A Block-wise-based Fragile Watermarking Hybrid Approach using Rough Sets and Exponential Particle Swarm Optimization

Lamiaa M. El Bakrawy[1], Neveen I. Ghali[1], Tai-hoon Kim[2] and Aboul ella Hassanien[3]
[1]Al-Azhar University, Faculty of Science, Cairo, Egypt
Email: lamiaabak@yahoo.com, nev_ghali@yahoo.com
[2]Hannam University, Korea, taihoonn@hannam.ac.kr
[3]Cairo University, Faculty of Computers and Information, Cairo, Egypt
Email:aboitcairo@gmail.com

Abstract

In this paper, we propose a fragile watermarking hybrid approach using rough set k-means and exponential particle swarm optimization (EPSO) systems. It is based on a block-wise dependency mechanism which can detect any alterations made to the protected image. Initially, the input image is divided into blocks with equal size in order to improve image tamper localization precision. Then feature sequence is generated by applying rough k-means and EPSO clustering to create the relationship between all image blocks and cluster all of them since EPSO is used to optimize the parameters of rough k-means. Both feature sequence and generated secret key are used to construct the authentication data. Each resultant 8-bit authentication data is embedded into the eight least significant bits (LSBs) of the corresponding image block. We gives experimental results which show the feasibility of using these optimization algorithms for the fragile watermarking and demonstrate the accuracy of the proposed approach. The performance comparison of the approach was also realized. The performance of a fragile watermarking approach has been improved in this paper by using exponential particle swarm optimization (EPSO) to optimize the rough k-mean parameters. The proposed approach can embed watermark without causing noticeable visual artifacts, and does not only achieve superior tamper detection in images accurately, it also recovers tampered regions effectively. In addition, the results show that the proposed approach can effectively thwart different attacks, such as the cut-and paste attack and collage attack, while sustaining superior tamper detection and localization accuracy.

Keywords: Fragile Watermarking, rough sets,exponential particle swarm optimization

1 Introduction

The rapid expansion of the Internet and the overall development of digital multimedia content and nonlinear media distribution requires new enabling technologies, beyond traditional approaches such as password-based encryption that are used for safe custody of private keys do not provide adequate security due to very low entropy in user chosen passwords. Biometric-based personal identification techniques that use physiological or behavioral characteristics are becoming increasingly popular compared to traditional

token-based or knowledge based techniques such as identification cards (ID), passwords, etc. One of the main reasons for this popularity is the ability of the biometrics technology to differentiate between an authorized person and an impostor who fraudulently acquires the access privilege of an authorized person data and information hiding technology is a commonly used technique that embeds additional messages into the host signals by modifying their original content. These messages can serve as authentication codes, annotation, or secret data depending on the purpose of the application itself. For instance, if it is a case of copyright protection, a robust digital watermarking method would be a good choice; in case it is the security of secret communication that the users are seeking, and then image steganography (information hiding) should be taken into consideration. The basic idea in digital watermarking is to embed a watermark signal into the host data for the purpose of copyright protection, access control, broadcast monitoring, fingerprinting, broadcast monitoring, image authentication, etc. [10, 16].

A watermark can be a tag, label, digital signal or biometric human print such as iris, signature, etc. A host may be multimedia object such as an image, audio or video. 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. Adding a unique marking to a document can serve many purposes.

As watermark-based image authentication schemes are efficient and attractive, some types of watermarks such as logos, labels, trademark, or random sequence, representing the author's ownership, are embedded into the desired digital image. Generally, a registration to the authentication center is necessary, which helps to solve ownership disputes by identifying the owner of the disputed media. If necessary, the embedded watermark in the digital image can be used to verify ownership [1, 2, 4].

The authentication digital watermark-based approaches can be classified as either fragile watermarking or semi-fragile watermarking. A fragile watermarking can detect any possible modification of the pixel values. On the other hand, semi-fragile watermarking can distinguish content-preserving operations from malicious manipulations [3, 11, 14]. Various approaches for fragile watermarking [15, 16] and semi-fragile watermarking [17, 18] have been proposed. Since tamper detection and localization are well defined in fragile watermarking approaches, the work presented in this paper concentrates on the latter.

In this paper, a novel block-based fragile watermarking approach for image authentication is proposed. To effectively break block-wise independency, the proposed approach first applies hybrid rough k-means and exponential particle swarm optimization (EPSO) to create the relationship between all image blocks and cluster all of them. The EPSO has a great impact on global and local exploration it is supposed to bring out the search behaviour quickly and intelligently as it avoid the particles from stagnation of local optima

by varying inertia weight exponentially, so that the movement of the particles will be faster and distant from each other. The EPSO is used to find optimal parameters of the rough k-means. Both feature sequence and generated secret key are used to construct the authentication data. Each resultant 8-bit authentication data is embedded into the eight least significant bits (LSBs) of the corresponding image block. Experimental results show that the proposed approach can embed watermark without causing noticeable visual artifacts, and does not only achieve superior tamper detection in images accurately, it also recovers tampered regions effectively. In addition, the results show that the proposed approach can effectively thwart different attacks, such as the cut-and paste attack and collage attack, while sustaining superior tamper detection and localization accuracy.

The remainder of this paper is ordered as follows. Brief introduction of rough sets and particle swarm optimization algorithms are introduced in Section (2). Some improvement of the rough k-means and particle swarm optimization are discussed in Section (3). The details of the proposed fragile watermarking approach using hybrid rough k-means and exponential particle swarm optimization is presented in Section (4). Section (5) shows the experimental results. Conclusions are discussed in Section (6).

2 Preliminaries: Rough Sets and Particle Swarm Optimization

Due to space limitations we provide only a brief explanation of the basic framework of rough set theory and particle swarm optimization, along with some of the key definitions. A more comprehensive review can be found in sources such as [6–8, 20, 21].

2.1 Rough sets

Pawlak proposed rough set theory, which deals with the uncertainty of data. The theory is a new intelligent mathematical tool. It is based on the concept of approximation spaces and models of the sets and concepts [6–9]. The main advantage of rough set theory is that it does not need any preliminary or additional information about data: like probability in statistics or basic probability assignment in Dempster − Shafer theory, a grade of membership or the value of possibility in fuzzy set theory [12, 13] Also rough set theory is very useful, especially in handling imprecise data and extracting relevant patterns from crude data for proper utilization of knowledge [16].

Let $\mathcal{O}, \mathcal{F}$ denote a set of sample objects and a set of functions representing object features, respectively. Assume that $B \subseteq \mathcal{F}, x \in \mathcal{O}$. Further, let $[x]_B$ denote: $[x]_B = \{y : x \sim_B y\}$. Rough sets theory defines three regions based on the equivalent classes induced by the feature values: lower approximation $\underline{B}X$, upper approximation $\overline{B}X$ and boundary $BND_B(X)$. A lower approximation of a set X contains all equivalence classes $[x]_B$ that are proper subsets of X, and upper approximation $\overline{B}X$ contains all equivalence classes $[x]_B$ that have objects in common with X, while the boundary $BND_B(X)$ is the set $\overline{B}X \setminus \underline{B}X$, *i.e.*, the set of all objects in $\overline{B}X$ that are not contained in $\underline{B}X$.

2.2 Particle swarm optimization

The concept of particle swarms, although initially introduced for simulating human social behaviors, has become very popular these days as an efficient search and optimization

technique. Particle swarm optimization [20,21], does not require any gradient information of the function to be optimized, uses only primitive mathematical operators and is conceptually very simple. PSO has attracted the attention of a lot of researchers resulting into a large number of variants of the basic algorithm as well as many parameter automation strategies. The canonical PSO model consists of a swarm of particles, which are initialized with a population of random candidate solutions. They move iteratively through the d-dimension problem space to search the new solutions, where the fitness, f, can be calculated as the certain qualities measure. Each particle has a position represented by a position-vector $\vec{x}_i$ (i is the index of the particle), and a velocity represented by a velocity-vector $\vec{v}_i$. Each particle remembers its own best position so far in a vector $\vec{x}_i^{\#}$, and its j-th dimensional value is $x_{ij}^{\#}$. The best position-vector among the swarm so far is then stored in a vector $\vec{x}^*$, and its j-th dimensional value is x_j^*. During the iteration time t, the update of the velocity from the previous velocity to the new velocity is determined by Eq. (1). The new position is then determined by the sum of the previous position and the new velocity by Eq. (2).

$$v_{ij}(t+1) = \begin{cases} wv_{ij}(t) + c_1 r_1 (x_{ij}^{\#}(t) - x_{ij}(t)) \\ +c_2 r_2 (x_j^*(t) - x_{ij}(t)) \end{cases} \quad (1)$$

$$x_{ij}(t+1) = x_{ij}(t) + v_{ij}(t+1). \quad (2)$$

where w is called as the inertia factor which governs how much the pervious velocity should be retained from the previous time step , r_1 and r_2 are the random numbers, which are used to maintain the diversity of the population, and are uniformly distributed in the interval [0,1] for the j-th dimension of the i-th particle. c_1 is a positive constant, called as coefficient of the self-recognition component, c_2 is a positive constant, called as coefficient of the social component. From Eq. (1), a particle decides where to move next, considering its own experience, which is the memory of its best past position, and the experience of its most successful particle in the swarm. In the particle swarm model, the particle searches the solutions in the problem space with a range $[-s, s]$ (if the range is not symmetrical, it can be translated to the corresponding symmetrical range). In order to guide the particles effectively in the search space, the maximum moving distance during one iteration must be clamped in between the maximum velocity $[-v_{max}, v_{max}]$ given in Eq.(3):

$$v_{ij} = sign(v_{ij}) min(|v_{ij}|, v_{max}). \quad (3)$$

The value of v_{max} is $p \times s$, with $0.1 \leq p \leq 1.0$ and is usually chosen to be s, i.e. $p = 1$. The end criteria are usually one of the following: maximum number of iterations, number of iterations without improvement, or minimum objective function error

3 Some improvement

3.1 Adaptation of K-means to rough set theory

K-means clustering algorithm originates from the means of the k clusters that are created from n objects [7]. Let us assume that the objects are represented by m-dimensional vectors. The objective is to assign these n objects to k clusters. Each of the clusters is also represented by an m-dimensional vector, which is the centroid or mean vector for

that cluster. The process begins by randomly choosing k objects as the centroids of the k clusters. The objects are assigned to one of the k clusters based on the minimum value of the distance $d(v, x)$ between the object vector $v = (v_1, ..., v_j, ..., v_m)$ and the cluster vector $x = (x_1, ..., x_j, ..., x_m)$. After the assignment of all the objects to various clusters, the new centroid vectors of the clusters are calculated as:

$$x_j = \frac{\sum_{v \epsilon x} v_j}{|x|} \tag{4}$$

Where $1 \leq j \leq m$, $|x|$ is the size of cluster x. Incorporating rough sets into K-means clustering requires the addition of the concept of lower and upper bounds [7,8]. Calculation of the centroids of clusters from conventional K-means needs to be modified to include the effects of lower as well as upper bounds. The modified centroid calculations for rough sets are given in Algorithm(1).

Algorithm 1 The modified centroid calculations for rough sets

if $\underline{B}X \neq \emptyset$ and $\overline{B}X - \underline{B}X = \emptyset$ **then**
  Compute $x_j = \frac{\sum_{v \in \underline{B}X} v_j}{|\underline{B}X|}$
end if
if $\underline{B}X = \emptyset$ and $\overline{B}X - \underline{B}X \neq \emptyset$ **then**
  Compute $x_j = \frac{\sum_{v \in (\overline{B}X - \underline{B}X)} v_j}{|\overline{B}X - \underline{B}X|}$
else
  Compute $x_j = w_{lower} \times \frac{\sum_{v \in \underline{B}X} v_j}{|\underline{B}X|} + w_{upper} \times \frac{\sum_{v \in (\overline{B}X - \underline{B}X)} v_j}{|\overline{B}X - \underline{B}X|}$
end if

Where $1 \leq j \leq m$. The parameters w_{lower} and w_{upper} correspond to the relative importance of lower and upper bounds, and $w_{lower} + w_{upper} = 1$. If the upper bound of each cluster were equal to its lower bound, the clusters would be conventional clusters. Therefore, the boundary region $(\overline{B}X - \underline{B}X)$ will be empty, and the second term in the equation will be ignored. Thus, the equation on Algorithm (1) will reduce to conventional centroid calculations.
The next step in the modification of the K-means algorithm for rough sets is to design criteria to determine whether an object belongs to the upper or lower bound of a cluster given as follows:

For each object vector, v, let $d(v, x_j)$ be the distance between itself and the centroid of cluster x_j. Let $d(v, x_i) = min_{1 \leq j \leq K} d(v, x_j)$.The ratio $d(v, x_i)/d(v, x_j)$, $1 \leq i, j \leq k$, are used to determine the membership of v. Let $T = \{j : d(v, x_i)/d(v, x_j) \leq$ threshold ϵ and $i \neq j\}$.

1. If $T \neq \emptyset, v \in \overline{B}X_i$ and $v \in \overline{B}X_j), \forall j \in T$. Furthermore, v is not part of any lower bound. The above criterion guarantees that property (3) is satisfied.
2. Otherwise, if $T = \emptyset$, $v \in \underline{B}X_i$. In addition, by property (2), $v \in \overline{B}X_i$. It should be emphasized that the approximation space A is not defined based on any predefined relation on the set of objects. The upper and lower bounds are constructed based on the criteria described above.

3.2 Exponential particle swarm optimization

An improvement to original PSO is constituted by the fact that w is not kept constant during execution. It is starting from a maximal value and then linearly decremented as the number of iterations increases down to a minimal value [22, 23]. In this paper we initially set the maximal number to 0.9 and decreasing to 0.4 over the first 1500 iterations. In case if the iterations are above 1500, and remaining 0.4 over the remainder of the run according to Eq.(5):

$$w = (w - 0.4)\frac{M - I}{M} + 0.4 \tag{5}$$

M and I represents the maximum number of iterations and the number of iterations, respectively.

4 A Block wise-based fragile watermarking approach

In this section, we explain the proposed fragile watermarking approach. The system contains three phases: (1) Rough k-means and exponential particle swarm algorithm, (2) watermark embedding procedure, and (3) tamper detection procedure. These three phases are described in detail in the following section along with the steps involved and the characteristics feature for each phase.

4.1 Rough K-means and exponential particle swarm algorithm

The k-means algorithm is a simple and efficient clustering algorithm [19]. In spite of its simplicity, the K-means algorithm can be trapped into local optimal error (i.e., it finds local optimal solution, instead of finding the global optimal solution). To overcome this problem, the rough set theory and particle swarm optimization are proposed to enhance the performance of the k-means algorithm.

Moreover, rough k-means has two parameters that need to be determined, lower approximation and threshold value. Manual adjustment through testing is not practical for image authentication in general. Hence, the particle swarm optimization is proposed to alleviate the limitation by automatically searching and modifying the parameters during the image authentication process. The algorithm that combines rough k-means and EPSO algorithm is as follows:

4.2 Watermark embedding procedure

Let us consider, I is the host image of size $M \times M$, where M is assumed to be an even number. The original image is divided into non-overlapping 2×2 blocks $B_j (1 \leq j \leq \frac{M}{2} \times \frac{M}{2})$ which are arranged by the order from left to right and then top to bottom.

To generate the watermark, the two LSBs of all the pixels within each block of the host image are first set to zero. Each block B_j can be regarded as a 4-dimensional vector,$B_j = (B_{j1}, B_{j2}, B_{j3}, B_{j4})$. Then rough k-means and EPSO algorithm is applied to classify all the blocks into k clusters. After performing the rough k-means and EPSO algorithm, for each block, B_j, let $d(B_j, x_c)$ be the distance between itself and the centroid of cluster

Algorithm 2 Rough K-means and EPSO

1: Initialize the cluster mean of each cluster x_i.
2: Initialize a number of particles where each of the particles are randomly assigned with lower approximation variable and threshold.
3: Classify each particle in the particles to either lower or upper approximation of each cluster. Find the minimum pair of distance to all clusters,
4: If the difference of the distance is less than threshold, then the pixel belongs to upper approximation of both clusters x_i and x_j
5: Otherwise, the particle belongs to lower approximation of cluster x_i
6: Calculate the Davies-Bouldin Index (DB Index) of each particle. Each particle saves DB Index obtained from the iterations and compares them with the other particles. Find the global best index and tune the lower approximation and thresholds of each particle according to the following guidelines.
7: If personal best DB Index = global best DB Index, then adjust threshold lower to include only the particle that are definitely in lower approximation.
8: If personal best DB Index > global best DB Index, then adjust the lower approximation variable and threshold of the particle toward the values of particles with global best DB index.
9: Calculate the new mean for each cluster x_i
10: Repeat steps 3 to 9 until all particles converge.

$x_c, 1 \leq c \leq k$. Let $d(B_j, x_i) = min_{1 \leq c \leq\ k} d(B_j, x_c), d(B_j, x_m) = max_{1 \leq c \leq\ k} d(B_j, x_c), 1 \leq i, m \leq\ k$. Then, we compute feature sequence $F = \{f_1, f_2, \ldots, f_{\frac{M}{2} \times \frac{M}{2}}\}$ by using the following equation.

$$f_j = \frac{d(B_j, x_i)}{d(B_j, x_m) - d(B_j, x_i)} \tag{6}$$

When $f_j < 0.1$ then $f_j = 0$ other wise $f_j = 1$, assume that $R = \{r_1, r_2, ..., r_{\frac{M}{2} \times \frac{M}{2}}\}$ is a random sequence created by using a pseudorandom number generator (PRNG) seeded with a secret key SK, where $r_j \in [0, 255]$. For each block B_j, its corresponding authentication data a_j is constructed by the following Equation:

$$a_j = f_j \bigoplus r_j \tag{7}$$

where, $\bigoplus$ denotes the XOR operation. Each resultant 8-bit authentication data is embedded into the 8 LSBs of the corresponding image block, and the watermarked image I' is thus obtained. Finally, the set of cluster centers x acquired after performing the RKM clustering on image I, and the secret key SK should be kept securely by the image owner for further tamper detection.

4.3 Tamper detection phase

The possibly distorted image I'', as in the authentication data embedding procedure, is first divided into non-overlapping 2×2 blocks $B''_j (1 \leq j \leq \frac{M}{2} \times \frac{M}{2})$. By verifying the watermark embedded in each image block, we can determine whether an image block has

been tampered with.

To perform tamper detection, the embedded watermark sequence, $A = \{a_1, a_2, \ldots, a_{\frac{M}{2}\times\frac{M}{2}}\}$ is extracted from all the blocks of image I'', and then the two LSBs of all the pixels within each block are set to zero. Employing the set of cluster centers x kept by the image owner, to all blocks a feature sequence $F'' = \{f_1'', f_2'', \ldots, f_{\frac{M}{2}\times\frac{M}{2}}''\}$ can be derived by

$$f_j'' = \frac{d(B_j'', x_i)}{d(B_j'', x_m) - d(B_j'', x_i)} \tag{8}$$

When $f_j'' < .1$ then $f_j'' = 0$ otherwise $f_j'' = 1$. Let $R = \{r_1, r_2, \ldots, r_{\frac{M}{2}\times\frac{M}{2}}\}$ be a random sequence created by using the PRNG seeded with the secret key SK kept by the image owner, where $r_j \in [0, 255]$. The authentication data sequence $A'' = \{a_1'', a_2'', \ldots, a_{\frac{M}{2}\times\frac{M}{2}}''\}$ corresponds to image I'' can be computed by applying f'' and R to Eq.(7). Finally, the legitimacy of each block B_j'' can be recognized by comparing a_j'' with a_j. If they are the same, B_j'' is a legitimate block; otherwise, B_j'' is regarded as a tampered block.

5 Experimental results and analysis

Various experiments are carried out in this section to demonstrate the validity of the proposed fragile watermarking approach. In this implementation we set k =3, and w_{lower} and threshold are evolved on the run by employing a EPSO algorithm. We find that the performance of the algorithm is dependent on the choice of parameters especially in decreasing the time of implementation.

For quantitative evaluation, peak signal-to-noise ratio (PSNR) was used to measure the image quality of the watermarked image I' in comparison with the original image I. Also, the true positive (TP) and false positive (FP) rates were used to measure the accuracy of tamper detection and localization, where the TP rate is the proportion of actual tampered pixels that were correctly reported as tampered pixels and the FP rate is the proportion of actual non-tampered pixels that were erroneously reported as tampered pixels.

5.1 Performance evaluation

5.1.1 Performance under cut-and-paste attack

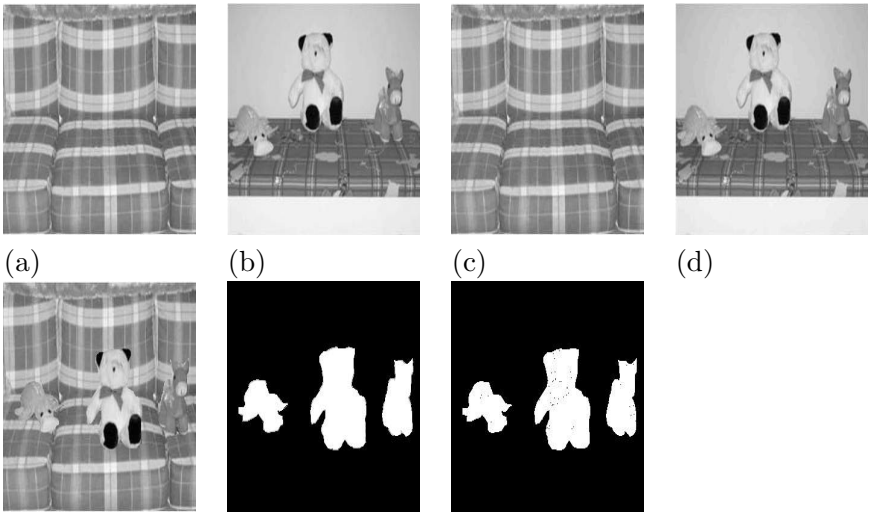
In this experiment, to simulate the cut-and-paste attack, the content of a watermarked image was modified by cutting regions from the same or another watermarked image and pasting them together to form a new image. We used 8-bit grayscale images, Pool image of size 256×256. It was used to simulate the cut-and-paste attack. Figure (2a) shows the original image and their corresponding watermarked image are shown in Figure (2b). From the figure (2) we observe that the watermarked Pool image was tampered by copying one black ball and one white ball from the watermarked image and pasting them into the same image.

(a) (b) (c) (d) (e)

Fig. 2 (a) Original pool image; (b) watermarked pool image; (c) tampered pool image; (d) ground truth image; (e) tamper detection result.

5.1.2 Performance under collage attack

To evaluate the performance under collage attack, a counterfeit image is formed by combining the portions of multiple watermarked images, while preserving their relative spatial location within the target image. Sofa and Doll images given in Figs. 3a, 3b respectively are used to evaluate the performance under the collage attack. The size of both images are 320×240 pixels. Figs. 3c and 3d show the corresponding watermarked images. The collage image, as shown in Fig. 3e, was created by copying the three dolls from Fig. 3d and pasting them in Fig. 3c. The ground truth of tampered regions and the tamper detection result are shown in Figs. 3f, 3g respectively.



(a) (b) (c) (d)

(e) (f) (g)

Fig. 3. (a) Original sofa image; (b) original doll image; (c) watermarked sofa image; (d) watermarked doll image; (e) tampered sofa image; (f) ground truth image; (g) tamper detection result.

5.2 Performance comparisons and analysis

Table (1) shows the comparison results of image quality, the value of PSNR of watermarked images in the proposed method is greater than the value of PSNR of watermarked images in Chen and Wang's [3] approach and is the same value of El-Bakrawy et al.'s [5] approach. It means that the watermarked image of our proposed method have better image quality. Table (2) shows that the proposed algorithm needs little time to make fragile watermarking approach with a block-wise dependency mechanism compared with El-Bakrawy

Table 1. Comparison results of PSNR of watermarked images.

Image	El Bakrawy et al's approach	Chen and Wang's approach	Proposed approach
Pool	46.53	44.48	46.53
Sofa	45.99	44.14	45.99
Doll	46.03	44.20	46.03

Table 2. Comparison results of time of implementation.

Image	Rough k_mean	Rough k_mean and PSO	Rough k_mean and EPSO
Pool	5.16	4.19	1.9
Sofa	38.64	15.95	4.05
Doll	3.4	6.15	1.6

et al. because in proposed algorithm we used PSO to determine lower approximation and threshold value. Also, we apply EPSO to determine lower approximation and threshold value and compare between them. Results show that applying EPSO makes time lesser than applying only PSO and El-Bakrawy et al.'s approach in all images but applying PSO makes time lesser than [5] in both pool and sofa images.

The comparison results of tamper detection are listed in Table (3). The results demonstrate that the proposed approach outperforms Chen and Wang's approach approaches [3] in both TP and FP rates but has the same values as in [5]. Furthermore, the results show that the proposed approach can completely resist collage attack, as all the blocks which have been modified by collage attack can be correctly identified by our approach.

6 Conclusions

In this paper, the proposed fragile watermarking approach is presented. It can detects and locates any modification of the embedded image if it is tampered. Realizing that the basic requirement of thwarting counterfeiting attacks is to break blockwise independency, the proposed approach used rough set k-means and exponential particle swarm optimization (EPSO) systems. It is based on a block-wise dependency mechanism which can detect any alterations made to the protected image. Initially, the input image is divided into blocks with equal size in order to improve image tamper localization precision. Then feature sequence is generated by applying rough k-means and EPSO clustering to create the relationship between all image blocks and cluster all of them since EPSO is used to opti-

Table 3. Comparison results of tamper detection.

Image	El-Bakrawy et al. approach		Chen and Wang's approach		Proposed approach	
	TP (%)	FP (%)	TP (%)	FP (%)	TP (%)	FP (%)
Pool	99.72	0.004	99.71	0.32	99.72	0.004
Sofa	98.77	0.11	99.30	0.81	98.77	0.11

mize the parameters of rough k-means. Both feature sequence and generated secret key are used to construct the authentication data. Each resultant 8-bit authentication data is embedded into the eight least significant bits (LSBs) of the corresponding image block. We gives experimental results which show the feasibility of using these optimization algorithms for the fragile watermarking and demonstrate the accuracy of the proposed approach. The performance comparison of the approach was also realized. The performance of a fragile watermarking approach has been improved in this paper by using exponential particle swarm optimization (EPSO) to optimize the rough k-mean parameters. The proposed approach can embed watermark without causing noticeable visual artifacts, and does not only achieve superior tamper detection in images accurately, it also recovers tampered regions effectively. In addition, the results show that the proposed approach can effectively thwart different attacks, such as the cut-and paste attack and collage attack, while sustaining superior tamper detection and localization accuracy.

References

[1] Chang C., Chen K., Lee C., and Liu L., A secure fragile watermarking approach based on chaos-and-hamming code. The Journal of Systems and Software, vol.2, pp. 1-9, 2011.

[2] Chan C.S., and Chang C.C., An efficient image authentication method based on Hamming code. Pattern Recognition, vol. 40, pp. 681-690, 2007.

[3] Chen W.C., and Wang M.S., A fuzzy c-means clustering-based fragile watermarking approach for image authentication. Expert Systems with Applications, vol. 36, pp. 1300-1307, 2009.

[4] Rawat S., and Raman B., A chaotic system based fragile watermarking approach for image tamper detection. International Journal of Electronics and Communications (AE), vol. 16, pp. 1-8, 2011.

[5] El Bakrawy L., Ghali N., Hassanei, A., Kim T., A Rough K-means Fragile Watermarking Approach for Image Authentication. Proceedings of the Federated Conference on Computer Science and Information Systems, pp. 19-23, 2011.

[6] Hassanien A, Abraham A., Peters J.F., and Kacprzyk J., Rough sets in medical imaging: foundations and trends. Computational Intelligence in Medical Imaging: Techniques and Applications, G. Schaefer et al. (Eds.), CRC Press, USA, ISBN 978-1-4200-6059-1, Chapter 3, pp. 47-87, 2008.

[7] Lingras P., Applications of rough set based K-means. Kohonen SOM, GA clustering. Transactions on Rough Sets, Lecture Notes in Computer Science, vol. 2, pp. 120-139, 2007.

[8] Lingras P., Interval set clustering of web users with rough K-Means. Journal of Intelligent Information Systems, vol. 23, pp. 5-16, 2004

[9] Pawlak Z., On Rough Sets, Bulletin of the European Association for Theoretical Computer Science. no.24, pp. 94-109, 1984.

[10] Aboul Ella Hassanien: A Copyright Protection using Watermarking Algorithm. Informatica, Lith. Acad. Sci. 17(2), pp.187-198, 2006.

[11] Lin C., and Chang S., A robust image authentication method surviving JPEG lossy

compression. Proceedings of SPI Einternational conference on storage and retrieval of image/ video database, vol. 3312, pp. 296-307, 1998.

[12] Pawlak Z., Skowron A., Rough Sets and Conflict Analysis. Studies in Computational Intelligence (SCI), vol. 37, pp. 35 74,2007.

[13] Pawlak Z., Skowron A., Rough sets: Some extensions. Information Sciences, vol. 177, pp. 28-40, 2007.

[14] Li C., and Yuan Y. , Digital watermarking approach exploiting nondeterministic dependence for image authentication. Optical Engineering, vol. 45(12), 2006.

[15] Zhang X., Wang S., Qian Z., and Feng G., Reversible fragile watermarking for locating tampered blocks in JPEG images. Signal Processing, vol. 90, pp. 3026-3036, 2010.

[16] Own H. S., Al-Mayyan W., Zedan H., Biometric-Based Authentication System Using Rough Set Theory. LNAI, vol. 6086, pp. 560569, 2010.

[17] Penga F., Guoa R., Li C., Long M., A semi-fragile watermarking algorithm for authenticating 2D CAD engineering graphics based on log-polar transformation. Computer-Aided Design, vol. 42, pp. 1207-1216, 2010.

[18] Qi X., and Xin X., A quantization-based semi-fragile watermarking approach for image content authentication. J. Vis. Commun. Image R., vol. 22, pp. 187-200, 2011.

[19] Hung C., Purnawan H., A Hybrid Rough K-Means Algorithm and Particle Swarm Optimization for Image Classification. Advances in Artificial Intelligence, Lecture Notes in Computer Science, vol. 5317, pp. 585-593, 2008.

[20] Cui X., Potok T., and Palathingal P., Document Clustering using Particle Swarm Optimization. the IEEE Swarm Intelligence Symposium USA, Vol. 10, pp. 185-191, 2005.

[21] Merwe DW., Engelbrecht AP., Data Clustering using Particle Swarm Optimization. IEEE Congress on Evolutionary Computation, Australia, Vol. 1, pp. 215-220, 2003.

[22] Ghali N., El-Dessouki N., A. N. Mervat, El Bakrawy L, Exponential particle swarm optimization approach for improving data clustering. International Journal of Electrical and Electronics Engineering Chance, Vol. 3, pp. 208-212, 2009.

[23] Jain A., Murty M., Flynn P., Data Clustering: A Review. ACM Computing Surveys, Vol. 31, pp. 265-325, 1999.