 2011.

[29] P. Raviraj and M. Y. Sanavullah, "The modified 2d-Haar wavelet transformation in image compression," *Middle-East Journal of Scientific Research*, vol. 2, no. 2, pp. 73–78, 2007.

[30] A. Said and W. A. Pearman, "An image multiresolution representation for lossless and lossy compression," *IEEE Transactions on Image Processing*, vol. 5, no. 9, pp. 1303–1310, 1996.

[31] S. S. Sujatha and M. Mohamed Sathik, "A novel DWT based blind watermarking for image authentication," *International Journal of Network Security*, vol. 14, no. 4, pp. 223–228, 2012.

[32] S. S. Tamboli and V. R. Udupi, "Image compression using Haar wavelet transform," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 2, no. 8, pp. 3166–3170, 2013.

[33] Y. Y. Tsai, J. T. Chen, and C. S. Chan, "Exploring LSB substitution and pixel-value differencing for block-based adaptive data hiding," *International Journal of Network Security*, vol. 16, no. 5, pp. 363–368, 2014.

[34] T. Vanitha, A. D. Souza, B. Rashmi, and S. Dsouza, "A review on steganography - least significant bit algorithm and discrete wavelet transform algorithm," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 2, no. 5, pp. 89–95, 2014.

[35] A. Verma, R. Nolkha, A. Singh, and G. Jaiswal, "Implementation of image steganography using 2-level DWT technique," *International Journal of Computer Science and Business Informatics*, vol. 1, no. 1, pp. 1–14, 2013.

[36] S. M. C. Vigila and K. Muneeswaran, "Hiding of confidential data in spatial domain images using image interpolation," *International Journal of Network Security*, vol. 17, no. 6, pp. 722–727, 2015.

[37] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," *IEEE Transactions on Image Processing*, vol. 13, no. 4, pp. 600–612, 2004.

[38] A. B. Watson, "Efficiency of a model human image code," *Journal of the Optical Society of America*, vol. 4, no. 12, pp. 2401–2417, 1987.

[39] C. Yang, C. Weng, S. Wang, and H. Sun, "Adaptive data hiding in edge areas of images with spatial LSB domain systems," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 3, pp. 488–497, 2008.

Anirban Goswami is currently working as Asstt. Professor in Techno India (An Engineering College under West Bengal University of Technology), Kolkata, West Bengal, India and pursuing his research work in the Department of Engineering and Technological Studies, University of Kalyani, West Bengal, India. He has 15 years of teaching experience and had contributed in more than 10 graduate level projects. He has 7 international conference and 2 international journal publications.

Dr. Nabin Ghoshal is a Professor in the Department of Engineering and Technological Studies, University of Kalyani, West Bengal, India. He received a Bachelor degree in Mathematics from the University of Calcutta in 1994. He got Master degree in Computer Applications from the University of North Bengal in 1998 and also obtained M. Tech. degree in Computer Science and Engineering from the University of Kalyani in 2005 respectively. He received his Ph. D. degree in Computer Science and Engineering from the University of Kalyani in 2011. Dr.Ghoshal is committed to professional teaching and research work for many years, accumulated rich experience in teaching and research on topics namely Steganography, Watermarking, Visual Cryptography, Security, Visual Cryptography through Steganography, Copyright protection and Legal Document Authentication (Audio/ Video). He has 41 research papers in various international journals and national and international conferences. He wrote a book entitled "Steganographic Techniques and Application in Document Authentication".