

A GENETIC ALGORITHM BASED IMAGE AUTHENTICATION TECHNIQUE USING DAUBECHIES WAVELET TRANSFORM (AGAIATDWT)

Dr. Amrita Khamrui

*Dept. of Computer Science, Vivekananda College, Madhyamgram, Kolkata
700129, West Bengal, India,*

Abstract

The modern days are being more occupied to the use of technology for facilitating day to day tasks. In this regard, authentication is turning to be great challenge when sending information from one place to another with the aid of technology. In this research a frequency domain based image authentication technique using Daubechies Wavelet Transform has been proposed. This research is based on frequency domain where Daubechies Wavelet Transform is implemented. First daubechies wavelet transform is applied on a 4×4 mask in row major order. It generates transformed coefficients. Secret information from the authenticating image are embedded onto the transformed coefficients. Reverse Daubechies Wavelet Transform is applied to generate spatial domain mask. This process is applied for the whole cover image to generate stego image. Stego image is processed through Genetic Algorithm to generate optimized stego image. The performance of this research work has been evaluated by different parameters. This research work has been compared with existing daubechies Wavelet Transformation based technique [7] and obtains better result as compared to the existing approach.

Keywords:

Discrete wavelet transform (DWT), structural similarity index measure (SSIM), mean square error (MSE), Image fidelity (IF), peak signal to noise ratio (PSNR).

1. INTRODUCTION

Transmitting image from one place to another has some security issues. Authentication can be achieved in various ways. One of the technique for image authentication is Steganography. Steganography is a technique of transmitting messages/ images through some communication media such that no one realize that there is some hidden information except sender and receiver . There are two types of Steganography spatial domain steganography [11], [12] and frequency domain steganography [10]. Image authentication is one of the technique to detect unauthorized access. The secret message is embedded inside the cover image without changing its visibility. Common steganographic technique is the least-significant bit (LSB) replacement [7] strategy through masking [17], [8],[18] filtering and transformations [9] on the source image. Steganographic technique uses picture [11], video, sound file as cover image. In modern day, to ensure the security a message may be hidden invisibly by using some steganographic algorithms [13], [14] which is big concern today for network trafficking. Steganography can be achieved by hiding information into images. Image authentication can be achieved by hiding information in the image without changing its visibility. Image authentication and verification of ownership [15] is very crucial for scientists, research institute and military people. To prevent unauthorized access of information, image authentication is very important for the digital image document. Information hiding refers to embedding of information invisibly within a cover data set such as message, image or video. The data hiding is a process of creating hypermedia document or image, which is very less convenient to manipulate. Steganography hides the secret message/image in the cover image by some algorithm and cryptography hides the message content. The process is to hide a message inside an image by keeping the visibility intact. The most common method of steganography is least-significant bit (LSB) substitution developed through masking, filtering and transformations on the source image.

In this research a frequency domain-based image authentication technique using Daubechies Wavelet Transform has been proposed. Previous research works embed minimum bits of the hidden image, but the proposed transformed domain based algorithm embeds large amount of information with a minimum distortion of visual property. Rest of the paper is organized as follows: section 2 deals with review of literature. Section 3 deals with the proposed approach.. Results, comparison and analysis are discussed in section 4. Social applications are discussed in sections 5. Conclusion is drawn in section 6 and References are drawn at end.

2. LITERATURE REVIEW

Some existing methodologies have been discussed in this section. Tevaramani Saleem S et al. [1] proposed image steganography in 2022 using discrete wavelet transform and alpha blending for secure communication. In this research a scaling parameters called alpha is used. Cover image and secret images are of different types and dimensions. Webcam images and other predefined images of different formats have been normalized and preprocessed. Haar Discrete Wavelet Transformation (DWT) is applied on the cover and authenticating images. Stego image is generated by encrypting the authenticating image in the source image. Varuikhina Vladimir et al. [2] proposed continuous Wavelet Transform applications in steganography in 2021. This paper hides information with the help of Wavelet Transformation without any visible changes in the source image. In this technique single level 2D Discrete Wavelet Transformation (Daubechies, Haar and coiflet transformation) are used and the result generated by each transformation has been compared with one another. Govindasamy V et al.[3] proposed coverless image steganography using Haar Integer Wavelet Transform in 2020. Recent technique of steganography is coverless image steganography which does not modify the source image that is carrying the secret information. This coverless image steganographic technique used Haar Integer Wavelet Transform to hide more secret information. Here the image has been divided into sub matrices. Integer Wavelet Transformation is used to generate coefficients of the submatrix. Then the sub-matrices are reshaped to form arrays. Binary bits are generated from the coefficients. 8 bits are generated from the secret message and matched with the block and starting location in the array. Receiver used the location map to obtain the secret information. Houssein Essam H. et al. [4] proposed an image steganography algorithm using Haar Discrete Wavelet transform with advanced encryption system in 2016. This paper used Advanced Encryption System (AES) to encrypt data and Haar Discrete Wavelet Transform (HDWT) is used for embedding. The complexity in image steganography has been decreases by using HDWT and ensures less image distortion and lesser detectability. In 2010 Hui-Yu Huang et al proposed a lossless data hiding technique which is based on [5] discrete Haar wavelet transform. In 2016 Tushara M et al [6] proposed a review of image Steganography using discrete wavelet transform which presents a review on steganography techniques that use discrete wavelet transform. In 2015 Shrestha A et al.[7] proposed Daubechies Discrete Wavelet Transform based color image steganographic technique. In this paper source image is transformed by Daubechies DWT and hidden information is embedded on the transformed coefficients of Daubechies DWT and generates stego image. Reverse process is followed to extract secret information from stego image. The performance of this technique is evaluated using PSNR and MSE. In 2012 Sengupta M et al. [8] proposed frequency domain based steganographic technique using Daubechies transformation where the source image is transformed into the transformed domain using Daubechies transformation. It generated four components such as, “Low resolution”, “Horizontal orientation”, “Vertical orientation” and “Diagonal orientation”. Authenticating bit streams are embedded in 3rd coefficient of every sub image in different positions. A delicate handling is performed to minimize the pixel difference. Reverse transformation is performed to generate stego image.

3. PROPOSED APPROACH

The technique (AGAIATDWT) is illustrated in this section. A mask of size 4×4 is taken in row major order from source color image The mask is processed through Daubechies Wavelet Transformation to generate transform coefficients. The Daubechies Wavelet Scaling functions and Transformation functions can be defined in equation [1] and [2].

$$\phi(t) = \sum_{n=-\infty}^{+\infty} h[n].\phi(2t - \tau) \quad [1]$$

$$\psi(t) = \sum_{n=-\infty}^{+\infty} g[n].\phi(2t - \tau) \quad [2]$$

Where sequence of lowpass impulse response filter coefficients is $h[n]$ and sequence of highpass impulse response filter coefficients is $g[n]$. Forward Daubechies transformation multiply the image matrix with the row transformation matrix followed by column transformation matrix. The resultant matrix of forward Daubechies transformation generates four coefficients. Inverse Daubechies transformation matrix is generated from forward daubechies transformation coefficients multiplied by column transformation matrix followed by row transformation matrix. The result generated from inverse Daubechies transformation is the original image. The equation of forward and inverse Daubechies transformation technique is shown in equation [3], [4], [5], [6] and [7] respectively where D and W are the coefficients of the row and column transformation matrix. The row transformation matrix and the column transformation matrix uses the coefficient value as follows

$$D0 = (1 + \sqrt{3}) / (4 * \sqrt{2})$$

$$D1 = (3 + \sqrt{3}) / (4 * \sqrt{2})$$

$$D2 = (3 - \sqrt{3}) / (4 * \sqrt{2})$$

$$D3 = (1 - \sqrt{3}) / (4 * \sqrt{2})$$

$$W0 = D3, W1 = -D2, W2 = D1, W3 = D0$$

The process of AGAIATDWT is shown in Figure 1. Process of embedding is explained in section 3.1 process of extraction is explained in section 3.2.

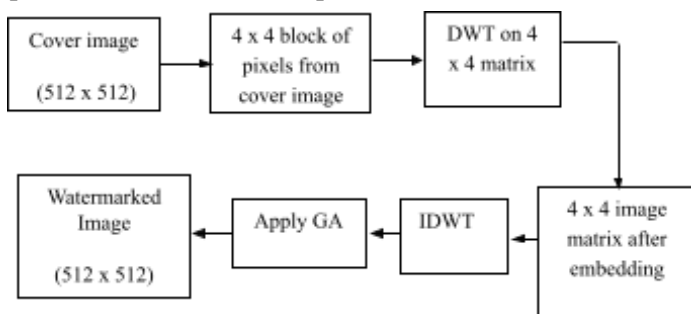


Figure 1. Schematic diagram of AGAIATDWT

Two bits of the authenticating image are extracted and embedded onto alternate transformed image coefficient sub mask. Spatial coefficients are generated by inverse Daubechies Wavelet Transform. The dimension of the hidden image is embedded first followed by the content of the hidden image. Optimized stego image is generated by processing the stego image through Genetic Algorithm. New Generation followed by Crossover and Mutation are applied on stego image. In New Generation operation eight chromosomes are taken randomly and taken as initial population. For part of the selection procedure Roulette wheel selection has been applied to get two fittest chromosomes using hash function. Two new off springs has been generated through crossover from two fittest chromosomes. Two off springs are processed through Mutation. Most fitted offspring is chosen for next iteration in elitism . This process is repeated until the optimum value has been received.

3.1 Algorithm for embedding

In AGAIATDWT source color image of size $p \times q$ is taken. Authenticating color image is of size of $m \times n$. Authenticating image bits are embedded in the transformed coefficients mask of source image.

Input: Source color image of size $p \times q$, authenticating color image of size $m \times n$.

Output: Optimized stego image of size $p \times q$.

Method: Embedding of authenticating color image bits into the source color image followed by GA

Step 1: The dimension of the authenticating image is extracted from the authenticating image

Step 2: Read source color image mask of size 4×4 in row major order. Daubechies Wavelet Transformation is applied to generate transformed coefficients.

Step 3: The authenticating image dimension is embedded followed by the content of authenticating image onto two LSBs of alternate coefficients. Width of the authenticating image is embedded onto the first sixteen embedding positions and next sixteen embedding positions are reserved for height.

- Step 4: Spatial coefficients are generated by inverse Daubechies Wavelet Transform.
- Step 5: Stego image is generated by applying the embedding process for the whole cover image.
- Step 6: Optimized stego image is generated by applying GA on the stego image. As part of GA eight random chromosomes are taken as initial population.
- Step 7: The hidden informations are fabricated on last two LSB of alternate coefficients positions. Roulette Wheel selection is applied on it with a hash function to select two fittest chromosomes among the initial populations. The hash function is taken as $f(n) = 1/(\text{mod}(s(x,y) - c(x,y))+1)$, where fitness function is $f(n)$, $s(x,y)$ is stego image intensity value for the coordinate (x, y) . $c(x, y)$ is intensity value of the source image for the coordinate (x, y) . The fittest value is one.
- Step 8: In Crossover process Uniform crossover process is followed in which first bit is from first parent and second bit is from second parent is taken and it will be started from fourth bit.
- Step 9: Crossovered chromosomes are processed through Mutation. In Mutation a bit flipping operation is performed which will be started from fourth bit.
- Step 10: In Elitism the best chromosome is forwarded to the next iteration and the weak chromosome is eliminated. In elitism the alternate coefficients of the 4×4 mask will be unchanged to ensure proper decoding.
- Step 11: Optimized stego image is generated by repeating Step 7 to Step 10 for the whole stego image.

3.2 Algorithm for decoding

The optimized stego image (spatial domain) is transmitted through network. At the receiver end Optimized stego image is received and the hidden image is extracted from it.

Input: optimized color stego image of size $p \times q$.

Output: Source color image of size $p \times q$, authenticating color image of size $m \times n$.

Method: Decoding of authenticating color image from embedded image

Step 1: Read optimized color image mask of size 4×4 in row major order. Inverse Daubechies Wavelet Transformation is applied to generate transformed coefficients.

Step 2: Authenticating image bits are extracted from the two LSBs of alternate coefficient. Authenticating image bit positions are replaced in the block by '1'. For each eight bits extraction one byte of the authenticating image pixel is formed. Width is formed from first sixteen bit extraction and height is formed from next sixteen bit extraction from the authenticating image.

Step 3: Step 1 and step 2 is repeated to regenerate authenticating image as per size of the authenticating image.

Step 4: Stop

4. Results, comparison and analysis

The performance of the proposed technique AGAIATDWT has been discussed in this section. Some benchmark images has been taken from the USC-SIPI Image Database: Version 5, Original release: October 1997, Signal and Image Processing Institute, University of Southern California, Department of Electrical Engineering [16] for experimental verification. All the experiments has been performed on Intel Core 2 Duo CPU, 3.00 GB RAM and 2.00 GHz machine with GCC compiler. Source color images are of dimension 512×512 , authenticating color image is of size 180×150 and optimized stego color image is of dimension 512×512 . This section discusses the results of the algorithm in terms of visual interpretation and performance of the algorithm based on some statistical parameters such as PSNR, MSE, IF and SSIM. Source images shown from Figure 2.i to 2.v are Lenna, Baboon, Pepper, Tahoe, Toucan. Authenticating image shown in Figure 2.vi is jet. Figure 2.vii to 2.xi shows the optimized stego images using AGAIATDWT. Figure 2 shows that no such changes visible in the optimized stego image as compared to the source image. The result of statistical analysis (PSNR, MSE, IF and SSIM [23] value) is shown in Table 1 for each of the embedded image against the source image. The maximum value of PSNR shown in Table 1 is 38.062263 and that of minimum value of the PSNR is 33.859158. PSNR stands for peak signal to noise ratio and high value

of PSNR indicates that the better quality of the optimized stego image. MSE stands for mean square error. Low error indicates low value of MSE. IF stands for image fidelity and is used to check two images. IF is equal to 1 means two images are identical. Structural similarity index measurement is denoted by SSIM and is obtained by comparing the pixel intensities. It compares the image degradation due to information hiding. The formula for PSNR, MSE, IF and SSIM is given in equation (8), (9), (10) and (11) respectively, where equation (12) denoted the formula for μ_x and μ_y and equation (13) and (14) denotes σ_x^2 and σ_y^2 . Equation (15) denotes σ_{xy} and equation (16) indicates constants C1, C2, K1, and K2. Table II shows the result of comparison of AGAIATDWT with existing [7]. The proposed technique obtains better result as compared to the existing technique [7]. The following formula is used to calculate PSNR, MSE and IF (image fidelity) and SSIM.

(8)

$$PSNR = 10 \log(\max(I_{m,n}^2)/I) \quad (9)$$

$$MSE = \frac{1}{MN} * \sum_{m,n} (I_{1m,n} - I_{2m,n})^2 \quad (10)$$

$$IF = 1 - \sum_{m,n} (I_{1m,n} - I_{2m,n})^2 / \sum_{m,n} I_{2m,n}^2$$

$$SSIM = 2(\mu_x\mu_y + C_1)(2\sigma_{xy}+C_2)/((\mu_x * \mu_x + \mu_y * \mu_y + C_1) * (\sigma_x * \sigma_x + \sigma_y * \sigma_y + C_2)) \quad (11)$$

$$\mu_x = 1/N \sum_{i=1}^N X_i, \mu_y = 1/N \sum_{i=1}^N Y_i \quad (12)$$

$$\sigma_x * \sigma_x = 1/N-1 \sum_{i=1}^N (X_i - \mu_x)^2 \quad (13)$$

$$\sigma_y * \sigma_y = 1/N-1 \sum_{i=1}^N (Y_i - \mu_y)^2 \quad (14)$$

$$\sigma_{xy} = 1/N-1 \sum_{i=1}^N (X_i - \mu_x)(Y_i - \mu_y) \quad (15)$$

The value of C₁, C₂ and C₃ with K₁ and K₂ are from [19] given in equation (16)

$$C1 = (K_1 L)^2, C2 = (K_2 L)^2, K1 = 0.01, K2 = 0.03 \quad (16)$$




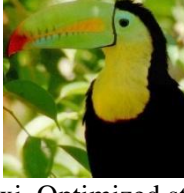
 i. Source image lenna	 vii. Optimized stego lenna
 ii. Source image baboon	 viii. Optimized stego baboon
 iii. Source image pepper	 ix. Optimized stego pepper
 iv. Source image tahoe	 x. Optimized stego tahoe
 v. Source image toucan	 xi. Optimized stego toucan
 vi. Authenticating image jet	

Figure 2: Visual interpretation of various source and optimized stego images along with authenticating image.

Table 1: PSNR, MSE, IF & SSIM values of various optimized stego images

<i>Cover image</i>	<i>PSNR</i>	<i>MSE</i>	<i>IF</i>	<i>SSIM</i>
lenna	36.825966	13.504664	0.999322	0.99997
baboon	37.033325	12.875012	0.999328	0.999986
pepper	36.372753	14.990113	0.999098	0.999979
avion	38.062263	10.159074	0.999710	0.999987

barnfall	37.226166	12.315829	0.998339	0.999995
blakeyed	33.859158	26.740210	0.997630	0.999965
blueeye	35.889240	16.755463	0.996850	0.999991
toucan	34.993084	20.595478	0.998365	0.999872
tahoe	37.030392	12.883716	0.998416	0.999995
manhatan	37.704216	11.032116	0.998968	0.999958

Table II

comparison of psnr values obtained for various images using AGAIATDWT and existing[7]

Source image	PSNR values of AGAIATDWT	MSE values of AGAIATDWT	PSNR values of existing[7]	MSE values of existing[7]
Image1	36.825966	13.504664	24.56	227.559
Image2	37.033325	12.875012	16.10	1593.80
Image3	36.372753	14.990113	17.83	1069.40

5. Social Applications

The proposed technique can be find applications in the following areas:

i) Image authentication

This technique (AGAIATDWT) can be used for Image authentication. source image is considered as the image that needs to be authenticated. Authenticating image is an image which is smaller size than source image. Authenticating image is embedded using AGAIATDWT and send across the network by keeping the visibility of the source image intact. At the receiver end authenticating image is extracted by the receiver using extraction algorithm. If the extracted image and the original authenticating images are same, then the image is authentic.

ii) Telemedicine

Remote medical services via real time on both way communication between patient and the doctor using audio or visual electronic means is refers to as Telemedicine. If the image is communicated over the transmission media then it should be authenticated. The authentication process is stated in previous example. So AGAIATDWT can be used in image authentication.

iii) Document authentication

AGAIATDWT can be used in document authentication. Take a legal image. The document consists of an image part and a text part. If someone tampers the document it can be recognized through AGAIATDWT. From the text part, a digest can be generated using any message digest algorithm and it can be embedded in the image part of the legal document. When it needs to be authenticated the digest is extracted from the image part of the legal document and another digest is generated from the text part of the legal document. If both are same then the legal document is authenticated.

iv) Bank transaction

AGAIATDWT technique can be used in bank to secure e-payment method. Online shopping is very familiar now a days. This required online transaction. So there is an important task to protect the customer's information through this technique.

v) Smart city application

AGAIATDWT can be used in smart city application to hide the health record electronically.

vi) Secure message transmission

Secure message transmission can be ensured by AGAIATDWT. The message that is to be transmitted in secure way should be hidden in the source image and can be transmitted over network. At the receiver end it is extracted from the transmitted image in reverse way.

6. CONCLUSION

The technique AGAIATDWT is a frequency domain technique for image authentication. This technique hides large amount of message by Daubechies Wavelet Transformation and Genetic Algorithm is used for optimization. This technique has been compared with some existing Daubechies Wavelet Transformation-based approaches and it shows that the technique shows better performance than the existing approach.

Availability of data and materials

The dataset is taken from The USC-SIPI Image Database by Allan G. Weber. Version 5, Original release: Signal and Image Processing Institute, October 1997, Department of Electrical Engineering, University of Southern California. <http://sipi.usc.edu/database/> (Last accessed on 20th January, 2011).

References

- [1] Tevaramani Saleem S et al. "Image steganography performance analysis using discrete wavelet transform and alpha blending for secure communication ", *Global Transitions Proceedings Volume 3, Issue 1, June 2022, Pages 208-214.*
- [2] Varuikhina Vladmir et al. "Continuous Wavelet Transform Applications In Steganography", 14th International Symposium on Intelligent Systems, *Procedia Computer Science 186 (2021) 580–587.*
- [3] Govindasamy V et al. "Coverless Image Steganography using Haar Integer Wavelet Transform ", *Proceedings of the Fourth International Conference on Computing Methodologies and Communication (ICCMC 2020) IEEE Xplore Part Number:CFP20K25-ART; ISBN:978-1-7281-4889-2*
- [4]. Houssein Essam H. et al. "An Image Steganography Algorithm using Haar Discrete Wavelet Transform with Advanced Encryption System", *Proceedings of the Federated Conference on Computer Science and Information Systems* pp. 641–644, DOI: 10.15439/2016F521, ACSIS, Vol. 8. ISSN 2300-5963, 978-83-60810-90-3/\$25.00 c 2016, IEEE.
- [5] Hui-Yu Huang et al. "A lossless data hiding based on discrete Haar wavelet transform", *CIT 2010, 978-0-7695-4108-2/10 \$26.00 © 2010, IEEE DOI 10.1109/CIT.2010.276*
- [6] Tushara M et al. "Image Steganography using discrete wavelet transform- A Review", ISSN: 2321-2004, Vol 3, Special Issue 1, February 2016, *International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering.*
- [7] Shrestha A et al. "Color Image Steganography Technique Using Daubechies Discrete Wavelet Transform", 9th International Conference on Software, Knowledge, Information Management and Applications (SKIMA), 2015.
- [8] Sengupta M. et al. "An Authentication Technique in Frequency Domain through Daubechies Transformation (ATFDD)" *International Journal of Advanced Research in Computer Science, Volume 3, No. 4, July- August 2012, ISSN No. 0976-5697.*
- [9] Lifang Yu et al "Improved Adaptive LSB steganography based on Chaos and Genetic Algorithm", *EURASIP Journal on Advances in Signal Processing, volume 2010, Article ID 876946.*
- [10] Khamrui, A et al., "A Genetic Algorithm based Steganography on Color Images (GASCI)" *International journal of Signal and Imaging Systems Engineering (IJSISE), 2014 Vol.7 No.1, pp.59 – 63, Inderscience publishers.*
- [11] Khamrui, A et al., "An Image Authentication Technique in Frequency Domain using Genetic Algorithm (IAFDGA)", *International Journal of Software Engineering & Applications (IJSEA), ISSN : 0975-9018 (Online),0976-2221(Print),Indexed on DOAJ,EBSCO,INSPEC,ProQuest etc.,DOI:10.5121/ijsea.2012.3504, Vol. 3, No. 5, pp.39-46, Sept. 2012.(<http://airccse.org/journal/ijsea/papers/3512ijsea04.pdf>),2012.*



- [12] Khamrui, A. et al. "A Genetic Algorithm based approach in image authentication using Z transform" (GAIAZT), AMSE Journals 2014 series: Advances B, Vol. 57,N⁰1, pp 20-30.
- [13] Khamrui A et al. , 'A Data Embedding Technique for Gray Scale Image Using Genetic Algorithm (DEGGA)', IEEE Sponsored International Conference on Communication, Computing & Security (Proceedings by Excel India Publishers ISBN-978-93-80697-505), NIT Rourkela, pp.19–22 7–9 January 2010.
- [14] Khamrui A.et al., "A Data- Hiding Scheme for Digital Image using Pixel Value Differencing (DHPVD)", International Symposium on Electronic System Design (ISED),Print ISBN:978-1-4577-1880-9, 19-21 December, Kochi, India, 2011.
- [15] Hashad A. I. et al "A Robust Steganography Technique using Discrete Cosine Transform Insertion" Information and communication Technology, 2005. Enabling Technologies for the New Knowledge Society: ITI 3rd International Conference.ISBN:0-7803-9270-1.
- [16] Khamrui A. et. al. "A Novel Genetic Algorithm Based Data Embedding Technique in Frequency Domain Using Z Transform (ANGAFDZT)", DPPR- 2012, Advances in Intelligent Systems and Computing, 177, ISSN No.:2194-5357, Springer, pp.885-893, July 13 -15, Chennai, India(2012).
- [17] Khamrui A., Mandal, J. K, "A spatial Domain Image Authentication Technique using Genetic algorithm", International Conference on Computational Intelligence, Communications, and Business Analytics, CICBA 2017, Computational Intelligence, Communications, and Business Analytics pp 577–584, Springer Link.
- [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/>(Last accessed on 20th January, 2011).
- [19] Mandal Jyotsna Kumar, "Reversible Steganography and Authentication via Transform Encoding", Studies in Computational Intelligence 901, Springer Nature.