An Image Authentication Technique by Handwritten Signature Verification using DWT and ANN

Tanmay Bhattacharya
Asst. Professor Dept. of IT,
JIS College of Engineering,
Kalyani, West Bengal, India

Sirshendu Hore
Asst. Professor Dept. of CSE,
Hooghly Engineering &
Technology College, Hooghly,
West Bengal, India

S. R. Bhadra Chaudhuri
Professor, Dept of E&TCE,
Bengal Engineering and
Science University, Shibpur,
West Bengal, India

ABSTRACT
Image authentication is important in content delivery to preserve originality as well as integrity of data. Using handwritten signature we can authenticate a person accurately. This paper proposes an efficient image authentication technique by hiding handwritten signature image in selected DWT sub-band of the image. At the receiver end signature image is extracted and verified with template signature using Artificial Neural Network and hence image authentication is achieved.

General Terms
Image Authentication, Handwritten Signature verification

Keywords
DWT, Aspect Ratio, Cross & End points, Confusion Matrix, Center of Gravity, ANN

1. INTRODUCTION
Image authentication verifies the originality of an image by detecting malicious manipulations there by prevents image originality Development of robust image authentication techniques becomes an important issue. Two methods have been suggested for achieving the authenticity of digital images: having a digital camera sign the image using a digital signature [1], or embedding a secret code in the image [2].

Data hiding [4, 5, 6] is the process of hiding data within a host message and extracting it at its destination. Anyone else viewing the message will fail to know it contains secret/encrypted data.
LSB [8] insertion is a very simple and common approach to embedding information in an image in special domain. The limitation of this approach is vulnerable to every slight image manipulation. Converting image from one format to another format and back could destroy information secret in LSBs. Stego-images can be easily detected by statistical analysis like histogram analysis. This technique involves replacing N least significant bit of each pixel of a container image with the data of a secret message. Stego-image gets destroyed as N increases. In frequency domain data can be secret by using Discrete Cosine Transformation (DCT) [11, 14]. Main limitation of this approach is blocking artifact. Grouping the pixel into 8x8 blocks and transforming the pixel blocks into 64 DCT co-efficient each. A modification of a single DCT co-efficient will affect all 64 image pixels in that block. Discrete Wavelet Transformation (DWT) approach [12, 13 & 16].is one of the modern approaches used for steganography. In this approach the imperceptibility and distortion of the Stego image is acceptable and it is resistant to several attacks.

Biometrics, described as the science of recognizing an individual based on her physiological or behavioral traits, is beginning to gain acceptance as a legitimate method for determining an individual's identity. Different biometrics such as fingerprints, hand geometry, iris, retina, face, hand vein, Face, signature, voice, etc. to either validate or determine an identity.[10]

Handwritten signature is widely used as a means of personal Authentication [3, 9 & 15]. Authentication can be performed either Offline or Online based on the application [7]. Online systems use dynamic information of a signature captured at the time signature is made. Offline systems work on the scanned image of a signature.The features that are used mostly are Baseline Slant Angle, Aspect Ratio, Normalized Area, Center of Gravity, number of edge points, number of cross points, and the Slope of the line joining the Canters of Gravity of two halves of a signature image.

Discrete Wavelet Transformation

The wavelet transform describes a multi-resolution decomposition process in terms of expansion of an Image into a set of wavelet basis function. The wavelet transform describes a multi-resolution decomposition process in terms of expansion of an Image onto a set of wavelet basis functions. Discrete Wavelet Transformation has its own excellent space frequency localization properly. Applying DWT in 2D images corresponds to 2D filter image processing in each dimension. The input image is divided into 4 non-overlapping multi-resolution sub-bands by the filters, namely (LL1), (LH1), (HL1) and (HH1). The sub-band (LL1) is processed further to obtain the next coarser scale of wavelet coefficients, until some final scale "N" is reached. When "N" is reached, we'll have 3N+1 sub-bands consisting of the multi-resolution sub-bands (LLN) and (LHX), (HLX) and (HHX) where "X" ranges from 1 until "N". Generally most of the Image energy is stored in these sub-bands.

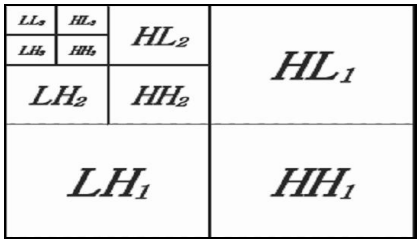


Fig 1: Three phase decomposition using DWT

The Forward Discrete Wavelet Transform is very suitable to identify the areas in the Host image where a stego image can be embedded effectively due to its excellent space-frequency localization properties. In particular, this property allows the exploitation of the masking effect of the human visual system such that if a DWT co-efficient is modified, it modifies only the region corresponding to that coefficient.

The embedding secret image in the lower frequency sub-bands (LLX) may degrade the image significantly, as generally most of the Image energy is stored in these sub-bands. Embedding in the low-frequency sub-bands, however, could increase robustness significantly. In contrast, the edges and textures of the image and the human eye are not generally sensitive to changes in the high frequency sub-bands (HHX). This allows the stego-image to be embedded without being perceived by the human eye. The compromise adopted by many DWT based algorithms, to achieve acceptable performance of imperceptibility and robustness, is to embed the secret image in the middle frequency sub-bands (LHX) or (HLX) and (HHX). The Haar wavelet is also the simplest possible wavelet. Haar wavelet is not continuous, and therefore not differentiable. This property can, however, be an advantage for the analysis of signals with sudden transitions.

Code Division Multiple Access (CDMA) Spread-Spectrum Technique

Spread-spectrum technique can be described as a method in which a signal generated in a particular bandwidth when deliberately spread in the frequency domain, results in a signal with a wider bandwidth. If distortion is introduced in this signal by some process such as noise or filtering which damages only certain bands of frequencies, the message will be still in a recoverable state. In spread spectrum communications, the signal energy inserted into any one frequency is too undersized to create a visible artefact and the secret image is scattered over a wide range of frequencies, that it becomes robust against many common signal distortions. Because of its good correlation properties, noise like characteristics, easier to generate and resistance to interference, Pseudo noise sequences are used for Steganography.

ANN

Artificial neural networks are constituted of artificial neurons. An ANN is a system consisting of processing elements (PE) with links between them. A certain arrangement of the PEs and links produce a certain ANN model, suitable for certain tasks [14]. A Multi-Layer-Perception (MLP) is a kind of feed-forward ANN model consisting of three adjacent layers; the input, hidden and output layers. Each layer has several PEs. Figure 2 illustrates the structure of a MLP

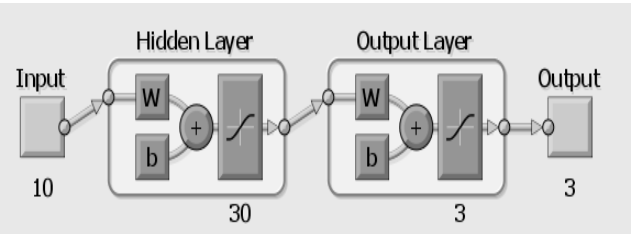


Fig 2: A schematic diagram of a MLP neural network

2. PROPOSED ALGORITHM

2.1 Biometric Signature Template Generation

a. Image Acquisition
b. Enhancement of the Image
c. Feature extraction
d. Training with different sample images using ANN
e. Template Signature is obtained

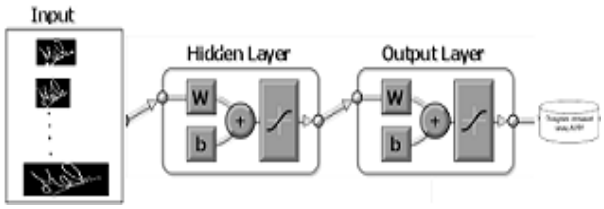


Fig 3: Image Template Generation Process

2.2 Handwritten Signature Hiding

a. Host image is decomposed into four sub bands (LL, LH, HL and HH) using DWT.

b. HH band is further decomposed using DWT.

c. Handwritten Signature image is converted into 1D Vector.

d. A pseudo random 2D sequence is generated by the session based key.

e. HH2 sub band of the Host image is modified using corresponding PN sequence depending upon the content of the corresponding 1D image vector to be embedded.

f. Four sub bands including modified sub bands are combined to generate the Stego image using IDWT twice.

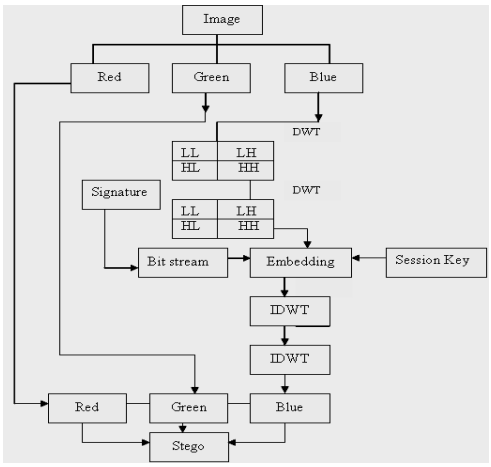


Fig 4: Handwritten Signature Hiding Process

2.3 Handwritten Signature Extraction

a. Session key and Size of the signature image are sent to the intended receiver via a secret communication channel.
b. Signature can recovered from the Stego image using Correlation function and knowing the size of the signature image.
c. Extracted Signature Image is filtered to remove the unwanted signal.

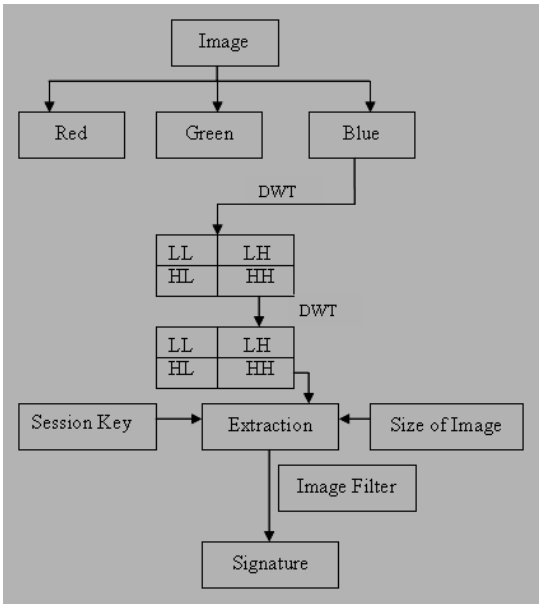


Fig 5: Handwritten Signature Extraction Process

2.4 Recovered Handwritten Signature Authentication

a. Enhancement of the Image
b. Feature extraction
c. Compare with the Template Image, if the match scoring is with in the threshold, signature image is authenticated

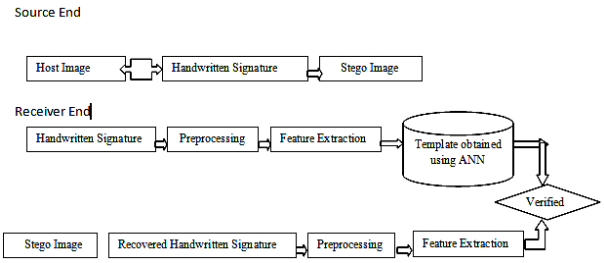


Fig 6: Schematic diagram: The sequence of Handwritten Signature authentication process

3. EXPLANATION OF THE ALGORITHM

3.1 Biometric Signature Template Generation

After obtaining the signature image various preprocessing operation are performed to remove the noise caused by the scanner. The image is then cropped, to the bounding rectangle of the signature. Finally transform the signature image from color to grayscale, and to black and white. From the enhanced signature image we calculate the center of gravity, center of mass, no of cross & edge points, slant angel ,Number of black pixel, Image area and the aspect ratio .stored those value in the Input matrix.

The Center of Gravity is the 2-tuple (X,Y) given by,

$$X = j=0\sum N\text{-}1\ PV(j)*j/\Delta$$

$$Y = i=0\sum M\text{-}1\ PH(i)*i/\Delta$$

Where, PV and PH are the vertical and horizontal projections

The edge point is a point that has only one 8-neighbor. In order to extract the edge points in a given signature, we used a 3×3 structuring element with all coefficients equal to 1.

Cross point is a point that has at least three 8-neighbors. The structuring element that was used to extract edge points, was also used to extract the cross points in a signature.

To determine the slant angle the ratio of the maximum horizontal projection to the width of the projection is maximized over a range of values of angle of rotation θ.

$$PH(i) = j=0\Sigma N\text{-}1\ IT(i,j)$$

$$\rho(\theta) = H(\theta)/W(\theta)\ -\theta 1<\theta<\theta 2$$

$$H(\theta) = Max(\ PH(i))$$

$$W(\theta) = \text{number of non-zero elements in } PH(i)$$

Black pixel is which whose value is ‘ 0’ In order to count the no of black pixel value run a loop where the no of iteration is the size of image and increment the count where

$$Image\ (I, J) = =0;\ Cnt{+}{+}$$

Image Area (IA) is the ratio of the area occupied by signature pixels to the area of the bounding box.

$$IA = \Delta/(WxHy)$$

Where, Δ is the area of signature pixels.

The aspect ratio (A) is the ratio of width to height of the signature. The bounding box coordinates of the signature are determined and the width (Wx) and height (Hy) are computed using these coordinates.

$$A = Wx / Hy$$

Before the ANN training the data (Extracted features of signature Image) was divided into three datasets; the training, validation and test. The training set was used to train the MLP, the validation set was used for early-stopping of the training process and the test set was used to evaluate the MLP performance after completion of the training process. The training data set consist of different sample images.

Forward propagation: The output of each node in the successive layers is calculated

$$O\ (\text{output of a node}) = 1/\ (1+\exp\ (-\Sigma Wij\ xi)) \qquad (a)$$

The Error E (Im) of an image pattern Im is calculated with respect to Target (T)

$$E(Im) = 1/2(\Sigma T(Im) - O(Im))\ 2 \quad (b)$$

Reverse Propagation: The error δ for the nodes in the output layer is calculated

$$\delta(\text{output layer}) = o(T) - o(Im) \quad (c)$$

The new weights between output layer and hidden layer are updated

$$W(n+1) = W(n) + \acute{\eta}\,\delta(\text{output layer}) \quad (d)$$

The training of the network is stopped when the desired mean square error (MSE) is achieved

$$E(MSE) = \Sigma E(Im) \quad (e)$$

3.2 Handwritten Signature Hiding

Using DWT the Host image is decomposed into four sub bands (LL, LH, HL and HH) Signature is converted into one dimensional vector. A pseudo random sequence is generated using a session based key and the size of any sub bands of the cover image. Bits of the signature vector embedded in HH sub-band depending upon the elements of the one dimensional vector and the pseudo random sequences. The general equation used to embed the signature image is:

$$IS(x, y) = I(x, y) + k \times S(x, y) \ldots\ldots\ldots (1)$$

In which I(x, y) representing the selected DWT sub band of the cover image, IS (x, y)) is the modified cover image, K denotes the amplification factor that is usually used to adjust the invisibility of the signature in corresponding sub band. S (x, y) is the pseudo random sequences. Taking all the sub bands including the modified HH sub band, stego image is obtained applying IDWT (Inverse Discrete Wavelet Transformation) twice.

3.3 Handwritten Signature Extraction procedure

The session key and the size of the signature image is provided to the intended receiver through a secrete communication channel. Select the sub-bands into which the handwritten signature was embedded after applying DWT on Stego image. Regenerate the pseudo random sequence (PN) using the same session based key which was used in the signature image embedding procedure. Calculate the correlation between the selected stego sub-band and the generated pseudo random sequence. Compare each correlation value with the mean correlation value. If the calculated value is greater than twice the mean, then the extracted watermark bit will be taken as a 0, otherwise it is taken as a 1. The recovery process then iterates through the entire PN sequence until all the bits of the signature vector has been recovered.
Filter is used on recovered signature to remove unwanted signals.

3.4 Recovered Handwritten Signature Authentication procedure

Taking the recovered handwritten signature from the stego image pre-process it , extract the features and compare it with the template to find whether the matching score is within the threshold. If it is within the range then recovered handwritten signature is authenticated

4. RESULTS

This work tested with painting and signature of Rabindra Nath Tagore downloaded from internet, in image format, only for the sake of experiment.

Fig. 7: Host Image
(Painting of Rabindra Nath Tagore)

Fig. 8 Handwritten Signature
(of Rabindra Nath Tagore)

Fig. 9: Stego Image

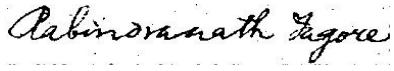


Fig. 10: Recovered Handwritten Signature

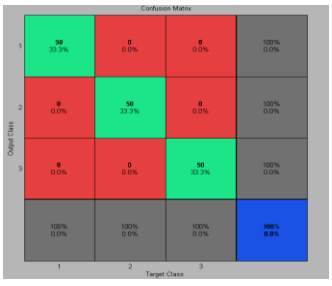


Fig. 11: Confusion Matrix Classification of pattern

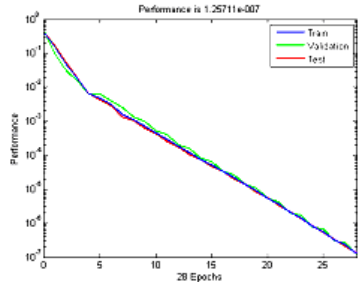


Fig. 12: Learning Performance Vs Epoch in ANN Training

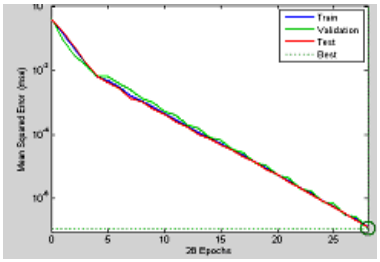
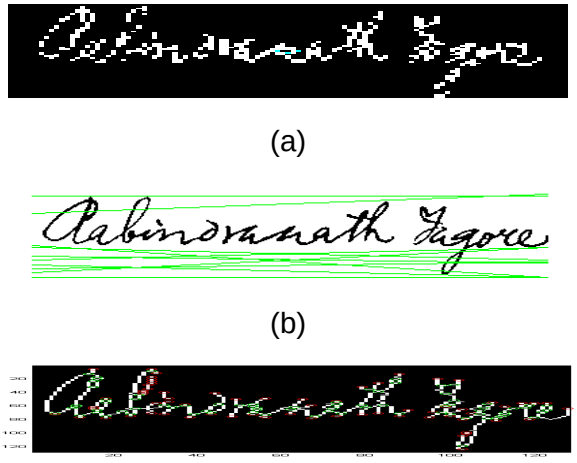


Fig. 13: Validation Performance Testing Vs Epoch



(a)

(b)

(c)

Fig. 14: (a) Center of Gravity (b) Slant Angel (c) No of Cross & Endpoints within the Image

Peak Signal to Noise Ratio (PSNR)

It measures the quality of a Stego image. This is basically a performance metric and use to determine perceptual transparency of the Stego image with respect to host image:

$$PSNR = \frac{MN \max_{x,y} P_{x,y}^2}{\sum_{x,y} \left(P_{x,y} - \overline{P}_{x,y}\right)^2} \qquad (a)$$

Where, M and N are number of rows and columns in the input image

$P_{x,y}$ is the original image and $\overline{P}_{x,y}$ is the Stego Image.

Table 1. PSNR between Cover Image and Stego Image

Cover Image and Stego Image	PSNR
	41.214

Correlation coefficient

After signature image embedding process, the similarity of original Host image x and Stego images x' was measured by the standard correlation coefficient as follows:

$$Correlation = \frac{\sum (x - x')(y - y')}{\sqrt{(x - x')^2}\sqrt{(y - x')^2}} \qquad (b)$$

Where y and y' are the discrete wavelet transforms of x and x'

Correlation between the original Handwritten Signatures and recovered Handwritten Signature after applying filter is 0.9524 shown inTable2.

Table 2. Correlation between original Handwritten Signatures and recovered Handwritten Signature

Correlation Coefficient
0.9524

5. CONCLUSION

In the proposed method handwritten signature image is dispersed in the DWT sub band of the host image randomly so hidden information will remain unaffected after normal distortion of the host image and it will be difficult for any traditional steganalysis method to detect the existence of the hidden information. There is a small visual change in between Host image and stego image that is not visible by human eyes. But due strong security aspects this small amount of imperceptibility is acceptable. In the proposed approach four features are extracted and used for signature verification more number of features can be incorporated to enhance the accuracy of the work. This approach can be extended by using biometric characteristic like iris; retina, ear etc. for multifactor authentication.

6. REFERENCES

[1] G. L. Friedman, "The trustworthy digital camera: Restoring credibility to the photographic image," IEEE Trans. Consumer Electron. vol. 39, pp. 905–910, Nov.1993.

[2] S. Walton, "Image authentication for a slippery new age," Dr. Dobb's J., pp. 18–26, April 1995.

[3] V. Nalwa. Automatic on-line signature verification. Proceedings of the IEEE, 85(2):215– 239, 1997

[4] N. F. Johnson and S. Katzenbeisser," .A survey of steganographic techniques", in S. Katzenbeisser and F. Peticolas (Eds.): Information Hiding, pp.43-78. Artech House, Norwood, MA, 2000.

[5] Lou, D.C.and Liu, J. L. 2002. "*Steganography Method for Secure Communications*". Elsevier Science on Computers& Security, 21, 5: 449-460.

[6] J. Fridrich and M. Goljan, .Practical steganalysis of digital images-state of the art., Proc. SPIE Photonics West, Vol. 4675, pp. 1-13, San Jose, California, Jan. 2002.

[7] A.K. Jain, F. Griess, and S. Connell. On-line signature verification. Pattern recognition, 35(12):2963 2972, 2002

[8] Chan, C. K. and Cheng, L. M. 2003. Hiding data in image by simple LSB substitution. Pattern Recognition, 37:469-474.

[9] M. Kalera, S. Srihari, and A. Xu. Offline signature verification and identification using distance Statistics, 2004.

[10] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," IEEE Trans. on Circuits and Systems for Video Technology, vol. 14, pp. 4–20, Jan 2004.

[11] Iwata, M., Miyake, K. and Shiozaki, A. 2004. "Digital Steganography Utilizing Features of JPEG Images", IEICE Transfusion Fundamentals, E87-A, 4:929-936.

[12] Po-Yueh Chen* and Hung-Ju Lin, "A DWT Based Approach for Image Steganography", International Journal of Applied Science and Engineering 2006. 4, 3: 275-290

[13] Ali Al-Ataby and Fawzi Al-Naima, "A Modified High Capacity Image Steganography Technique Based on Wavelet Transform", The International Arab Journal of Information Technology, Vol. 7, No. 4, October 2010

[14] Blossom Kaur, Amandeep Kaur, Jasdeep Singh, "Steganographic Approach for Hiding Image in DCT Domain", International Journal of Advances in Engineering & Technology, July 2011.

[15] Tanmay Bhattacharya, Sirshendu Hore and S. R. BhadraChaudhuri, "*A Novel Data Encryption Technique by Genetic Crossover of Robust Finger Print Based Key and Handwritten Signature Key",* International Journal of Computer Science Issues (IJCSI), Vol. 8, Issue 5, No 2, September 2011, Pp209-214.

[16] Tanmay Bhattacharya**,** Nilanjan Dey and S. R. BhadraChaudhuri, "A Session based Multiple Image Hiding Technique using DWT and DCT", International Journal of Computer Applications (IJCA) (0975 – 8887) Volume 38– No.5, January 2012, Pp 18-21.