ISSN–2278-5655

AMIERJ

AARHAT MULTIDISCIPLINARY INTERNATIONAL EDUCATION RESEARCH JOURNAL

Volume–X, Issues– III May - June 2021

SELECTION OF OPTIMAL FEATURE REGION SET BASED ON SIMULATED ATTACKING AND MDKP TECHNIQUES

S. Krishnaveni

Assistant Professor,

Department of Computer Applications,Don Bosco College of Arts and Science

MS Univesity,Tirunveli.Tamilnadu,India.

M. A. Arul Rozario

Dean, Don Bosco Polytechnic College, Directorate of Technical Education,

Kazhiappanallur,Tharangambadi, Nagapattinam Dt, Tamilnadu, India

Abstract

"Selecting Optimized feature region set for digital image using Algorithm" is discussed here. Enhancement of a digital watermarking algorithm is denoted by the robustness of embedded watermarks against various attacks. Method based on the simulated attacking and the GA-based MDKP solving procedure is developed to select the most adequate feature regions for robust digital image watermarking under the constraint of preserving image quality. Finally, we select most robust region from selected primary feature regions using generic algorithm.

Keywords— *feature detection, genome, mutation*

Introduction

The main goal is to find most robust region from simulated attacking, regions which can sustain the many attacks are considered as most robust region and we proved that the selected regions can retain watermark for both kind of attacks, such as geometric attacks and signal processing attacks. A watermarked feature region may have different degrees of protection against different attacks. It would be helpful to find out the most robust regions if there is priorinformation of each region's attack resistance capability. As a result, we propose a feature region selection method based on the idea of simulated attacking and multidimensional

ISSN–2278-5655

AMIERJ

AARHAT MULTIDISCIPLINARY INTERNATIONAL EDUCATION RESEARCH JOURNAL

Volume–X, Issues– III May - June 2021

knapsack problem (MDKP) optimization techniques. This technique can be integrated into the feature-based watermarking schemes to ensure their robustness against various types of attack. Finally track-with prune algorithm is used to find out most robust region from primary feature set.

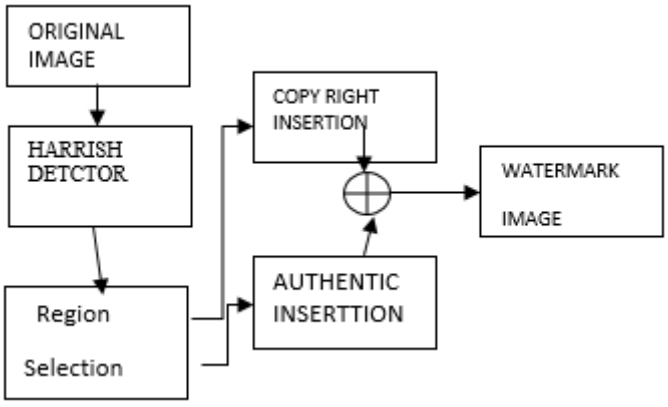
Related work

A. Feature regions selection

Harris-Laplacian detector is used to select the feature regions set (high frequency regions). **Harris affine region detector** belongs to feature detection. Feature detection is a pre-processing step of several algorithms that rely on identifying characteristic points or interestpoints so to make correspondences between images, recognize textures, categorize objects or build panoramas.

B. Watermarking Insertion

In this module watermark or data hide or embed on selected regions set is performed using Digital Wavelet Transform. The main intension to watermark on only high frequency region because high frequency regions are most robust, it can with stand many attacks but not low frequency regions; generally Key is used in order to protect the secret data. PSNR is calculated to check the quality of the image, the main goal here is to obtain PSNR value more.



A block diagram of the proposed feature region selector is shown above, where its input is the region set obtained by a feature detector, and the output is a set of robust feature regions selected. The first operational stage is responsible to find out a minimal feature region set under the objective of resisting as many predefined attacks as possible. Here, a track-with-pruning algorithm is

ISSN–2278-5655

AMIERJ

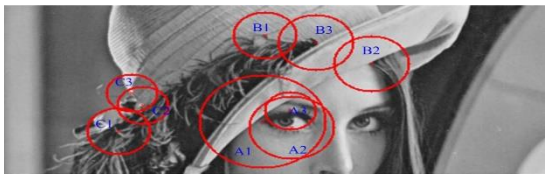
AARHAT MULTIDISCIPLINARY INTERNATIONAL EDUCATION RESEARCH JOURNAL

Volume–X, Issues– III May - June 2021

developed to seeking for the optimal solution. In the second operational stage, the primary feature set is extended by a genetic algorithm-based search procedure to enhance its robustness to undefined attacks.

Proposed Work

A.Primary Feature Set Searching Stage



As shown in Fig., at first, the watermark sequence is pseudo randomly generated and repeatedly embedded into the feature regions in the watermark insertion phase. Then, a few representative attacks are applied to the watermarked feature regions for evaluating their robustness in the simulated attacking phase. The attacks are difficult to be formulated by a common model because of their diverse characteristics. In our experiment, they are generated from the Stir Mark benchmark program including JPEG, Median Filter, Sharpening Filter, Rotation, Scaling, and Cropping. The attack resistance analysis phase is implemented by a two-step method. In this phase, the original feature regions are first checked if they can be re-detected in the attacked image.

The watermark $W_r$embedded in each successfully redetected region is then extracted to examine the consistency (bit error) between itself with the original watermark W. Using$d_{r,a}$ to indicate whether the region can resist the predefined attack or not, it is defined as

$$d_{r,a} = \begin{cases} 1, & BER(W, W_r) \leq T \\ 0, & otherwise \end{cases} \quad (1)$$

Where $BER(W, W_r)$ denotes the bit error between W and W_r.

is a predefined bit error threshold T.

Bit Rate

The bit rate of a watermark refers to the amount of information a watermark can encode in a signal. This is especially important for public watermarks.

ISSN–2278-5655

AMIERJ

AARHAT MULTIDISCIPLINARY INTERNATIONAL EDUCATION RESEARCH JOURNAL

Volume–X, Issues– III May - June 2021

In the final phase, the most robust and smallest set of nonoverlapping feature regions is selected according to the result of attack resistance analysis. This work is formulated as follows:

$$R_p^* = \arg\max \mathrm{Rp}\ \{\ \sum_{i=1}^{Na} x_{ai}^{Rp} \min \mathrm{Rp}\ ; \quad \forall \mathrm{rk}, \mathrm{r_j} \in \mathrm{R_p}, \mathrm{k} \neq \mathrm{j} \rightarrow \mathrm{r_k} \cap \mathrm{r_j} = \emptyset\} \qquad (2)$$

where $\mathrm{R_p}$is the set of selected feature regions in which any tworegions $\mathrm{r_k}$ and$\mathrm{r_j}$ are not overlapped, and the value of x_{ai}^{Rp} for a predefined attack a_i is determined by

$$x_{ai}^{Rp} = \begin{cases} 1, \exists r \in R_p, d_{r,ai} \neq 0 \\ 0, otherwise \end{cases} \qquad (3)$$

R_p^* is R_p the satisfying with the maximum value of $\mathrm{a_i}$. A track-with-pruning algorithm is proposed to carry out the work of this phase, and the symbols used in this algorithm.

B. Feature Set Extension Stage

By the previous stage, an optimal feature region set is chosen for watermarking to hold out against the predefined attacks. Because this set may fail to protecting some non-predefined attacks, we need to add some auxiliary regions selected from those residual feature regions to enhance the robustness of watermarked image against undefined attacks under preserving its visual quality. The symbol $g_r^a$is defined to indicate the overall resistance degree of the region r against all predefined attacks, and it is determined by

$$g_r^a = \left(d_{r,a1} + d_{r,a2} + \cdots + d_{r,aNa}\right) = \sum_{i=1}^{Na} d_{r,ai} \qquad (4)$$

Where $d_{r,ai} \in \{0,1\}$ and indicates if the region r can resistthe ith predefined attack a_i , and N_a is the total number of predefined attacks. The resistance of a region against a predefined attack is regarded as a possible characteristic of the region r against all predefined attacks, and it is determined by

$$g_r^a = \left(d_{r,a1} + d_{r,a2} + \cdots + d_{r,aNa}\right) = \sum_{i=1}^{Na} d_{r,ai} \qquad (4)$$

Where $d_{r,ai} \in \{0,1\}$ and indicates if the region r can resistthe ith predefined attack a_i , and N_a is the total number of predefined attacks. The resistance of a region against a predefined attack is regarded as a possible characteristic of the region. The symbol g_r^a is the

ISSN–2278-5655

AMIERJ

AARHAT MULTIDISCIPLINARY INTERNATIONAL EDUCATION RESEARCH JOURNAL

Volume–X, Issues– III May - June 2021

summary representation of N_a characteristics of a region. The two generic characteristics of feature regions, the corner response and the integration scale, since we cannot exclude the possibility that there are undefined attacks with the characteristics never occurred in the predefined attacks. We use a binary symbol g_r^σ to indicate whether the scale value of a region belongs to the middle-scale band or not. The range of the middle-scale band is determined according to the suggestion. Therefore, the work of the extension stage can be formulated as an optimization problem with multiple constraints as follows,

$$Maximize \quad \sum_{j=1}^{Rp^*} (g_{rj}^a + g_{rj}^c + g_{rj}^\sigma) s_{rj} \qquad (5)$$

$$subject\ to, \quad \sum_{j=1}^{R_p^*} q_{rj}\, s_{rj} \leq Q_c$$

$$\sum_{j=1}^{R_p^*} P_{ri,rj}\, s_{ri}\, s_{rj} \ < 1, i = 1,2, \dots, \left|R_p^*\right| \qquad (6)$$

where R_p^* is the number of feature regions except those in the primary feature set as well as the regions overlapped with them, and s_{rj} is defined as

$$s_{rj} = \begin{cases} 1, & if\ the\ region\ r_j\ is\ selected \\ 0, & otherwise \end{cases} \qquad (7)$$

The summation is used in (5) since the properties denoted by the symbols represent the characteristics of the region and they are equally important. It is better to select a region with better properties which indicate higher possibility to resist undefined attacks. Equation (6) is used to formulate the constraint that no region overlapped with any one of the selected regions can be selected. The value $p_{ri,rj}$ of indicates whether the two regions

$$= \begin{cases} 1, & r_i \cap r_j \neq \emptyset \\ 0, & otherwise \end{cases} \qquad (8)$$

The variable, q_{rj} , denotes the distortion of a watermarked region, r_j . The parameter, Q_c , denotes the limitation of quality degradation of an image after being watermarked, and is determined by considering the peak signal-to-noise ratio(PSNR) value between a cover image and a watermarked image.

ISSN–2278-5655

AMIERJ

AARHAT MULTIDISCIPLINARY INTERNATIONAL EDUCATION RESEARCH JOURNAL

Volume–X, Issues– III May - June 2021

The optimization problem formulated by (5) and (6) can be transformed into a MDKP that is a knapsack problem with a collection of different constraints or one multidimensional constraint, as defined by,

$$Maximize \quad \sum_{j=1}^{Rp^*} \left(g_{rj}^{a} + g_{rj}^{c} + g_{rj}^{\sigma}\right) s_{rj} \qquad (9)$$

$$subject\ to, \quad \sum_{j=1}^{R_p^*} w_{k,rj}\, s_{rj} \leq C_k, \quad k = 1,2,\ldots,m \qquad (10)$$

where m -constraints are involved in (6) and $m = 0.5\left(R_p^{*\,2} - |R_p^*|\right) + 1.$ The variables $w_{k,rj}$ and C_k represent the composite weights and constraints of quality distortion and overlapping conditions illustrated in (6).

Proposed Algorithms

A.**Track-With Pruning**

1. Input: All feature regions detected by feature detector, R_0.
2. Output: primary feature set, R_p^*.
3. /* Initialize associated parameters and set the size of inspected feature region sets as one. */

$$R_p \leftarrow \emptyset, R_{prune} \leftarrow \emptyset, M \leftarrow \sum_{i=1}^{N_a} x_{a_i}^{R_p}, M_o \leftarrow \sum_{i=1}^{N_a} x_{a_i}^{R_p}, K \leftarrow 1.$$

4. /*Check if the termination condition is satisfied. */

$$\textbf{while}\left((K \leq |R_o|)\text{and}(M \neq M_o)\right)$$

5. /*Find the candidate feature region sets with the cardinality equal to current K value and satisfying the two conditions that Each feature region in the set is non-overlapped.

All elements of its power set are not in the pruned set. */

select R_q from $P(R_o)$, where

$$R_q = \left\{R_{qv} \middle| |R_{qv}| = K; \forall r_k, r_i \in R_{qv}, K \neq i \rightarrow r_k \cap r_i = \emptyset; P\left(R_{qv}\right) \cap p_{prune} = \emptyset\right\}$$

6. for $v \leftarrow 1\ to\ |R_q|$
7. /* candidate set is included in the pruned set while it cannot resist more attacks by adding

ISSN–2278-5655

AMIERJ

AARHAT MULTIDISCIPLINARY INTERNATIONAL EDUCATION RESEARCH JOURNAL

Volume–X, Issues– III May - June 2021

more feature regions.*/

$$\textbf{if}\left(\sum_{i=1}^{N_a} x_{a_i}^{R_{qv}} == \sum_{i=1}^{N_a} x_{a_i}^{R_{qv} \cup \tilde{R_{qv}}}\right)$$

8. **then** $R_{prune} \leftarrow \{R_{qv}\} \cup R_{prune}$
9. **end-if**
10. /* Update the primary feature region set with a candidate feature region set if the latter can resist more attacks than the former. */

$$\textbf{if}\left(M < \sum_{i=1}^{N_a} x_{a_i}^{R_{qv}}\right)$$

11. then $R_p \leftarrow R_{qv}$
12. $M \leftarrow \sum_{i=1}^{N_a} x_{a_i}^{R_p}$
13. end-if
14. end-for
15. /* Increase the cardinality of inspected feature region sets for further searching.*/ K← K+1
16. end-while
17. $R_p^* \leftarrow R_p$

B. GeneticAlgorithm

In our project Genetic algorithm is used for the final selection of the feature set. A **genetic algorithm (GA)** is a searchheuristic that mimics the process of natural evolution. This heuristic is routinely used to generate useful solutions to optimization and searchproblems. Genetic algorithms belong to the larger class of evolutionary algorithms (EA), which generate solutions to optimization problems using techniques inspired by natural evolution, such as inheritance, mutation, selection, and crossover.

To use a genetic algorithm, you must represent a solution to your problem as a *genome* (or *chromosome*). The genetic algorithm then creates a population of solutions and applies genetic operators such as mutation and crossover to evolve the solutions in order to find the best one(s). This presentation outlines some of the basics of genetic algorithms.

ISSN–2278-5655

AMIERJ

AARHAT MULTIDISCIPLINARY INTERNATIONAL EDUCATION RESEARCH JOURNAL

Volume–X, Issues– III May - June 2021

C. False-Positive Analysis

The bit error threshold T which determines the presence of a target watermark in a region is generally decided by examining the false positive rate. Define PFA_{Bit} as the false-positive rate of a watermark bit from its corresponding repeating bits, and assume each extracted repeating bit is an independent random variable with probability 0.5. Then, based on the Bernoulli trials, PFA_{Bit} can be calculated by

$$PFA_{Bit} = \sum_{i=\left\lceil \frac{t+1}{2} \right\rceil}^{t} \binom{t}{i} (0.5)^i \ (0.5)^{t-i} \qquad (11)$$

where is the repeating times and the $\lceil . \rceil$ is a ceiling function that outputs the smallest integer greater than or equal to a real argument. To judge the existence of watermark in a region, we check if the bit error between the detected watermark sequence and the original watermark sequence is smaller than T . The false positive rate of detecting the watermark from a feature region, PFA_W, is given by

$$PFA_W = \sum_{i=Lw-T}^{t} \binom{Lw}{i} (PFA_{Bit})^i \ (1 - PFA_{Bit})^{Lw-i} \qquad (12)$$

where L_w is the length of the detected watermark sequence. The detection of watermark for each region is performed by locally searching times to tackle the problem of feature detection errors. If there is at least one successful detection,the region is claimed as watermarked. Therefore, the false-positive rate of each feature region, PFA_R, is PFA_W. Finally, the existence of watermarks in an image is determined by the condition which there are at least regions successfully detected as watermarked. That is, the false positive rate of an image, PFA_{Image} , can be calculated by

$$PFA_{Image} = \sum_{i=l}^{N_R} \binom{N_R}{i} (PFA_R)^i \ (1 - PFA_R)^{N_R - i} \qquad (13)$$

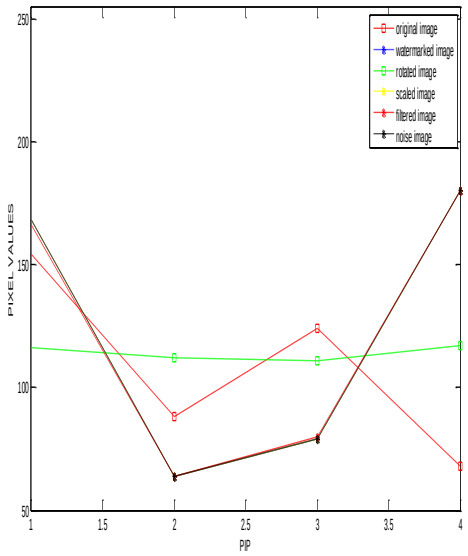
Result Analysis

ISSN–2278-5655

AMIERJ

AARHAT MULTIDISCIPLINARY INTERNATIONAL EDUCATION RESEARCH JOURNAL

Volume–X, Issues– III May - June 2021



In the experiment of this paper, the local search is performed 25 times (five for orientation and five for location), and the threshold is set as 30 to keep the low false positive rate of an image. Accordingly, the probability of successful detecting at least one watermark region from an unwatermarked image is depends on selected regions.

Conclusions

A novel method based on the simulated attacking approach and the GA-based MDKP solving procedure is developed to select the most adequate feature regions for robust digital image watermarking under the constraint of preserving image quality. Compared with other feature-based watermarking methods, the robustness against various attacks is significantly improved by the proposed method, and the image quality after watermarking is still preserved. It may be considered that our method consumes too much computation time in measuring the robustness of feature regions due to the simulated attacking. But in practice, according to the experimental results, this is not a concern if the adopted predefined attacks are representative, since a small number of candidate feature regions will be sufficient to reach full robustness.

References

I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, “Secure spread spectrum watermarking for multimedia,” *IEEE Trans. Image Process.*, vol. 6, no. 12, pp. 1673–1687, Dec. 1997.

C. S. Lu, S. K. Huang, C. J. Sze, and H. Y. Mark Liao, “Cocktail watermarking for digital image protection,” *IEEE Trans. Multimedia*, vol. 2, no. 4, pp. 209–224, Dec. 2000.

ISSN–2278-5655

AMIERJ

AARHAT MULTIDISCIPLINARY INTERNATIONAL EDUCATION RESEARCH JOURNAL

Volume–X, Issues– III May - June 2021

I. J. Cox, M. L. Miller, and J. A. Bloom, *Digital Watermarking*. San Francisco, CA: Morgan Kaufman, 2001.

D. Zheng, S. Wang, and J. Zhao, "RST invariant image watermarking Algorithm with mathematical modeling and analysis of the watermarking Processes," *IEEE Trans. Image Process*, vol. 18, no. 5, pp.1055–1068, May 2009.

K. Mikolajczyk and C. Schmid, "A New Approach for Optimal Multiple Watermarks Injection",*Int. J. Computer Vision*, vol. 60, no. 1, pp. 63–86, Oct.2004.