PSO BASED OPTIMIZED SECURITY SCHEME FOR IMAGE AUTHENTICATION AND TAMPER PROOFING

K. Kuppusamy[1] and K. Thamodaran[2]

[1]Professor, [2]Research Scholar
[1,2] Dept. of Computer Science and Engineering
Alagappa University, Karaikudi-630003, Tamilnadu, India.
[1]kkdiksamy@yahoo.com ,[2]k_thamodharan@rediffmail.com

ABSTRACT

The hash function offers an authentication and an integrity to digital images. In this paper an innovative optimized security scheme based on Particle swarm optimization (PSO) for image authentication and tamper proofing is proposed. This scheme provide solutions to the issues such as robustness, security and tamper detection with precise localization. The features are extracted in Daubechies4 wavelet transform domain with help of PSO to generate the image hash. This scheme is moderately robust against attacks and to detect and locate the tampered areas in an image. The experimental results are presented to exhibit the effectiveness of the proposed scheme.

KEYWORDS

Image Authentication, dabechies4, hash function, PSO and tamper detection.

1. INTRODUCTION

An impact of information communication technologies and powerful digital image processing tools the multimedia contents such as digital images are easily manipulated and reused**.** Hashing techniques are playing vital role to ensure the authentication of multimedia contents, verify content integrity and prevent forgery. An image hash is a content-based digital signature of the image data. A secret key is used to extract certain features from the image data to generate image hash. This image hash is either by appended or embedded with host image by the sender. At the receiver side, the authenticator uses the same key to generate the hash values to compare with the transmitted hash for verifying its authenticity. Classification of image authentication techniques are broadly two types: watermark-based and hash-based signature techniques. Watermarking techniques embed imperceptible signal generated from the cover image to form a watermarked image. At the receiver, the extracted content based watermark from the watermarked image is used for authentication. A public key based watermark system that generates the watermark by calculating EX-OR of a bi-level watermark image and a hash value is obtained using MD5 from the original image [4]. An authentication system in which a content based watermark is generated from three level Haar wavelet decomposition using Sobel edge detection and then the hash is computed using MD5 and embedded in the middle frequency coefficients[8]. Content-based spatial domain image authentication scheme using the advantages of cryptography and

David C. Wyld (Eds) : ICCSEA, SPPR, CSIA, WimoA - 2013
pp. 143–152, 2013. © CS & IT-CSCP 2013 DOI : 10.5121/csit.2013.3515

imperceptibility feature of digital image watermarking. The secret key is used to generate watermark based one-way hash function. Each bit of watermark is embedded into respective blocks of the original image, in raster scan order[17]. An optimized frequency domain watermarking based image authentication scheme using DCT, GA and PSO. This scheme hybrids PSO with Cauchy mutation and natural selection strategy based on roulette wheel selection to reduce its tendency of trapping into local minima and avoid the premature convergence of the standard PSO[18]. An optimized frequency domain watermarking based image authentication scheme using Z transformation and GA. In this scheme a 2×2 mask is considered from the source image in row major order. New Generation is tracked by Crossover and Mutation are applied[19].

Hash based techniques are differed from the watermark based techniques in an image authentication. An image hashing techniques are extract a set of features from the image to form a compact representation that can be used for authentication. The advantages of hash based techniques are no distortion is introduced in the image to be authenticated and content hash generated in frequency domain which has more robust to geometric distortions compared to their spatial domain counterparts. Several hash based signature techniques have been available. These techniques use data from different domains such as DCT coefficients [7], [9], Wavelet transform coefficients [3], [10] and Fourier transform coefficients [12], Daubechies wavelet transform[1] to generate the signature. An authentication technique based on DCT coefficient relationship in which the DCT coefficients are first scaled and quantized. Then, a binary string is generated which serves as the content hash[2]. A geometric distortion resilient image hashing scheme is proposed for copy detection and authentication with help of low frequency components of an image in wavelet domain. DCT based hash extraction method is employed to create a short binary hash sequence [3]. Content-based spatial domain image authentication scheme is suggested by Ee-Chien Chang et al.. In this scheme the signature is generated from the result of an extremely low-bit-rate content based compression which is guided by a space-variant weighting function whose values are higher in the more important and sensitive region. This scheme is robust against image processing distortions like low-pass filtering, JPEG compression and tampering[6]. A JPEG-tolerant image authentication system which constructs a Message Authentication Code incorporating a number of feature codes that are used to protect regions of interest in an image[9]. An authentication scheme is competent to resist all distortions that may be introduced by JPEG2000 compression. The feature extraction is applied after the EBCOT process. This encoded information is encrypted with ECC algorithm to form a digital content based signature [11]. An algorithm for generating an image hash based on Fourier-Mellin transform features which are invariant to two-dimensional affine transformations and incorporates key-dependent outputs to form a secure and robust image hash [12]. Frequency domain image authentication scheme using DFT is offered. In this scheme transformed values are generated using DFT sub matrix has been engaged from source image matrix as a window and authenticating message bits are embedded within the real part of the transformed data. The size and content of authenticating message and MD-5 key is embedded to the transformed source [14]. An authentication scheme using DFT to generate hash features. An innovative idea is employed to use the hashing technique in CBIR. The hash value generated and is utilized for extracting the images similar to query image from the large image database. Performance of the work is measured by means of hamming distance [16]. In this paper the content based frequency domain optimized authentication scheme based on the daubechies4 wavelet transform and PSO is proposed. The results of experimentation on the robustness of the proposed scheme to unintentional manipulations like lossy compression, noise, filters and sensitivity to intentional attacks like insertions, crop, rotations are also presented.

The section organization of this paper is offered as follows. Section 2 provides the information concerning particle swarm optimization techniques. Section 3 illustrates our proposed optimized image hashing scheme anchored in daubechies4 wavelet transform and PSO. The formula for Completeness of Signature(CoS) as measure of performance is given in section4. The

experimental outcomes and security assessment are presented in Section 5 and Section 6 finish off this paper.

2. PARTICLE SWARM OPTIMIZATION

An evolutionary computation scheme known as PSO has developed by Kennedy and Eberhart [13]. A particle swarm optimization technique is shaped from the imitation of the social behaviour of bird flocks. Swarm Intelligence is an ingenious distributed intelligent conception to solve optimization problems that initially regard as its motivation from herding phenomena in vertebrates [5]. In PSO scheme, the particle is regarded as a bird in the search space to generate a solution. Every particle establish the direction and distance of the next move with respect to velocity and optimized function which decides a fitness function. The scheme tracks the optimal particle at present in the solution space. In modified particle swarm optimization algorithm, every particle fix on its inertial factor concurrent to the nearer degree between the fitness of itself and the optimal particle [15]. Each particle makes effort to amend its position with regard to consequent information:

- the space between the present position and position of particle best
- the space between the present position and position of global best

This amendment can be represented by the concept of velocity. The amendment of velocity of each agent is performed with help of equation (1) in inertia weight approach (IWA).

$$v_{k+1} = w * v_k + c_1 * r_1 * (p_k - x_k) + c_2 * r_2 * (g_k - x_k) \quad (1)$$

where,w –non negative inertia factor, v_k - velocity of particle , x_k - present position of particle, c_1-determine the relative influence of the cognitive component, c_2- determine the relative influence of the social component, p_k - *pbest* of particle , g_k - *gbest* of the group, r_1, r_2 - the population is getting diversity with help of random numbers and are consistently distributed in the interval [0,1]. The particle make a decision to move to next position by means of equation (1) and regarding its own experience, which is the memory of its best earlier position, and the practice of its most successful particle in the swarm. The particle explores the solution in the problem space in the range of [−s, s]. The particle updating its position by means of equation (2).

$$x_{k+1} = x_k + v_{k+1} \quad (2)$$

3. PROPOSED OPTIMIZED IMAGE AUTHENTICATION SYSTEM

The proposed security scheme for image authentication and tamper proofing is developed with help of on the daubechies4 transform and particle swarm optimization (PSO). The 256 bit secret key is incorporated. daubechies transform outputs to form secure and robust 512 bit image hash using SHA-512. In the process of hash generation, the daubechies4 wavelet transformed sub bands LL, LH, HL are considered. According to LL, all coefficients are considered for feature generation and PSO optimization with 256 bit secret key is used to select high energy coefficients to generate hash features from 8x8 non-overlapped blocks of LH, HL sub bands. In this paper, an inventive idea is used to adjust the inertial factor adaptively is proposed. Every particle prefers its inertial factor concurrent to similar degree between the fitness of itself and the optimal particle. A particle decides minor inertial weight to identify its better fitness value and a particle decides bigger inertial weight to identify its poorer fitness. The proposed scheme utilize this tactic

to search in large scope and the estimated location of the optimal solution is established rapidly and search in small scope in the behind iterations so that the correct solution is established. A random number(rn) is used in evaluating the inertia weight in the algorithm in order to jump out from local optimum and a minimum inertial weight factor is used to prevent the premature convergence. Considering a maximization problem, the inertial factors of the particles are updated according to equation(3). Fitness function f(x) for PSO training is given in equation (4).

$$w_m = \frac{rn}{pm}\left|\frac{f_{cp} - f_{opc}}{f_{opc}}\right|, \quad \text{if } w_m > w_0 \text{ then } w = w_m, \quad \text{if } w_0 > w_m \text{ then } w = w_0 \quad (3)$$

where, rn-random number, pm-Parameter, f_{cp} -fitness of current particle, f_{opc} -optimum particle currently.

$$\text{Fitness Function } f(x) = \frac{1}{n}\sum_{i=1}^{n} COS_i \quad (4)$$

3.1 PSO Algorithm

Step 1 Generate randomly the initial position and velocity of the particles within predefined ranges.

Step 2 At each iteration, the velocities of all particles are revised according to equation(1)where w will be gained based on equation(3).

Step 3 The positions of all particles are revised according to equation(2). After revising, x_k should be checked and limited to the allowed range.

Step 4 Update pbest and gbest when condition is met according to equation(5),

$$\text{if } f(p_k) > \text{pbest, then pbest} = p_k$$

$$\text{if } f(g_k) > \text{gbest, then gbest} = g_k \quad (5)$$

where f(x) is the objective function to be optimized.

Step 5 The algorithm repeats steps 2 to 4 until certain terminating conditions are fulfilled, such as a pre-defined number of iterations. Once stopped, the algorithm reports the values of gbest and f(gbest) as its solution.

3.2 The Hash Generation Procedure for Daubechies4 Domain and PSO

Step 1 Perform daubechies4 on the host image I to decompose it into four non-overlapping multi- resolution coefficient sets: LL1, LH1, HL1 and HH1.

Step 2 Perform Daubechies4 again on LL1 coefficients sets to get four coefficient sets: LL12, LH12, HL12 and HH12.

Step 3 Generate the secret key sk.

Step 4 Form feature vectors using all coefficients of daubechies4 transformed LH12, HL12 and HH12 coefficient sets and select high energy coefficients of LH1, HL1 coefficient sets with help of particle swarm optimization.

Step 5 Compress the feature vector in required length using SHA-512.

Step 6 Concatenate the hash bits generated to form the final hash H.

Step 7 Perform entropy coding and obtain I^*.

3.3 The Hash Extraction Procedure.

Step 1 Perform daubechies4 on the host image I^* to decompose it into four non-overlapping multi-resolution coefficient sets: LL1, LH1, HL1 and HH1.
Step 2 Perform daubechies4 again on LL1 coefficients sets to get four coefficient sets: LL12, LH12, HL12 and HH12.
Step 3 Generate the secret key sk.
Step 4 Form feature vectors using all coefficients of daubechies4 transformed LH12, HL12 and HH12 coefficient sets and select high energy coefficients of LH1, HL1 coefficient sets with help of particle swarm optimization.
Step 5 Compress the feature vector in required length using SHA-512.
Step 6 Concatenate the has bits generated to form the final hash H*.
Step 7 Compare the generated hash H* with the received hash H and compute the CoS value. If the CoS value > 0.75, then declare the image to be authentic else declare the image to be unauthentic and return the tampered block numbers.

4. MEASURES OF PERFORMANCE

4.1. Completeness of Signature (CoS)

The proposed technique produces a PSO based optimized hash code or a digest using user defined key value. The computed optimized hash value is then transmitted to the receiver along side with the compressed image. An optimized hash code is created from the received image and compared with the received hash regarding Completeness of Signature (CoS) which is stated by the equation(6) .

$$CoS = \frac{(F_m - F_n)}{F_t} \tag{6}$$

where F_m denotes the number of feature vectors that match, F_n is the number of feature vectors that do not match and F_t is the total number of feature vectors that are considered for generating the optimized hash code. The received image is declared as authentic when the fixed condition is fulfilled otherwise unauthentic.

5. EXPERIMENTAL RESULTS AND SECURITY ANALYSIS

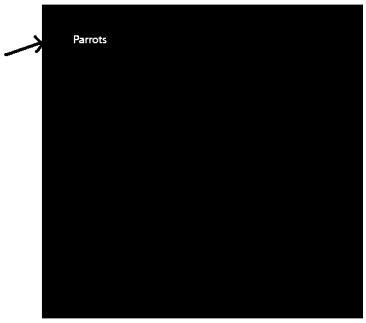
In this proposed optimized image authentication system experiments, more than 100 standard images of size (512 × 512) are used for training and testing processes. In the process of hash generation, the daubechies4 wavelet transformed sub bands LL, LH, HL are considered for generating hash features. According to LL all coefficients are considered for feature generation and PSO optimization with 256 bit secret key is used to select high energy coefficients to generate hash features from 8x8 non-overlapped blocks of LH, HL sub bands. The parameters $p = 20$, $r_1 = 1$, $r_2 = 1$, are used. Results are presented for two categories, namely without PSO and with PSO using unintentional attacks compression, noise and filters and intentional distortions such as cropping, insertions. Resultant images of proposed scheme are given in figure(1) and figure(2).

(a)Parrots-Original

(b) Compression 10%QF

(c) Gaussian Noise 5%

(d) Text introduced at the top left portion



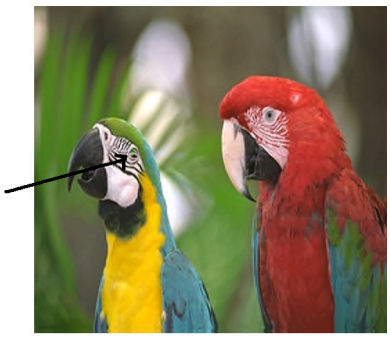
(e) Tampered Region of (d) indicated by arrow

Figure1. Results After Various Incidental and Intentional Distortions on Parrots Image Without Using PSO

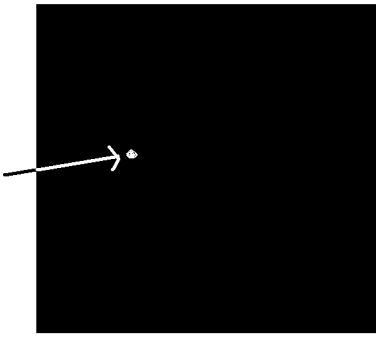
(a) Compression 10%QF

(b) Gaussian Noise 5%

(c) Median Filter 3PR

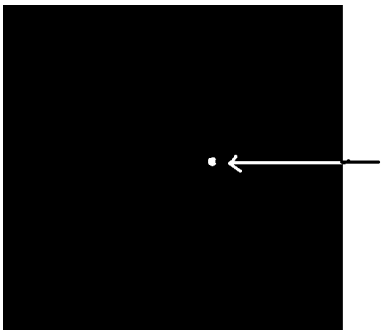


(d) Left eye of parrot-1 rotated



(e) Tampered Region of (d) indicated by arrow

(f) Mouth Center portion of parrot-2 cropped



(g) Tampered Region of (f) indicated by arrow

Figure. 2. Results after Various Incidental and Intentional Distortions on Parrots Image Using PSO

The correlation between the embedded and extracted hash features are measured by the metric called completeness of signature(CoS) regarding equation(6) to identify whether the received image is authentic or not. If the (CoS >= 0.75) then the received image is authentic, otherwise unauthentic. The CoS values and authentication results after incidental distortions on parrots image are offered in table 1. The CoS values and authentication results after intentional distortions on parrots image are offered in table 2. Also the tampered regions recognized are given in table (2) and tampered regions are indicated by arrow.

Table 1. Authentication Results after Incidental Distortions on Parrots Image

Attacks	Parameter	Completeness of Signature(CoS)			
		WOPSO		PSO	
		COS	A/UA	COS	A/UA
Without Attack	----	0.9492	A	0.9648	A
JPEG comp	QF= 10	1.0000	A	1.0000	A
Gaussian Noise	Noise= 5%	0.9751	A	1.0000	A
Uniform Noise	Noise=10%	0.9532	A	0.9688	A
Salt and Pepper	Noise=10%	0.9727	A	0.9844	A
Low pass Filter	STD Devi=10	0.9843	A	1.0000	A
Median Filter	Radius=3pixels	0.9492	A	1.0000	A
Sharpening	----	0.9453	A	0.9727	A
Gamma Correction	Gamma value= 3	0.9649	A	0.9921	A

QF- Quality Factor , A – Authentic , UA – Unauthentic

Table 2. Authentication Results on Intentionally Tampered Parrots Image

Intentional Distortion	Completeness of Signature(CoS) and Authentication					
	WOPSO			PSO		
	COS	A/UA	Tampered Blocks	COS	A/UA	Tampered Blocks
Text Parrots introduced at the top left portion	-0.7148	UA	(0,0), (0,1)	-0.7657	UA	(0,0),(0,1), (1,0), (1,1)
Left eye of parrot-1 rotated	-0.8007	UA	(2,3)	-0.8265	UA	(2,3)
Mouth Centre portion of parrot-2 cropped	-0.7382	UA	(4,3), (5,3)	-0.7618	UA	(4,3),(5,3)

A – Authentic , UA – Unauthentic

6. CONCLUSION

In this paper the optimized robust image authentication technique with the daubechies4 wavelet based transformation and PSO are proposed. The high energy coefficients are selected and used to form the feature vector with help of 256 bit secret key. The system selects the high energy coefficients among the daubechies4 based transformed coefficients to generate the hash code which is robust to incidental distortions. From the experimental results it is evident that, the proposed scheme is effective in discriminating incidental distortions from intentional distortions. The proposed scheme is compared with their daubechies4 based transform without PSO and it is observed that the proposed PSO based scheme is more robust to Gaussian noise ,low pass and high pass filters than the Daubechies4 based transform without PSO schemes. It is found that the proposed scheme based on PSO offers better tolerance to incidental distortions than the daubechies4 based transform without PSO. It is also found that the proposed scheme based on PSO offers better results in intentionally tampered images than the daubechies4 based transform without PSO and both schemes are better in detecting the tampered regions.

REFERENCES

[1] Arne Jense and Anders la Cour-Harbo, (2001) "Ripples in Mathematics: the Discrete Wavelet Transform", Springer publications.

[2] Chai Wah Wu. . (2002) "On the design of content-based multimedia authentication systems", IEEE ransactions on Multimedia. Vol. 4, No. 3, pp 385-393.

[3] Chang C., Hwang K. F. and Hwang M.S.. (2002) "Robust authentication scheme for protecting copyrights of images and graphics", Proceedings of IEEE conference on Visual Image and Signal Processing. Vol. 149, No.1, pp 43-50.

[4] Wang Y.,Doherty and Van Dyck R. E., (2002) "A wavelet-based watermarking algorithm for ownership verification of digital image", IEEE Transactions on Image Processing, Vol.11, No.2, pp 77-88.

[5] Clerc M and Kennedy J, (2002) " The particle swarm-explosion, stability, and convergence in a multidimensional complex space", .IEEE Transactions on Evolutionary computation, vol. 6(1), pp 58-73.

[6] Ee-Chien Chang, Mohan S. Kankanhalli, Xin Guan, Zhiyong Huang, YinghuiWu, (2003) "Robust image authentication using content based compression. Multimedia Systems", Springer-Verlag., pp 1-10.

[7] Chun-Shien Lu and Chao-Yong Hsu., (2004) "Geometric distortion-resilient image hashing scheme and its applications on copy detection and authentication.

[8] Shensheng Yu, Yuping Hu and Jingli Zhou, (2004) "Content-based watermarking scheme for image authentication", Proceedings of the 8th International Conference on Control, Automation, Robotics and Vision, Kunming, China, pp1083-1087.

[9] Takeyuki Uehara, Reihaneh Safavi-Naini and Philip Ogunbona, (2004) "A secure and flexible authentication system for digital images", Multimedia Systems, Springer Verlag, Vol. 9, pp 441-456.

[10] Fawad Ahmed and M.Y. Siyal.,(2005), "A secure and robust hashing scheme for image authentication", .Proceedings of the IEEE International Conference on Information, Communication and Signal Processing, pp 705-709.

[11] Sun Q, Chang SF, (2005) "A secure and robust digital signature scheme for JPEG 2000 image authentication", IEEE Transactions on Multimedia, vol 7(3), pp 480–4 94.

[12] Ashwin Swaminathan, Yinian and Min Wu, (2005) " Robust and secure image hashing", IEEE Transactions on Information Forensics and Security, Vol. 1, No. 2, pp 215-229.

[13] Maurice Clerc, (2007) Particle Swarm Optimization, ISTE publishers, First South Asian Edition.

[14] Nabin Ghoshal, Jyotsna Kumar Mandal (2008), " A Novel Technique for Image Authentication in Frequency Domain using Discrete Fourier Transformation Technique", Malaysian Journal of Computer Science, Vol. 21(1), pp 24-32.

[15] Jinrong Zhu (2009), "A Modified Particle Swarm Optimization Algorithm" Journal of Computers, Vol. 4, No. 12, pp 1231-1236.

[16] H. B. Kekre, Dhirendra Mishra, (2009) "Image Retrieval Using Image Hashing", Techno-Path: Journal Of Science, Engineering & Technology Management, Vol. 1 No.3.
[17] Sarabjeet S. Bedi, Shekhar Verma and Geetam Tomar, (2010) "An Adaptive Data Hiding Technique for Digital Image Authentication", International Journal of Computer Theory and Engineering, Vol. 2, No. 3, pp 338-344 .
[18] Sawsan Morkos Gharghory, (2011) " Hybrid of Particle Swarm Optimization with evolutionary operators to fragile image watermarking based on DCT", International Journal of Computer Science and Information Technology, Vol 3, No 3, pp 141-157.
[19] J.K.Mandal, A.Khamrui, (2012) "An Image Authentication Technique in Frequency Domain using Genetic Algorithm", International Journal of Software Engineering and Applications, Vol.3, No.5, pp 39-46.

Authors

Dr.K.KUPPUSAMY is working as Professor in the Department of Computer Science and Engineering, Alagappa University, Karaikukdi, Tamilnadu, India. He has received his Ph.D in Computer Science and Engineering from Alagappa University, Karaikudi, Tamilnadu. He is having rich teaching P.G.experience about 27 years in ever growing Computer Science field. He is guiding more Mphil., and P.hD., scholars. He has Presented many research papers in the National and International conferences and published many research papers in National and International Journals. His areas of research interest includes Information/Network Security, Algorithms, Neural Networks, Fault Tolerant Computing, Software Engineering and Testing and Optimization Techniques.

K.THAMODARAN is a research scholar in the Department of CSE, Alagappa University, Karaikukdi, Tamilnadu, India. He has received his M.Sc(CS) degree and M.Phill(CS) degree from Bharathidasan University, Trichy, TamilNadu, India. He is having teaching experience around 21 years. He has published 4 research papers in International Journals and presented 6 papers in the National and International conferences. His area of interest includes Network Security, Image Security and Optimization Techniques.