International Journal of Security and Its Applications
Vol. 12, No. 2 (2018), pp.1-8
http://dx.doi.org/10.14257/ijsia.2018.12.2.01

An Invisible Image Watermarking Based On Modified Particle Swarm Optimization (PSO) Algorithm

Atheer Bassel[1, 2], Md Jan Nordin[1] and Mohammed B. Abdulkareem[3]

[1,2] Center for Artificial Intelligence Technology, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, 43600 Bangi, Selangor Darul Ehsan, Malaysia
[2]Computer College, University of Anbar, Al Anbar, Iraq
[3] Department of Computer Engineering and Technology, Almaaref University College. Al Anbar, Iraq
atheerbassel@siswa.ukm.edu.my, jan@ukm.edu.my and f_com22@yahoo.com

Abstract

Tradeoff between the embedding energy of watermark and the perceptual translucence and the image fidelity following attacks represent an important issue in watermarking images. The present work introduces a brand new invisible watermarking algorithm grounded on modified Particle Swarm Optimization (PSO) algorithm with Human Visual System (HVS) model into consideration. The purpose was to improve the ownership and imperceptibility of image. In PSO invisible watermarking, the global and local characteristics of the host as well as watermark images within the Singular Value Decomposition (SVD) domain were utilized. The experimental results of Modified PSO (JPSO) algorithm demonstrate high PSNR values for the watermarked images, while the watermark remains invisible under numerous signal processing, in particular, the attack of watermark removal (also, adaptive watermarking in the different types of attacks).

***Keywords**: Digital watermarking, singular value decomposition (SVD), jumping particle swarm algorithm (JPSO), false positive problem*

1. Introduction

Nowadays, with pervasive growth of internet and increasing the speed of communication networks, websites and social networks are used in human's real life as some of the basic tools. These applications provide users with easy access to digital assets such as images, videos, sounds, *etc*. So they can buy and sell or copy the digital media without the permission of their owners. Therefore, the protection of ownership rights of digital media has become a challenge for content producers. One of methods of dealing with this issue is digital watermarking. Digital watermarking is embedding a piece of digital copyright information in the media that can be a logo or a pseudo random sequence. Watermarking is one of the solution to prevent unauthorized use of digital media. This solution can help the protection of ownership rights by embedding the copyright information in the intended media.

Image watermarking can be authentication within the spatial and the transformed domains for the detection of the tamper regions in watermarked image. The systems of transform domain are clearly more robust and secure as opposed to those of spatial domain schemes[1]. For every technique of image steganography, Imperceptibility, ability to embed, robustness against attacks and resistance to Steganalysis, are critical parameters of design[2]. In steganalysis, there are diverse statistical approaches to deal with, in order to break steganography algorithm. However, development in information theory and

Received (August 23, 2017), Review Result (November 20, 2017), Accepted (November 24, 2017)

ISSN: 1738-9976 IJSIA

techniques of coding has generated the system of steganography that are more flexible and robust against numerous operations of imageto processing. It is important to achieve a sound trade-off between capacity, imperceptibility and robustness, for instance, when embedding capacity is increased, imperceptibility may degrade, making intruder suspect secret message is present [1,2].

The two alternatives for the addition of a watermark to a digital image are the visible mark and the imperceptible mark. Visible watermarks impact an image in terms of its commercial. However, this paper will consider this option. An example of visible watermark can be found in company logos. On the other hand, the imperceptible marks comprise the side information placed imperceptibly, typically alongside certain perceptual model. The imperceptible mark can be added either with or without the host image partition into blocks. This enables the embedding of more than one bit. In addition, within the spatial domain, the encoding is performable through direct change of pixel values. The transform domain maps image to other domain. Then, the domain's coefficients are changed to become Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT) as well as Singular Value Decomposition (SVD). According to [3], the method of transform domain appears more robust against diverse types of attacks as opposed to the spatial domain.

As for reference watermarks, those explored in an arbitrary image is easily discoverable by attackers. This strategy has led to the problem of false positive, when certain watermark was embedded. Here, the attacker can simply attest the ownership of the arbitrary watermarked image with no awareness with respect to the initial watermark that is embedded in the host image. Therefore, the false positive rate for this application should be approximately zero and that proof of ownership cannot otherwise be reliable. Another problem in ownership identification occurs in a situation where only scalar value of the scaling factor is employed in this trustworthy SVD- based image watermarking [4]. Employing the small value for scaling factor, the watermark's invisibility attained high peak signal to noise ratio (PSNR) of the watermarked image. However, the watermarked image is not as robust when there are some common attacks. The factor of scaling highly contributes to the control of the watermark images in terms of transparency and robustness [5]. It is worth mentioning that high scaling factor results in unacceptable watermarked image quality, and yet the watermark remains robust [4].

In addition, this work will provide more information for the false positive, false negative and scaling factor. The drawback for defining the false positive and false negative should be taken into account; the false position means false watermark detection while false negative denotes failure in detecting the already available watermark. In this work, a simple model is employed to enable an analysis for the estimation of the distribution of probability of false positive as well as false negative for the technique proposed. In short, correlation coefficient (CC) is to be employed in order to ascertain the degree of similarity between the original and extracted watermark image. The problem of false positive that emerges in nearly all the SVD-based algorithms caused by the fact that there is only the process of embedding watermark into the original image [5].

The scaling factor is very important applying with optimization because a decrease in the scale factor value during the optimization process can generate high quality final outcome [6]. The scaling factor in the proposed watermarking scheme employs control on the tradeoff between the imperceptibility and robustness [7].

Conflict requirements do occur between the watermarked image quality and robustness in the system of watermarking. Thus, increasing the robustness of watermarking ill negativel impact the quality of watermarked image. In relation to this, there have been some recommendations from past studies for overcoming this problem. One study recommended the use of heuristic weight which was developed based on is human vision system (HVS).

Thus, based on the above, this work aims to:

1. Propose a PSO for the embedding part of our process to make the system more robust.

2. Propose how the PSO can define the chromosome (the population) and define the fitness function (objective) based on watermarking evaluation under the number of maximum iteration.

3. Perform evaluation and comparison with state of the art methods.

Following the introducing section, section 2 iproceeds with the review of algorithms for image watermarking in the transform domain, section 3 highlights the PSO and JPSO algorithm, section 4 contains the elaboration on the proposed method, section 5 reports the experimental results and finally, section 6 provides the study's the conclusion.

2. Singular Value Decomposition (SVD)

Singular value decomposition comprises a linear algebra technique for symmetric matrix diagonalization. A digital image is also a form of a matrix of integer numbers. As such, SVD is performable on digital images right away. The techniques of traditional transform including DFT, DCT and DWT just decompose a signal with respect to a standard basis set. In some sense, this is not an optimal representation. The attractive properties and unique features of SVD includes its stability with little disturbance. This is why SVD has been employed in numerous applications of signal processing. SVD is also a type of orthogonal transform and a numerical technique to diagonalize matrix, and thus, it can be used as a technique for linear algebraic within the transformed domain which contain foundation states, which, in some sense, are optimal. SVD decomposes a specified matrix into three factions: left singular matrix U, right singular matrix V and singular matrix S, on an image size A with size (M × N). The expression is presented as the following [11].

$$A=USV^T \tag{1}$$

Matrix S comprises just the diagonal element and termed as singular values. it contains the singular values in downward sequence. Meanwhile, matrix U and V comprise the image's decomposed and detailed information. providing that A represents the rectangular matrix of the order (n × n), matrix S is thus allowed to contain maximum n diagonal elements. In general, elements (S) symbolize the involvement of every layer of decomposed image within the final image formation [11]. The parent matrix (A) is reproducible using the smaller elements of matrix s.

$$\boldsymbol{A=USV^T}=\begin{pmatrix} u_{1,1} & \cdots & u_{1,M} \\ \vdots & \ddots & \vdots \\ u_{M,1} & \cdots & u_{M,M} \end{pmatrix} \times \begin{pmatrix} s_{1,1} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & s_{M,N} \end{pmatrix} \times \begin{pmatrix} v_{1,1} & \cdots & v_{1,N} \\ \vdots & \ddots & \vdots \\ v_{N,1} & \cdots & v_{N,N} \end{pmatrix}^T = \sum_{i=1}^{m}\sum_{j=1}^{n}\sum_{k=1}^{n} u_{i,k} \times s_{k,k} \times v_{k,j} \tag{2}$$

Where: U denotes a (M × M) matrix, V denotes a (N × N) matrix and S denotes a (M × N) diagonal matrix with positive elements from the first to ending row in downward order. The diagonal elements of S are termed SVs of A, which are nonnegative and they are presumed to be downwardly organized. This fulfils the relation equation (2) where r denotes the matrix rank.

$$S_{1,1} \geq S_{2,2} \geq \ldots\ldots \geq S_{r,r} \geq S_{r+1,r+1} = S_{r+2,r+2} \ldots\ldots = S_{M,N} = 0 \tag{3}$$

In watermarking that is grounded on SVD, a signal is treatable as a matrix and decomposed into three matrices. The SVD computation involves the discovery of the eigenvalues as well as of the eigenvectors of AA^T and A^TA. The eigenvectors of A^TA comprise the columns of matrix V and the eigenvectors of AA^T consist of the columns of matrix U.

3. Particle Swarm Optimization Algorithm (PSO)

PSO is classified as a stochastic metaheuristic optimization method based on swarm intelligence (SI) [8], [15]. Each particle denotes a candidate solution that is improved based on its own experiences and those of its neighbors. PSO is a population-based algorithm. It uses a group of individuals in the search process. Both swarm particles and individuals will be optimized based on their velocity, past experience, as well as the experience of their neighbors. The problem search space is sought by PSO by adapting the paths of travelling particles within a multidimensional space.

In the context of PSO, a population of n solutions is represented as a swarm of n particles. i^{th} particle in the swarm is denoted within d-dimensional space with a position in the search space $x_i = (x_{i1}, x_{i2}, . . . , x_{id})$ and velocity $v_i = (v_{i1}, v_{i2}, . . . , v_{id})$, where d is the number of dimensions. The method of standard PSO updates every particle's velocity and position as in equations.

$$v_{id}(t+1) = w \times v_{id}(\mathrm{t}) + \mathrm{c}_1 \times r_1 \times (\mathrm{p}_{id} - x_{id}) + \mathrm{c}_2 \times r_2 \times (\mathrm{p}_{gd} - x_{id} \tag{4}$$

$$x_{id}(t+1) = v_{id}(t+1) + x_{id}(t) \tag{5}$$

Where c_1 and c_2 denote two positive acceleration constants; r_1 and r_2 are arbitrary numbers in (0, 1); p_{id} and p_{gd} denote the superior positions identified according to the i^{th} particle and each particle respectively; t denotes the current iteration number; while w represents an inertia weight that usually decreases during the run of the algorithm in linear form. W is responsible for balancing the local and global searches.

Initially, PSO was created as a solution for solving continuous optimization problem, whereas a variant known as discrete particle swarm optimization (DPSO) was first introduced by Kennedy and Eberhart [8]. A DPSO algorithm known as Jumping Particle Swarm Optimization (JPSO) algorithm has been introduced recently [9]. The algorithm was created as a solution for combinatorial optimization problem. JPSO algorithm delineates different jumps (moves) for particles to enable movment from one position to another within a discrete hyper-space with no application of velocity concept [9]. For our knowledge, this is the first work that implemented JPSO with watermarking problem. The idea underpinning JPSO: a group of individual's agent search that crosses a discrete space concurrently moving from one solution to another without plummeting in intermediate position, and this emulates the natural behavior of a group frogs in a pool jumping from one stone to another [9,10]. JPSO keeps the original PSO's conspt of simplicity while running on a discrete search space; this is major of advantages of JPSO. JPSO can be an effective candidate for tackling complex engineering optimization problems. Thus, this paper attempts to formulate a JPSO algorithm for solving the problem of digital image watermarking.

4. The Proposed Method

The present section illustrates the steps of the scheme proposed. The DWT-SVD with JPSO has been used in different application and performance of the DWT-SVD scheme and JPSO demonstrated better performance as opposed to the methods used in the past in each specific application. The JPSO algorithm searches its population to obtain the best solution using each and every potential combination of the DWT-SVD sub-bands togather with factors of watermark amplification. It is important that the strength of the watermark or the amplification factor is optimized because doing so will result in algorithmthat is robust against attacks. In the proposed JPSO with watermarking, firstly, we deal with the scenario as a set of solution in one population as optimization problem. Secondly, we calculate the fitness for each solution in my fitness including the image, watermark, attack image, extracted watermark and input parameter for DWT-SVD and JPSO. Finally, we compute the correlation between the original and extract watermark and the Peak Signal to Noise Rate (PSNR), between the original image and after embedding image.

The procedure of the proposed technique as the following, first, our technique finds the best solution in the population based on the objective function. Second, the algorithm will start the optimization process based on the JPSO procedure and update the population by adding the best solution obtained and delete the worst solution in the population.

For the embedding watermarking by using the JPSO generate the initial population by random. Here, each solution is a row vector of size $m \times m$ which equals to the watermark size. After this, for each solution i of the JPSO population, the execution of the watermark embedding algorithm is expressed as:

$$S' = S + \delta * Sw \tag{6}$$

Where δ is the scaling factor.

The procedure of extracting watermark by JPSO is as following:

1- Apply T type's image processing attacks on the signed image I' which meanes apply one by one types of attacks. This produces T different types of attacked watermarked images for the signed image *I'*.

2- Experform watermark extraction from the attacked watermarked image.

3- Compare the PSNR between the original image I and the signed image I' and the values of correlation for attacked image.

4- compute JPSO's objective value utilizing the objective function as expressed below:

$$\textit{Objective function} = PSNR + 100 * \textit{correlation} \tag{7}$$

Where: the correlation comprises the normalized cross-correlation between the original and the extracted watermark from each attacked signed image.

5- Choose the individuals that have the best fitness values.

6- Create new population using the chosen individuals.

7- Repeat the operations until the stopping criteria, which is the maximum amount of iteration (MAX-it) is achieved.

5. Experimental Results and Discussion

This section illustrates the assessment of performance of the recommended system of watermarking and comparison with state-of-the-art algorithms. In this experiment, the host images with size 512 × 512, (gray scale image) and 50x20 grey scale image alongside the 'copyright' watermark for owner's signature are to be used. Our proposed, show in Figure 1, where the PSNR of our method was 51.21dB.

All the systems take into account the exact size of the host image and watermark images for the experimental analysis. MATLAB is used for coding of the system while the execution is performed using a personal computer (Intel Pentium (R) Core i5 CPU at 3.40 GHz with 4 gigabyte RAM), running on windows 10 operating system (64-bit).

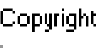
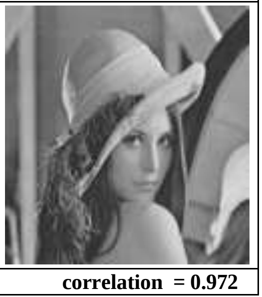
Original image	Waterm ark	Original image + watermark
		
The (PSNR) = 51.218		**correlation = 0.972**

Figure 1. Embedding Watermark with Orignal Image using SVD-JPSO

As shown the literature, the imperceptible by way of objective process is performed by taking into account the quantitative index, peak signal to noise ratio (PSNR).

$$PSNR = 10.log_{10}\left(\frac{MAX^2}{MSE}\right) \tag{8}$$

Where: the Mean Square Error (*MSE*) represents the aggregate squared error amid the altered and the actual image. Meanwhile, PSNR represents the peak error measure while MAX denotes the highest pixel's value.

For the robustness watermark under types of attacks, normalized correlation (*P*), is employed in the similarity assessment between the original watermark (*w*) and the extracted watermark (*w'*) as expressed below:

$$\boldsymbol{P(\mathbf{W}, \mathbf{W}') = \frac{\sum_{i=1}^{N} w_i w_i'}{\sqrt{\sum_{i=1}^{N} w_i^2 \sum_{i=1}^{N} w_i'^2}}} \tag{9}$$

Where: ρ represents the introduced watermark w and abstracted watermark $\hat{w}$ in terms of correlation while *N* denotes the watermark image's measure.

In addition, the probability of the detection of false watermark is expressed as:

$$\boldsymbol{P_{fp} = p\{NC(W, W^{'}) \geq T_p | no\ watermark\}} \tag{10}$$

Where: *p{A|B}* denotes the probability of event A given that event *B*, *Tp* entails a threshold. Since *w(i)* and *w'(i)* are either *0* or *1*, respectively, $w^2(i)$ and $w'^2(i)$ are either *0* or *1*.

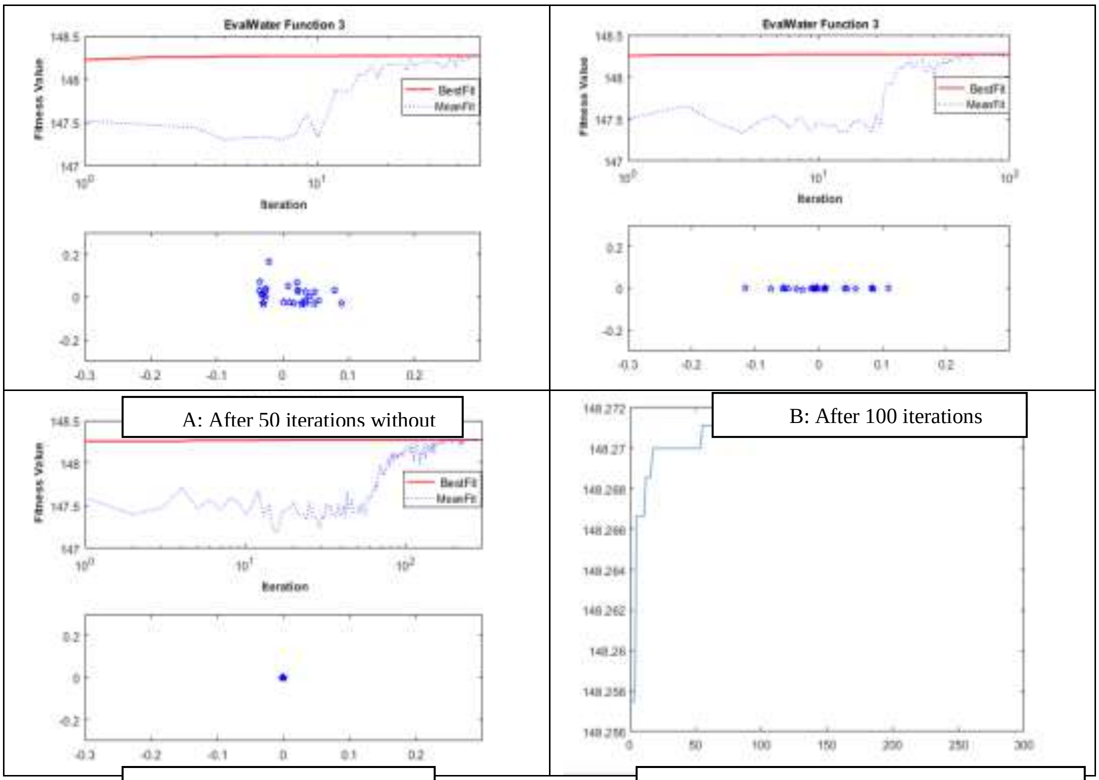
For direct comparison between the proposed method and the algorithm illustrated above [12] the author calculate the PSNR, the ratio for the PSNR (Lena image) was 45.12dB. Wang *et al.* 2011[14] the rate for the PSNR was 47.49dB, and the correlation was 0.99. The [13] proposed a GA based on discrete cosine transform (DCT), the PSNR was 34.79dB, and the correlation was 0.74.

In the Table 1, in our method the SVD-JPSO was the good result when compare with different algorithm that using the gray scale (Lena) image for testing and analysis the experimental result.

Table 1. Comparison of the Proposed Methods with other Techniques based on PSNR for Lena Image

#	Algorithm Symbol	reference	
1	DCT-GA	(Shieh *et al.* 2004) [12]	45.12
2	SDWCQ-PSO	(Wang *et al.*2011) [14]	47.49
3	LSB-GA	(Kanan & Nazeri 2014) [13]	34.79
4	SVD-JPSO	Our Method	**51.21**

Figure 2 explains the evaluated performance of the optimization algorithm using Lena image 512 × 512 original image, testing and calculate the ratio of the best fitness. SVD-JPSObased training procedure described, number of iteration was 50 and the population was 30, show in Figure 2 for part (A).



A: After 50 iterations without

B: After 100 iterations

C: After 300 iterations

D: After 300 iterations of the best fittness

Figure 2. Explains the Evaluated Performance of Iterations

In this work we show the value after number of iterations. In Figure 2 (B), calculate the best fitness and the mean fitness after 100 iteration, where the Figure 4 was the rate after 300 iteration. This result was obtained at the 300 iteration of SVD-JPSO optimization process and 30 of population size. The Figure 2 (C and D) showes the result of SVD-JPSO optimization process indicates that the fitness function was the maximum (148.4) without any types of attacks. The Figure 2 (D) , show the fitness value increases which mean the PSNR value and the correlation increases for the maximization.

6. Conclusions

Digital watermarking is an important task, the tradeoff between the embedding energy and perceptual translucence and the fidelity of image following the attacks. In this paper, we proposed SVD-JPSO for digital image watermarking scheme. The proposed SVD-JPSO used to optimize the performance of scaling factor in matrix form. The result obtained shows that the proposed SVD-JPSO got high robust watermarking image. The performance evaluated running the algorithm after number of iterations and see the result increasing the fitness value. The fitness value calculated in this work and prove the implement SVD-JPSO algorithm with watermarking play a good rule for maximum value of PSNR and correlation. The correlation between the original watermark and the extracted watermarked image can prove the ownership images. In addition, we treated the problem of false positive in SVD by using the proposed JPSO. For the future work, we are present to investigate the performance of (JPSO) by hybridize with local search algorithm so that the solution can be improved further in terms of quality.

Acknowledgments

This researchers has been made possible through research grants DIP-2016-018 awarded by Universiti Kebangsaan Malaysia (UKM) and Ministry of Higher Education, Malaysia. The researchers wish to express their gratitude to these institutions for their support.

References

[1] M. S. Subhedar and V. H. Mankar, "Image steganography using redundant discrete wavelet transform and QR factorization", Computers & Electrical Engineering, vol. 54, **(2016)**, pp. 406-422.

[2] M. S. Subhedar and V. H. Mankar, "Current status and key issues in image steganography: A survey", Computer Science Review,vol. 13, **(2014)**, pp. 95-113

[3] C.-S. Lu, "Multimedia Security", Steganography and Digital Watermarking Techniques for Protection of Intellectual Property: Igi Global, **(2004)**.

[4] R.-S. Run, S.-J. Horng, J.-L. Lai, T.-W. Kao and R.-J. Chen, "An improved SVD-based watermarking technique for copyright protection", Expert Systems with Applications, vol. 39, no. 1, **(2012)**, pp. 673-689.

[5] C. Jain, S. Arora and P. K. Panigrahi, "A reliable svd based watermarking schem", arXiv preprint arXiv:0808.0309, **(2008)**.

[6] Y. R. Wang, W. H. Lin and L.Yang, "An intelligent watermarking method based on particle swarm optimization", Expert Systems with Applications, vol. 38, no. 7, **(2011)**, pp. 8024-8029.

[7] A. Bassel and Md. J. Nordin, "Digital Image Watermark Authentication Using DWT-DCT", Journal of Engineering and Applied Sciences, vol. 11, **(2016)**, pp. 3227-3232.

[8] J. Kennedy and R. C. Ebrhart, "A discrete binary version of the particle swarm algorithm", IEEE conference on system, Man, and Cybernetics, vol. 5, **(1997)**, pp. 4104-4108.

[9] F. J. M. Garcia and J. M Perez, "Jumping frogs optimization: a new swarm method for discrete optimization", Documentos de Trabajo del DEIOC, vol. 3, **(2008)**.

[10] A. Bassel and M. J. Nordin, "Mutation and memory mechanism for improving Glowworm Swarm Optimization algorithm", In Computing and Communication Workshop and Conference (CCWC), 2017 IEEE 7th Annual IEEE, **(2017)**, pp. 1-7.

[11] E. J. Ientilucci, "Using the singular value decomposition", Rochester Institute of Technology, Rochester, New York, United States, Technical Report, **(2003)**.

[12] F. Y. Shih and S. Y. Wu, "Combinational image watermarking in the spatial and frequency domains", Pattern Recognition, vol. 36, no. 4, **(2003)**, pp. 969-975.

[13] H. R. Kanan and B. Nazeri, "A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm", Expert Systems with Applications, vol. 41, no. 14, **(2014)**, pp. 6123-6130.

[14] Y. R. Wang, W. H. Lin and L.Yang, "An intelligent watermarking method based on particle swarm optimization", Expert Systems with Applications, vol. 38, no. 7, **(2011)**, pp. 8024-8029.

[15] S.S. Bedi, G.S. Tomar and Shekhar Verma, "Robust Watermarking of Image in the Transform Domain using Edge Detection", 11th International Conference on Computer Modelling and Simulation, **(2009)**, pp.233-238.