Authentication through Hough transformation generated Signature on G-Let D3 Domain (AHSG)

Madhumita Sengupta* and J. K. Mandal

*Dept. of Computer Science & Engineering, University of Kalyani, Kalyani, Nadia-741235, West Bengal, India

Abstract

In this paper a G-Let based authentication technique has been proposed to authenticate digital documents through Hough transform generated signature generated from original autograph. The cover image is transformed into G-Let domain to generate n number of G-Lets out of which (n/2)-1 numbers of G-Lets are embedded with secret Hough signature bits for the purpose of authentication or copyright protection. The special feature of AHSG is to optimize the distortion rate, by adjustment at the last stage of the technique, using back propagation. Experimental results are computed and compared with the existing authentication techniques like Li’s method, SCDFI, Region-Based method based on Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Image Fidelity (IF), Universal Quality Image (UQI) and Structural Similarity Index Measurement (SSIM) which shows better performance in AHSG, in terms of low computational complexity and better fidelity.

© 2013 The Authors. Published by Elsevier Ltd.
Selection and peer-review under responsibility of the University of Kalyani, Department of Computer Science & Engineering

Keyword: Authentication; Steganography; G-Lets; Hough transform; Peak Signal to Noise Ratio (PSNR).

1. Introduction

Information hiding is a major concern in today’s world of open access internet through wide range of networks. Information can be hidden through various means of tact. Massive areas of such techniques are covered by

* Madhumita Sengupta. Tel.: +91-9432145902; fax: +91-33-2580-9617.
E-mail address: madhumita@klyuniv.ac.in, madhumita.sngpt@gmail.com.
cryptography and steganography. Cryptography converts the plain text of communication to cipher text so that no intruder can able to understand the message where as steganography is an art of hiding plain messages over cover medium secretly so that communication can done securely without intimating the intruder. As per the survey of philosopher, sending communication secretly using cryptographic algorithm is more prone to attack then sending secret communication with the help of steganography.

Steganography is required especially for secure communication, authentication, and ownership protection. Authentication and ownership protection is a process of approving the digital document/multimedia content by computation at sender side, which is able to proof the originality through some techniques or simple computation at receiver side on clam.

Authentication and secret message transmission algorithms based on transform domain are widely used for their robustness in nature, such as discrete cosine transformation [1, 17], Fourier transform [2, 8], Haar wavelet [3], Daubechies transform [4], Z transform [5] and many others. On other hand G-lets a newly developed transformation technique is not a single transform, but a group of linear transformations related with group theory. G-Let is the most natural signal decomposition algorithm for digitized signal without any approximations [6].

This paper proposed an authentication and copyright protection technique AHSG, where the cover image passes through G-Let transformation technique to generate n number of G-Lets. Out of which few selected G-lets from a set are embedded with secret signature generated by Hough transform technique. Rest of the G-Lets are used for adjustment to minimize the error factor.

Various parametric tests are performed and results obtained are compared with most recent techniques such as, Li’s Method [7] SCDFD [8], STMDF [9], Region-Based [10] and WTSIC [11] based on Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Image Fidelity (IF) and Universal Quality Image (UQI) analysis [12] to obtain a comparative statement between existing and proposed technique.

Section 2 of the paper deals with the proposed technique, signature generation through Hough transform is shown in section 3. G-Let Transformation process has been described in section 4. Section 5 deals with embedding, adjustment and authentication technique followed by results and discussions in section 6 and that of conclusion are drawn in section 7 with references cited at end.

2. Proposed Scheme

The proposed AHSG technique is divided into two major tasks, one at sender side for embedding and another at receiver end for authentication. The embedding operation takes grayscale autograph and source/cover image and generates stego-image after computation. The operation of embedding gray scale autograph image which is considered as secret image generates butterfly signature through Hough transformation [16, 17] and this butterfly signature is converted into stream of bits. Source/cover image is transformed through D3 G-Let linear transformation technique [6, 15] based on Dihedral group theory in a row major order of 2 x 2 window. As Dihedral group having only two transformations, namely rotations and reflections, thus after computation six G-Lets are generated labeled as G-Let 1, G-Let 2, G-Let 3, G-Let 4, G-Let 5 and G-Let 6. Out of which G-Let 2 and G-Let 3 are taken to fetch 2nd and 3rd component of every 2 x 2 window and secret bits are embedded from stream of bits generated previously. Two phases of adjustments are applied after embedding over 2 x 2 window to minimize the image distortion and error rate. The image is then reconstructed back with embedded G-Lets and the rest of all G-Lets. The schematic representation of the algorithm is shown in figure 1.

The output of embedding procedure is stego-image, which can be transmitted through mesh network. On receipt of stego-image at the receiver, stego-image passes a test of computation to check the authenticity of the image. D3 G-Let transformation technique is applied to generate ‘n’ number of g-lets and then predefined hash is used to fetch the bits from 2nd and 3rd components of 2 x 2 window in a row major order from G-Let 2 and G-Let 3 to generate a stream of bits. This stream of bits is compared with the bit stream generated separately from the autograph through
Hough transformation at receiver end. By comparing these two streams of bits ownership is verified.

3. Signature Generation

Signature is a unique pattern generated by a sequence of strokes. These strokes can be physical lines for Human signature or combination of many lines generated uniquely by set of steps. As digital document can’t be signed by pen by human thus in lieu of human signature computer generated signature are more popular now a day’s.

To generate a signature of an image, a special transformation technique is used named Hough [14]. Hough transform technique identifies and extracts significant features of image orientation by analyzing lines [13]. Hough transform maps the individual pixels from image domain into a shape in parameter domain [14] that’s creates a butterfly like pattern known as signature. In AHSG images of autographs are passed through Hough transform with a range of 0 to 100 pixel value in cover, as selected for proposed work, dependent on hash function.

Gray scale autograph image on passing through Hough transformation with range, and origin as center of image, generates a matrix of rho verses theta, by eq 1 and eq 2 where limits are $1 \leq \theta < \pi$ and $-N \leq \rho \leq N$.

$$N = \left(\frac{\sqrt{Row^2+Col^2}}{2}\right) \quad (1)$$

$$\rho_l = (x \cdot \cos \theta + y \cdot \sin \theta) \quad (2)$$

On calculation of rho for each value of theta and incrementing the matrix value of rho verses theta a butterfly like structure arise, that unique structure is termed as butterfly signature image as shown in figure 3.
4. G-Let Transformation Technique

Transformation techniques are used to convert spatial domain image into frequency domain to increases the robustness of the embedding technique. In AHSG G-Let transformation technique is used before embedding.

A G-Let transformation technique selects finite group transformation so that they are always completely reducible into irreducible representation. The dimension of the irreducible representations follows the properties [6] of equation 1.

\[ \sum_{i=1}^{n} d_i^2 = D_n \]  

(3)

where \( d_i \) = dimension of \( i^{th} \) irreducible representation, \( D_n \) = dimension of representation matrix and ‘n’ = number of irreducible representations.

In a dihedral group \( D_3 \), \( n = 3 \), means that there are ‘3’ rotation and ‘3’ reflections available. So there are \( 2 * 3 = 6 \) six matrices produced for each transformation. The rotation matrix \( R_\theta \) and reflection matrix \( S_\theta \) governing the transformation is given in equation 4 and 5 respectively.

\[ R_\theta = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} \]  

(4)

\[ S_\theta = \begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix} \]  

(5)

where \( \theta \) is \((0, 2\pi/3, 4\pi/3)\).

The computational complexity of the process depends mainly on the number of irreducible representations which is \((n+6)/2\) for even size signal ‘n’ and \((n+3)/2\) for odd size signal ‘n’.

4.1. Forward Transformation

Six different G-Lets are computed through D3 G-Let transformation technique. Those G-Lets coefficients are grouped based on rotation and reflection transformation used for computation. G-let 1, G-let 2 and G-let 3 through rotational transformation and G-let 4, G-let 5 and G-let 6 are by reflection transformation. The computation is simple matrix multiplication of \( R_\theta \) and \( S_\theta \) with 2 x 2 non overlapping mask of window in a row major order respectively for all three value of \( \theta \). Illustration through example for the transformation is given in figure 4 for D3. G-let with \( \theta \) taken as 0, \( 2\pi/3 \) and \( 4\pi/3 \) respectively and the computation result over few pixels of gray scale Elaine image is shown in figure 5.
The pictorial representation of forward G-let transformation over Elaine image of dimension 512 x 512 is shown in figure 5. Where G-Let 1, G-Let 2 and G-Let 3 are computed through rotational transformation and G-Let 4, G-Let 5 and G-Let 6 are computed through reflection transformation.

4.2. Inverse transformation

Inverse transformation is the reverse procedure to regenerate the original image. This can be achieved by simple addition of all the g-lets of a single basis for all the $\theta$ greater than 0 and less than $360^\circ$. In proposed AHSG cell by cell addition of G-let 2 and G-let 3 is done to regenerate the image/stego-image with negation as represented in figure 6.

5. Embedding with Adjustment & Authentication of AHSG technique

AHSG technique uses two different transformation technique, one for secret bit generation and another for making the embedding technique robust by converting cover image from spatial domain to frequency domain before embedding.

5.1. Embedding

Based on forward transformation through D3 G-Let, embedding is done on every 2nd and 3rd component of G-Let 2 based on hash function. The hash function ‘H’ is \((\text{col\_win} + \text{max\_bit}) \mod \text{hig\_pos}\) where col\_win is the column number based on active window and max\_bit is the maximum number of bits allowed per byte and hig\_pos is the highest position allowed for embedding from LSB towards MSB. In AHSG max\_bit is taken as two and the value of hig\_pos is three. An example of embedding is shown in figure 7 where 2nd and 3rd component of the G-Let 2 are embedded with two secret bits 0 and 1 at position LSB+3 and LSB+1 in 2nd and 3rd component respectively.
5.2. Adjustment

Two stage of adjustment is required to get the optimized statistical results. ‘Minimum Deviation of Fidelity’ [9] has been used as first step to minimize the error rate caused due to embedding. Secondly the absolute error figures out to maintain the symmetry by adjusting G-Let 3. This adjustment on G-Let 3 is done through the gap generated in G-Let 2 and embedded G-Let 2. In figure 7 2nd component deviates from -189 to -181 due to embedding that is deviation of +8 and in 3rd component deviation is -2. The calculated deviation needs to be implied on G-Let 3 at same position to maintain the symmetry as shown in figure 8. An integer in 2nd component of G-Let 3 is 10 after adjustment of +8 it’s become 18, and that of 3rd component in G-Let 3 is -148 that becomes -150. The embedded and adjusted components of G-Lets with other unaffected G-Lets construct stego image.

| G-let 3 | G-let 3 after Adjustment |
|---------|--------------------------|
| -212.514 | 10.09                  |
| -148.382 | 203                     |
| -212.514 | 18.09                  |
| -150.382 | 03.00                   |

Fig. 8. Adjustment on G-let 3 to maintain symmetry

5.3. Authentication

Authentication is a process of approving to the content transmitted through unsecured channel at receiver end. An example of embedding and adjustment is shown in figure 9 for the Baboon and Couple image. G-Let 2 and G-Let 3 of both the images are shown with corresponding embedded and adjusted G-Lets. Stego image and extracted secret image is also shown which when compared with original secret image gives zero error rates with infinite PSNR in dB.

Fig. 9. Example of embedding, adjustment and authentication over Baboon and Couple image
6. Results and Discussion

Ten pgm images have been taken as cover/source image [18] with ten different autographs [16] and AHSG is applied to compute the results respectively. All cover images are of 512 x 512 in dimension with autographs images of 256 x 256 in dimension and the corresponding Hough generated secret butterfly signature are 128 x 128 in dimension. Average MSE is 1.0 and that of PSNR is 48.1dB and the statistical calculation of image fidelity on average shows 0.99995, Universal Quality Image (UQI) and Structural Similarity Index Measurement (SSIM) is 0.999532 and 0.999548 respectively. All cover images are shown in figure 10. Ten grayscale autograph with Hough generated secret butterfly signature of dimension 128 x 128 are shown in figure 11. The detail computation is given in table 1.

Fig. 10. Cover images of dimension 512 x 512 in ppm formate

| Gray scale Autograph image 256 x 256 in dimension | a. Autograph 1 | b. Autograph 2 | c. Autograph 3 | d. Autograph 4 | e. Autograph 5 | f. Autograph 6 |
|-----------------------------------------------|---------------|---------------|---------------|---------------|---------------|---------------|
| Secret butterfly Signature of 128 x 128 in dimension | ![Secret Butterfly Signature 1](image1) | ![Secret Butterfly Signature 2](image2) | ![Secret Butterfly Signature 3](image3) | ![Secret Butterfly Signature 4](image4) | ![Secret Butterfly Signature 5](image5) | ![Secret Butterfly Signature 6](image6) |

Fig. 11. Ten gray scale autograph images with corresponding Hough generated butterfly signature
Table 1. Statistical analysis on embedding 128 x 128 dimensions secret butterfly signature

| Cover Image | MSE     | PSNR    | IF       | UQI     | SSIM    |
|-------------|---------|---------|----------|---------|---------|
| Baboon      | 1.006393| 48.103126| 0.999946 | 0.999730| 0.999735|
| Boat        | 0.996788| 48.144775| 0.999947 | 0.999771| 0.999774|
| Clock       | 0.998596| 48.136905| 0.999974 | 0.999845| 0.999846|
| Couple      | 1.007477| 48.098453| 0.999938 | 0.999608| 0.999616|
| Elaine      | 1.000916| 48.126829| 0.999952 | 0.999764| 0.999767|
| Jet         | 1.020554| 48.042445| 0.999967 | 0.998956| 0.999015|
| Map         | 1.002548| 48.119751| 0.999971 | 0.999677| 0.999683|
| Space       | 0.997475| 48.141785| 0.999941 | 0.999327| 0.999352|
| Tank        | 0.996841| 48.144543| 0.999945 | 0.999319| 0.999346|
| Truck       | 0.997772| 48.140490| 0.999918 | 0.999319| 0.999346|
| **Average** | **1.002536**| **48.11991**| **0.99995**| **0.999532**| **0.999548**|

6.1. Survival on Attack

Attacks are the malevolent action over an image during transmission through unsecured network without prior information to the owner or concern authority. Attack is a major concern in the field of steganography. The attacks in discussion are shown in figure 12. In the first attack few windows are copied from neighbor position. Second attack is the missing of information from an image with same image tone. Third attack is on the color intensity of an object present in an image without modifying object directly. Fourth one is the common attack known as crop attack and the fifth attack is a white mesh over an image. The statistical calculation of embedded image (A) with its corresponding attacked image (B) are also shown with the extracted secret from (A) before attack and (B) after attack. The fourth and fifth attack degrade the image with MSE 4181.3 and 7247.9 respectively, after applying the authentication algorithm of proposed AHSG technique the extracted secret image can be compared with the original secret image through human perception.
6.2. Comparison of AHSG with existing technique

A comparative study has been made among Li’s Method [7], SCDFT [8], Region-Based [6], STMDF [9], IAHTSSDCT [7] and AWTDHDS [8] with proposed AHSG technique on the basis of payload verses PSNR in dB. For maximum of 0.52 bits per byte of payload the maximum PSNR is 48.11. That can be achieved through proposed AHSG with robustness in algorithm to struggle against intentional attacks. The detail data are shown in table 2.

Table 2. Comparison of proposed AHSG with existing techniques

| Technique          | Capacity (bytes) | Size of cover image | bpB (Bits per bytes) | PSNR in dB |
|--------------------|------------------|---------------------|----------------------|------------|
| Li’s Method [7]    | 1089             | 257 * 257           | 0.13                 | 28.68      |
| SCDFT [8]          | 3840             | 512 * 512           | 0.12                 | 30.10      |
| Region-Based [6]   | 16384            | 512 * 512           | 0.5                  | 40.79      |
| STMDF [9]          | 16900            | 512 * 512           | 0.52                 | 42.74      |
| IAHTSSDCT [7]      | 16384            | 512 * 512           | 0.5                  | 47.48      |
| AWTDHDS [8]        | 16384            | 512 * 512           | 0.5                  | 44.87      |
| AHSG               | 16384            | 512 * 512           | 0.5                  | 48.11      |

Through the graphical representation of data presented in table 2 as shown in figure 13, it is clear that the proposed AHSG while applying for embedding or authentication generates stego-image with higher PSNR in dB then the other existing techniques.
References

[1] Madhumita Sengupta, J. K. Mandal “Image Authentication using Hough Transform generated Self Signature in DCT based Frequency Domain (IAHTSSDCT)”, IEEE, ISED- 2011, Kochi, Kerala, pp- 324-328, DOI 10.1109/ISED.2011.43, (2011).

[2] Ghoshal, Nabin, and Mandal, Jyotsna Kumar, “A Novel Technique for Image Authentication in Frequency Domain Using Discrete Fourier Transformation Technique (IAFDFTTT)”. Malaysian Journal of Computer Science, Vol 21 (No. 1). pp. 24-32. ISSN 0127-9084, Faculty of Computer Science & Information Technology, University of Malaya, Kuala Lumpur, Malaysia, (2008).

[3] Madhumita Sengupta, J. K. Mandal, “Authentication in Wavelet Transform Domain through Hough Domain Signature (AWTDHDS)”, UGC-Sponsored National Symposium on Emerging Trends in Computer Science (ETCS 2012), ISBN number 978-81-921808-2-3, pp 61-65, (2012).

[4] Madhumita Sengupta and J. K. Mandal, “Self Authentication of image through Daubechies Transform technique (SADT)”, First International Conference on Intelligent Infrastructure, CSI- 2012, 47th Annual National Convention, Organised by: Computer Society of India, Kolkata Chapter, Proceedings published by Tata McGraw Hill Education Private Limited, ISBN(13):978-1-25-906170-1, ISBN(10): 1-25-906170-1, pp-249-252, December, 2012.

[5] Madhumita Sengupta and J. K. Mandal, “Image coding through Z-Transform with low Energy and Bandwidth (IZEB)”, The Third International Conference on Computer Science and Information Technology (CCSIT- 2013), Published in Computer Science & Information Technology (CS & IT), pp. 225-232, DOI : 10.5121/csит.2013.3625, Bangalore, India, 18-20, Feb (2013).

[6] Rajathilagam, B., Rangarajan, M., Soman, K.P., “G-Lets: A New Signal Processing Algorithm”, International Journal of Computer Applications (0975 – 8887) Volume 37– No.6, Published by Foundation of Computer Science, New York, USA, doi : 10.5120/4609-6591, January 2012.

[7] Li Yuancheng, Xiaolei Wang, “A watermarking method combined with Radon transform and 2D-wavelet transform”, IEEE, Proceedings of the 7th World Congress on Intelligent Control and Automation, June 25 - 27, Chongqing, China, 2008.

[8] T. T. Tsui, X.-P. Zhang, and D. Androutsos, Color Image Watermarking Using Multidimensional Fourier Transformation, IEEE Trans. on Info. Forensics and Security, vol. 3, no. 1, pp. 16-28, 2008.

[9] J. K. Mandal, Madhumita Sengupta, “Steganographic Technique Based on Minimum Deviation of Fidelity (STMDF)”, IEEE, Second International Conference on Emerging Applications of Information Technology (EAIT 2011), print ISBN: 978-1-4244-9683-9, DOI: 10.1109/EAIT.2011.24, pp – 298 – 301, Issue Date: 19-20 Feb. 2011.

[10] A. Nikolaidis, I. Pitas, “Region-Based Image Watermarking”, IEEE Transactions on Image Processing, Vol. 10, NO. 11, pp. 1721-1740, November 2001.

[11] J. K. Mandal, Madhumita Sengupta, “Authentication /Secret Message Transformation Through Wavelet Transform based Subband Image Coding (WTSIC)”, IEEE, International Symposium on Electronic System Design, pp 225-229, ISBN 978-0-7695-4294-2, Bhubaneswar, India, Print ISBN: 978-1-4244-8979-4, Dec, 20th - 22nd, 2010, DOI 10.1109/ISED.2010.50, 2010.

[12] M. Kutter , F. A. P. Petitcolas, A fair benchmark for image watermarking systems, Electronic Imaging ’99. Security and Watermarking of Multimedia Contents, vol. 3657, Sans Jose, CA, USA, January 1999. The International Society for Optical Engineering.

[13] V.F. Leavers, “Shape detection in computer vision using the hough transformation”, Springer-Verlag, Berlin, 1992, 201 pages, ISBN- 3-540-19723-0, Published online by Cambridge University Press 09 Mar 2009, doi: 10.1017/S0263574700016210.

[14] P.V. C. Hough. A Method and Means for Recognizing Complex Patterns. US Patent: 3,069,654, Dec. 1962.

[15] Rajathilagam, B., Rangarajan, M., and Soman, K.P., G-lets: Signal Processing Algorithm Using Transformation Groups, IEEE Trans. Imag. Proc., 2011.

[16] Madhumita Sengupta, J. K. Mandal, “Authentication in Wavelet Transform Domain through Hough Domain Signature (AWTDHDS)”, UGC-Sponsored National Symposium on Emerging Trends in Computer Science (ETCS 2012), ISBN number 978-81-921808-2-3, pp 61-65, (2012).

[17] Madhumita Sengupta, J. K. Mandal “Image Authentication using Hough Transform generated Self Signature in DCT based Frequency Domain (IAHTSSDCT)”, IEEE, ISED- 2011, Kochi, Kerala, pp- 324-328, DOI 10.1109/ISED.2011.43, (2011).

[18] 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, 2013).