Journal of Information Hiding and Multimedia Signal Processing
Ubiquitous International
©2010 ISSN 2073-4212
Volume **1**, Number **3**, July **2010**

Digital Watermarking using Ant Colony Optimization in Fractional Fourier Domain

Hameed Al-Qaheri

Department of Quantitative and Information System, CBA
Kuwait University, Kuwait.
alqaheri@cba.edu.kw

Abhijit Mustafi

Department of Computer Science,
Birla Institute of Technology Mesra, India

Soumya Banerjee*

Department of Computer Science,
Birla Institute of Technology Mesra, India

Received March 2010; revised April 2010

Abstract. *The paper describes the implementation of a watermarking embedding and retrieval technique using a conceptual approach of bio-inspired algorithm e.g. ant colony optimization (ACO). The essential construct of ACO is pheromone; hence the detection part of watermark is followed through ant's pheromone trace. The advantage of the proposal is bi-focal, i.e. the incorporation of modified Fractional Fourier domain and subsequently the sharp and noiseless pheromone maps during retrieval reinforce the security against deliberate tampering if any. Finally, the results of the proposed algorithms are presented in terms of improved RMSE index of the watermarked retrieved image after comparing with other contemporary works.*

1. **Introduction.** The era of Internet has created many new opportunities for digital content creation and delivery. Examples of digital content include electronic advertising, real-time video and audio delivery, digital repositories and libraries, and Web publishing. And since the current copyright laws are not adequate to deal with the protection of these types of digital content, he protection of the rights of all participants becomes a critical and important issue as well. This has led to an interest towards developing new copy deterrence and protection mechanisms which becomes more and more crucial [5,11]. One such effort that has been attracting increasing interest is based on digital watermarking techniques which has recently been proposed as an effective way to protect the ownership of digital documents [2]. The goal is to embed the watermark that is imperceptible in the image, while the copyright holder is capable to detect its existence, by using a proper private information key. Frequency domain and spatial domain based watermarking techniques are confined with signal embedding and therefore may relinquish the loosely coupled information of the image against some unknown intended attempt of tampering.

The basic idea of watermarking is to add/subtract a watermark signal to the host data to be watermarked such that the watermark signal is secure. The embedded watermark information can partly or fully be recovered from the watermarked image later on [4]. Digital watermarking allows the user to add a layer of protection to the images by identifying copyright ownership and delivering a tracking capability that monitors and reports where the user's images are being used. Copyright protection of owner is becoming more elusive as computer networks such as the global Internet are increasingly used to deliver electronic documents. Document distribution by network offers the promise of reaching vast numbers of recipients. It also allows information to be tailored and preprocessed. To meet the needs of each recipient.However, these same distribution networks represent an enormous business threat to information providers-the unauthorized redistribution of copyrighted materials [1, 4]. Adding a unique marking to a document can serve many purposes.

This paper proposes a novel watermarking embedding and detecting algorithm for image using an adaptive bio-inspired algorithm, while retrieving the original information. The inclusion of ant colony in retrieval process demostrates the robustness of proposed process compared to other contemporary methods like conventional fractional Fourier domain. It should also be noted that in the proposed model the embedded image is 2 dimensional and the retrieval can quantify the higher degree of transformational reliability under tampering.

The remaining part of the work is organized as follows: Section 2 presents some watermarking background and related literature. Section 3 describes the proposed watermarking scheme. Section 4 presents the experimentation results and discussion and finally the conclusion is discussed in Section 5.

2. **Related research and preliminary background.**

2.1. **Digital watermarking.**

Digital watermarking or simply watermarking, which is defined as embedding information such as origin, destination, access level, etc., of multimedia data (e.g., image, video, audio, etc.) in the host data, has been a very active area of research in recent years [1, 6–10]. It is a descendent of a technique known as steganography, which has been in existence for at least a few hundred years [1, 6–8].

Steganography is a technique where a secret message is hidden within another unrelated message and then communicated to another party. Some of the techniques of steganography like the use of invisible ink, word spacing patterns in printed documents, coding messages in music compositions, etc., have been used by military intelligence since the times of ancient Greek civilization [1, 6–8]. And Applications include ownership protection, proof of ownership, fingerprinting and authentication and tampering detection [7].

Watermarking can be considered as a special technique of steganography where one message is embedded in another and the two messages are related to each other in some way. The most common examples of watermarking are the presence of specific patterns in currency notes, which are visible only when the note is held to light and logos in the background of printed text documents. The watermarking techniques prevent forgery and unauthorized replication of physical objects. Digital watermarking is similar to watermarking physical objects except that the watermarking technique is used for digital

content instead of physical objects [2].

In digital watermarking a low-energy signal is imperceptibly embedded in another signal. The low-energy signal is called watermark and it depicts some metadata, like security or rights information about the main signal. The main signal in which the watermark is embedded is referred to as cover signal since it covers the watermark. The cover signal is generally a still image, audio clip, video sequence or a text document in digital format. The purpose of watermarks is twofold [2]:

- They can be used to determine ownership;
- They can be used to detect tampering.

There are two necessary features that all watermarks must possess. First, all watermarks should be detectable. In order to determine ownership, it is imperative that one be able to recover the watermark. The steganographic system uses the shared secret to determine how the hidden message should be encoded in the redundant bits. Modern steganography attempts to be detectable only if secret information is known namely, a secret key [1, 10]. This is similar to Kerckhoffs Principle in cryptography, which holds that a cryptographic systems security should rely solely on the key material [6–10]. For steganography to remain undetected, the unmodified cover medium must be kept secret, because if it is exposed, a comparison between the cover and stego media immediately reveals the changes.

2.2. **Discrete fractional Fourier transform.** Discrete fractional Fourier transform of the image is computed as the first phase of the process and sort the array of discrete fractional Fourier transform coefficients [5, 23, 24] , which follows the actual watermark embedding into the coefficients. The watermark itself is a sequence of M complex numbers. The real and imaginary parts are drawn from a normal distribution with mean zero and variance $\frac{\sigma}{2}$. The sorted vector is modified to embed the watermark and results a new array, which is rearranged in the core two dimensional array of the original image. Finally, the watermarked image is then obtained by computing the inverse of discrete fractional Fourier transform [28]. As a generalized form of the the Fourier transform, the fractional Fourier transform has become a powerful and potential tool for time-varying and non-stationary signal processing [26]. As the classical Fourier transform corresponds to a rotation in the time-frequency plane over an angle, the FRFT can be considered as a generalized form that corresponds to a rotation over some arbitrary angle [26]. The p_{th} order FRFT of the signal is defined as:

$$F^p[f(x)] = \int_{-\infty}^{\infty} K_p(x,u) f(x) dx, 0 \leq |p| \leq 2 \tag{1}$$

Where p is the order of FRFT, α is the rotation angle, also the relationship of p and is $\alpha = \frac{p\pi}{2}$, $K_p(x,u)$ is the kernel function of the FRFT [26]. The inverse of an FRFT with an order p is the FRFT with order $-p$. $F(p)$ is defined as follows [26]:

$$F(x) = F^{-p}[F^p(f(x))] \tag{2}$$

2.3. **Ant Colony Optimization.** Ant colony optimization, which is specialized algorithm, is a recently developed population-based approach. It has been successfully applied to several NP-hard combinatorial optimization problems [15, 16, 22, 27, 29, 30]. ACO, as the name suggests, was inspired by observing real ants' foraging behavior. As ants live in colonies in searching for food they use a cooperative method and while moving, they initially explore the area surrounding their nest in a random manner leaving a chemical

pheromone trail on the ground. Ants smell pheromone to choose their way and this implies that, they tend to choose the paths marked by strong pheromone concentrations. During the return trip, the quantity of pheromone that an ant leaves on the ground may depend on the quantity and quality of the food. These pheromone trails progressively decrease by evaporation with time elapsing resulting in the amount of pheromone becomes larger on a shorter path. Then the probability that an ant selects this shorter path becomes higher [27]. One model of learning that exhibits these features is the pheromone mechanism used by insects to guide their collective decision processes [25]. And as described in [25]this mechanism has four components:

Aggregation: An entity (insect or simulation agent) marks an event by adding to an existing base of pheromone. This component effectively fuses multiple observations into a single variable.

Evaporation: Over time, pheromones gradually fade (unless new deposits reinforce them). This component is a novel mechanism for truth maintenance. In traditional AI, an agent remembers everything that it has learned unless there is reason to forget it. This approach is computationally intractable for logics beyond a certain level of expressiveness [19]. In contrast, an ant colony immediately begins to forget everything it learns as soon as it learns it, unless it is reinforced, a constant-time process.

Propagation: Pheromones disperse spatially, with the maximum concentration of a deposit remaining at the original point of deposit.

Sensing: Other entities make decisions or act based on the pheromone levels they sense in their environment.

3. The Proposed Watermarking Scheme.

Considering the four prosperities presented in the previous section, the logical flow of the watermarking embedment and detection has been formulated in Figure (1). The logical flow of the process elaborates that both target and signature is sensed by pheromone and it is preceded with two different domain α_1 and α_2. After embed dement and transform, the retrieval procedure of the original image is considered and to achieve better sharpness of retrieved watermarked image the pheromone sensing has

3.1. The Proposed Algorithm and the Associated Components.

The proposed algorithm has three distinct phases, it is defined as follows:

embdding: This phase start by detecting the initialized domain parameters α_1 and α_2, then choose the best value for normalized embedding domain factor based on heuristic and it guided by core algorithm through Ant Colony Optimization (ACO).

retrieving: In this phase, the pheromone trace mechanism is initiated to yield the better result in terms of original embedded image irrespective of tampering efforts against the post retrieval of the watermarked image, .

Ant Process: A certain quantity of Ants are placed randomly on a bi-dimensional lattice represented by an $N * N$ array and this array store values between 0 and 255, based on the 8-bit gray level of the pixels. For each iteration, each ant moves to an adjacent cell and reinforces the pheromone level on that spot. One cell may be occupied by one and only one ant (in this case, an ant will not move if it finds itself totally surrounded by others ants), or ants are allowed to share the same cell [18]. Ant chooses a particular cell of the subjected embedded image to trace according to its current direction and the pheromone intensity on the eight surrounding cells [18]. It is implied that, if an ant comes from south, and the eight cells have no pheromone, the chance of going north is higher, followed by the chance of going northeast or

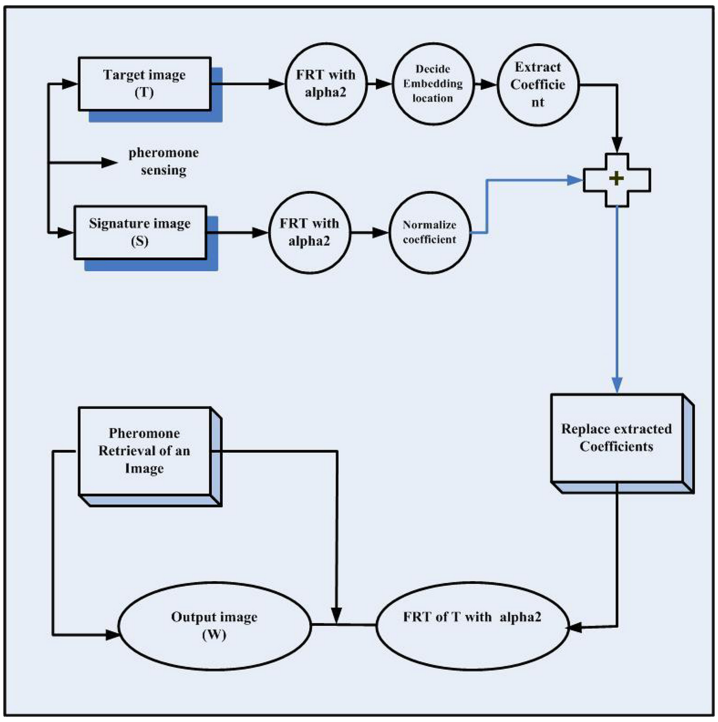

Fig. 1 The Proposed Watermarking Scheme

northwest, and so on, until the likelihood of returning south, which would be very low (refer fig. 2). This is represented by the function $w(\bowtie\bowtie)$, which is a probabilistic directional bias, where the domain consists of $\bowtie\bowtie\bowtie = 0$, $\bowtie\bowtie\bowtie = 45$, $\bowtie\bowtie\bowtie = 90$, $\bowtie\bowtie\bowtie = 135$ $\bowtie\bowtie\bowtie = 180$. A high value of Δ_{gl} means that the ant is making a transition from regions of the image with different gray-level pixels.

We have to note that the max Δ_{gl} represents the maximum Δ_{gl} found so far. This means that the energy of ants moving between two regions, where the difference between the gray-level median values is equal to max Δ_{gl}, it will remain the same, since it increases in an amount equal to the fixed amount decreased [18]. The final probabilities are dependent on the pheromone level found on the neighboring cells [17]. The relative probabilities to move to a cite i with pheromone density s_i are given by eq.(3), where $W(s)$ is given by eq.(4). Since a two dimensional lattice is used, i represents the eight cells that surround k.

$$P_{ik} = \frac{W(\sigma_{j/k})w(\Delta_\theta)}{\Sigma W(\sigma_j)w(\Delta_\theta)} \tag{3}$$

Where

$$W(\sigma) = (1 + \frac{\sigma}{1+\sigma})^\beta \tag{4}$$

Where β represents the osmotropotaxic sensitivity (controls the tendency to follow pheromone: high values of β result in ants heavily attracted by pheromone, while lower values cause the swarm to behave in a more randomly way) and $\frac{1}{d}$ is the sensory capacity, which describes the fact that each ant's ability to sense pheromone decreases somewhat at high concentrations.

The main steps of the proposed watermarking algorithm and its associated components are given in Algorithm (1).

Algorithm 1 the proposed watermarking algorithm and its associated components

Input Parameters: T, S, α_1, magarray, α_2, ImageCells, Normalizedfactor

Phase-I Embedding :

if (strcmp(k.ColorType,'truecolor')==1) **then**
  B = rgb2gray(A);
end if
if (strcmp(k.ColorType,'grayscale')==1) **then**
  B = A;
end if
Initialize α_1;
T = DFRT (new_{dim}, α_1);
F1 = T*C*T;
Initialize α_2
T = dFRT(256,α_1);
T = DFRT(new_{dim},α_1);
Sort mag_{array} ( );
call NormalizedEmbedding( );
if (alpha1 > 0.5) **then**
  call DisplayfftshiftedImage( );
else
  Display Image();
end if
Phase-II: Retrieving
if (Colortype != 'GrayScale') **then**
  Convert Gray ( );
end if
Initialize α_2
DFRT (α_2);
Deamplify( );
Extract Coefficients(normalizedembeddingloc);
Initialize α_1
Inverse DFRT (α_1);
Extract Signature ( );
Phase-III: Ant Process
for all agents **do**
  place agent at randomly at selected cell
end for
for t = 1 to tmax **do**
  for all agents **do**
    Compute W(s) and Pik According to equations (3) and (4)
    Move to a selected adjacent cell not occupied by other ant
    Increase pheromone at cell c
    P(c) = P(c) + [η+Δ_{gl}/255]
  end for
  Evaporate pheromone by K, at all cells
end for

Fig.(2a) Sign Image: $83 * 62$ pixels

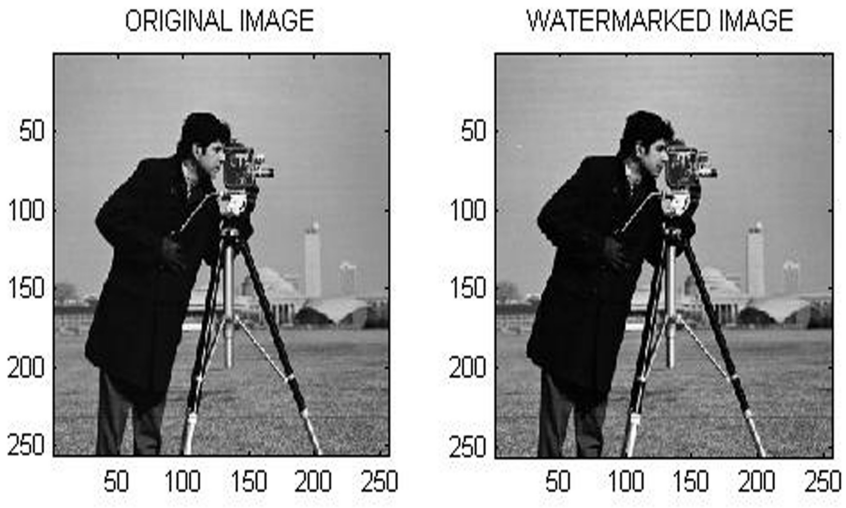

Fig.(2b) Original and Watermarked Image

4. **Experimental Results and Discussions.** The retrieved image watermarked through the proposed algorithm often suffers from low contrast and lack of perceived brightness. This can be compensated by using an "Amplification factor" during the embedding process. The amplification factor is a multiplicative index that can be used to proportionately boost the signal strength of the image post embedding. The retrieved image can be simplified. The sample image to be used as the water mark is shown in fig. 2a, which is embedded in fig. 2b.

The inclusion of ant's pheromone trace using equation (1) in post retrieval process yield the pheromone traced watermarked image (Refer Fig.2c). This may be one of the alternative approaches to achieve more precise and guided retrieved images even with presence of extreme tampering.

The parameters of the ant's pheromone in the simulation [20] were set to the following values:$\beta = 3.5$; $\sigma = 0.2$; $\eta = 0.07$; $k = 1.0$; $p = 1.5$; $S = 30\%$ (S is the size of the initial population of ants measured in percentage of the total environment space in pixels). The traced watermarked image is produced after 100 iterations and creates pheromone

Fig.(2c)Pheromone Traced Watermarked Image (Fixed population of ants)

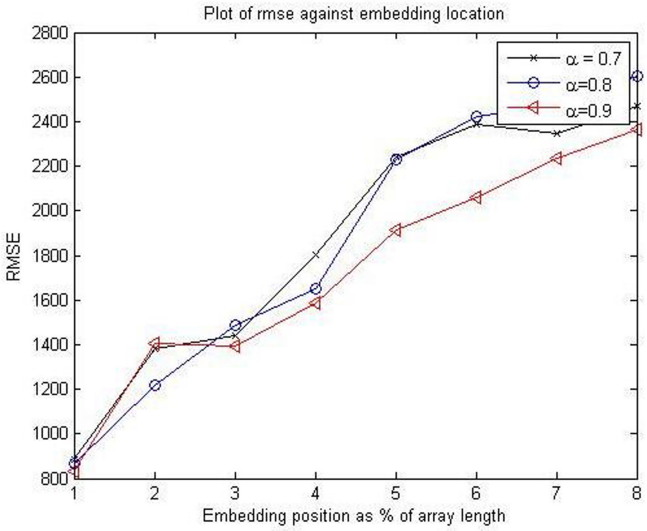

Fig.(3) Progressive value of RMSE index

maps with less noise and higher intensity regions of pheromone are reinforced while retrieved. From the simulation experiments, it is evident that the extracted image signature demonstrates a higher percentage of matches in case of tampering and illegal entry to the original image. Figures (3 and 4) demonstrate the performance of our algorithm when under attack and highlight the three variables the attacker must be in possession of for a successful attack. The parameters of confusion in our algorithm are:

- The FRT parameter α_2;
- The FRT parameter α_2
- The location of embedded watermark

As is evident from figure (4), the extracted signature is released only when the correct values of all the three parameters are identified. In case of failure in identifying even one of the parameters the extracted signature shows a high degree of RMSE and consequently would be unrecognizable. The proposed algorithm also performed remarkably well when a genuine image is under attack. The embedded signature was successfully retrieved from images corrupted with Gaussian noise, salt and pepper noise, skewed images and also

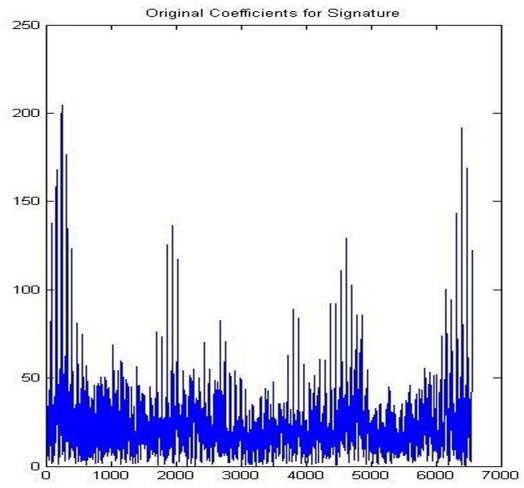

Fig.(4) Original and Extracted Coefficients of Signature for non tampered image

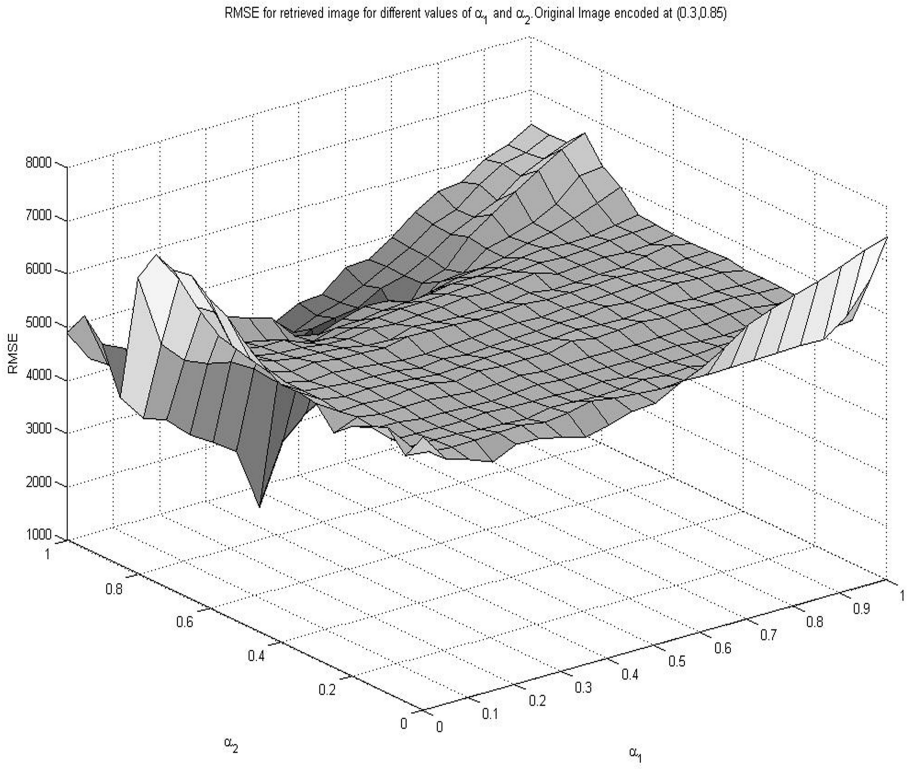

Fig.(5) Robustness of the watermark with varying α_1 and α_2 (Original Watermark Embedded at α_1=0.3 and α_2=0.85)

cropped images. Figure (5) shows such an instance of a cropped image. As it is shown from the sequence the extracted coefficients are in relatively close correspondence of the original coefficients except for images which are cropped to great extent.

The image sequence demonstrates the extracted coefficients for a cropped jpg image with increasing crop size (refer fig. 6). The first 6 watermark instances are still recognized when the crop size is 128x128 for an original image of size 256x256 pixels

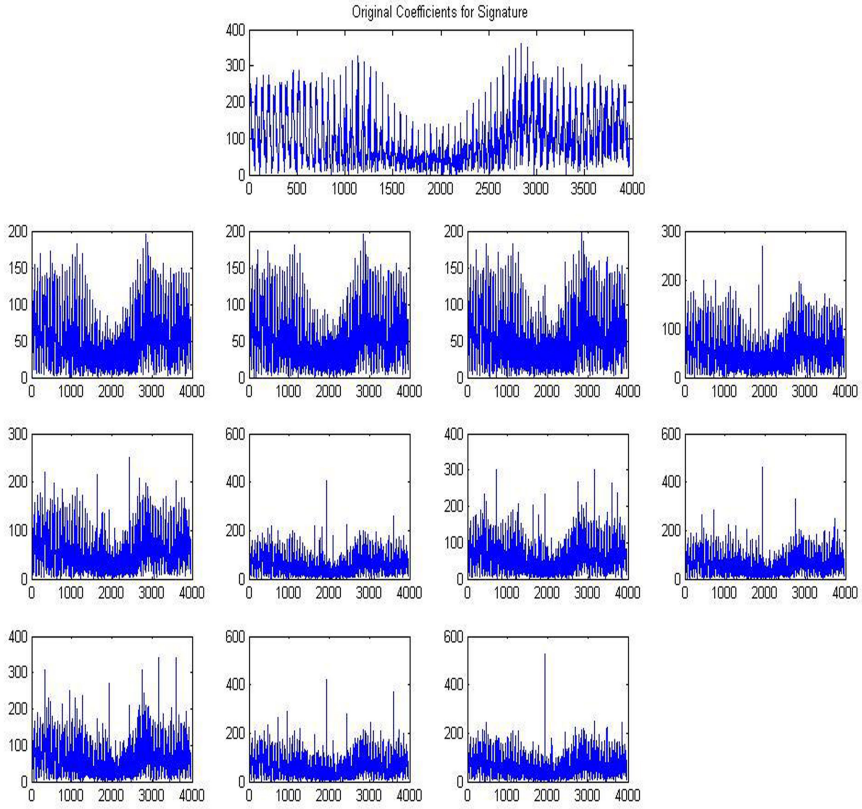

Fig.(6) Performance of Watermark under attack

5. **Conclusions.** The proposed algorithm satisfies all the requirements for a practical digital watermarking algorithm. It is simple to implement on a public key infrastructure and is highly robust. The inherent nature of the Fractional Fourier Transform is ideally suited for digital watermarking as the watermarks could be spread over a wide spectrum of frequency. The retrieval is equally simple and requires the invocation of the inverse FRT. Moreover under attack the algorithm relies on its multi step nature to avoid complete obliteration of the watermark except for images which are severely compromised in which case visual inspection is sufficient to gauge the difference.

REFERENCES

[1] Aboul Ella Hassanien, Ajith Abraham, and Crina Grosan, Spiking neural network and wavelets for hiding iris data in digital images, *Soft Computing*, vol. 13, pp. 401–416, 2009.

[2] Abou Ella HASSANIEN, A Copyright Protection using Watermarking Algorithm, *INFORMATICA*, vol. 17, no. 2, pp. 187–198, 2006.

[3] X. Y. Wang, Z. H. Xu and H. Y. Yang, *A robust image watermarking algorithm using SVR detection.*, Expert Systems with Applications, vol. 36, pp. 9056-9064, 2009.

[4] Michiel van der Veen, Aweke Negash Lemma and Ton Kalker. Electronic content delivery and forensic watermarking, *Multimedia Systems*, vol. 11, no. 2, pp. 174–184, 2005

[5] C. Candan, M. A. Kutay, and H. M. Ozaktas, The discrete Fractional Fourier Transform. *IEEE Trans. Signal Processing*, vol. 48, pp. 1329-1337, 2000.

[6] H. C. Huang and Wai-Chi Fang, Metadata-based image watermarking for copyright protection, Simulation Modelling Practice and Theory, 2009.

[7] J. S. Pan, H. C. Huang, L. C. Jain, and W. C. Fang (eds.), *Intelligent Multimedia Data Hiding*, Springer, 2007.

[8] H. C. Huang, C. M. Chu, and J. S. Pan. , The optimized copyright protection system with genetic watermarking, Soft Computing, vol. 13, no. 4, pp. 333-343, 2009.
[9] M. Boutell, and J. Luo, Photo classification by integrating image content and camera metadata. International Conference on Pattern Recognition, vol. 4, pp. 901-904, 2004.
[10] N. Sinha, Secure embedded data schemes for user adaptive multimedia presentation, Journal of Digital Information, vol. 6, no. 4, 2005.
[11] J. Guo, Z. Liu, and S. Liu. Watermarking based on discrete fractional random transform. Optics Communications, vol. 272, no. 2, pp. 344–348, 2007.
[12] Igor Djurovic, Srdjan Stankovic, and Ioannis Pitas, Digital watermarking in the fractional fourier transformation domain, Journal of Network and Computer Applications, vol. 24, no. 4, pp. 167–173, 2001.
[13] M. L. Miller, G. J. Doerr, and I. J. Cox, Applying informed coding and embedding to design a robust, high capacity watermark, *IEEE Trans. Image Processing*, vol. 13, no. 6, pp. 792–807, Jun. 2004.
[14] M. Juan Vilardy, O. Cesar Torres, and Lorenzo Mattos, Fingerprint Encryption using Fractional Fourier Transform 8th, *World Congress on Computational Mechanics (WCCM8) 5th. European Congress on Computational Methods in Applied Sciences and Engineering (ECCOMAS 2008)*, Venice, Italy, 2008.
[15] M. Dorigo, V. Maniezzo, and A. Colorni. The ant system: Optimization by a colony of cooperating agents, *IEEE Trans. Systems*, vol. 26, no. 1, pp. 1–13, 1996.
[16] M. Dorigo, T. Stutzle, Ant Colony Optimization. The MIT Press, 2004.
[17] C. Fernandes, V. Ramos, A.C Rosa , Varying the population size of artificial foraging swarms on time varying landscapes, in W. Duch, J. Kacprzyk, E. Oja, and S. Zadrozny (eds.), Artificial Neural Networks: Biological Inspirations, *Proc. of the 15th Int. Conf.*, vol. 3696, pp. 311-316, Sept. 2005.
[18] D. Chialvo, M. Millonas, How swarms build cognitive maps, In Steels, L. (eds.), The Biology and Technology of Intelligent Autonomous Agents, vol. 144, pp. 439–450, 1995.
[19] S. Brueckner, Return from the Ant: Synthetic Ecosystems for Manufacturing Control, Humboldt University Berlin, Berlin, Germany, Dr. rer. nat. Thesis, 2000.
[20] V. Ramos, F. Almeida, Artificial ant colonies in digital image habitats-a mass behavior effect study on pattern recognition, *Proc. of the 2nd Int. Wksp. on Ant Algorithms*, pp. 113-116, Sep. 2000.
[21] M. Hadun Ozaktas, Orhan Arikan, Digital Computation of the Fractional Fourier Transform, *IEEE Trans. signal processing*, vol. 9, pp. 2141-2149, 1996.
[22] X. X. Li and J. J. Wang, A steganographic method based upon JPEG and particle swarm optimization algorithm. Information Sciences, vol. 177, pp. 3099–3109, August 2007.
[23] M. Q. Fang and H. X. Wang , Chaos-based discrete fractional Sine transform domain audio watermarking scheme Computers & Electrical Engineering, vol. 35, pp. 506–516, May 2009.
[24] Igor Djurovic, Srdjan Stankovic, Ioannis Pitas Digital watermarking in the fractional Fourier transformation domain Journal of Network and Computer Applications, vol. 24, pp. 167–173, April 2001.
[25] H. Van Dyke Parunak, Sven A. Brueckner, and Robert Matthews, Pheromone Learning for Self-Organizing, May 2005.
[26] F. Q. Yu, Z. K. Zhang and M.H. Xu, A Digital Watermarking Algorithm for Image Based on Fractional Fourier Transform, *Proc. of the 1ST IEEE Conference on Industrial Electronics and Applications*, vol. 24-26, pp. 1-5, May 2006,
[27] X. S. Xu, J. Ma, and J. S. Lei, An Improved Ant Colony Optimization for the Maximum Clique Problem, *Proc. of the 3th International Conference* , vol. 24-27, pp. 766-770, Aug. 2007.
[28] Adhemar Bultheel, Digital watermarking of images in the fractional Fourier domain, Technical Report TW497, Dept. CS, pp. 1–12, July 2007.
[29] M. Dorigo, V. Maniezzo, A. Colorni. Ant system:Optimization by a colony of cooperating agents, *IEEE Trans. systems man and cybernetics part B-cybernetics*, vol. 26, no.1, pp. 29–41, 1996.
[30] S. C. Chu, John F. Roddick and J. S. Pan. Ant Colony System with communication Strategies, Information Sciences, vol. 167, pp. 63–76, 2004.