Watermarking Stack of Grayscale Face Images as Dynamic Multi-Objective Optimization Problem

Bassem S. Rabil, Robert Sabourin, and Eric Granger

Laboratoire d’Imagerie, de Vision, et d’Intelligence Artificielle
École de Technologie Superiérie (ÉTS), University of Quebec
1100, rue Notre-Dame Ouest, Montreal, QC H3C 1K3, Canada.

Abstract. Face images have been used in many access control applications to recognize individuals. Protecting face biometric templates against unauthorized digitization and manipulations is the main challenge in such applications. Intelligent watermarking addresses these challenges using optimization techniques to find the optimal embedding locations to maximize both watermark quality and robustness. Watermark quality measures the distortion resulting from watermark embedding, and robustness represents the resistance to different manipulations on watermarked image. The computational complexity of optimizing embedding for large stack of high resolution grayscale face images is high. In this paper, we propose to handle the overall optimization for stack of face images as one dynamic multi-objective problem rather than series of static problems. It is proposed to use multi-objective optimization to optimize simultaneously watermark quality and robustness in dynamic environment using incremental learning techniques. Experimental results show significant computational complexity reduction to find near optimal solutions for watermark optimization.

Keywords: biometrics, bio-watermarking, dynamic optimization, intelligent watermarking, multi-objective optimization, incremental learning

1 Introduction

Biometrics are the means to recognize individuals using intrinsic physical or behavioral characteristics. Many countries have become strong advocates of biometrics with the increase in fear of terrorism since September 11, 2001. Recently biometrics is synergistically merged into the digital watermarking technology to secure biometric templates, also to hide biometric traits invisibly inside other biometric templates to improve recognition rates using multiple biometrics traits [12]. Digital watermarking is deployed in many domains to assure integrity and authenticity of the original signal via fragile and robust watermarking respectively. A fragile watermark [14] is a type of watermark to ensure integrity, but it is broken if the watermarked image is manipulated or altered, while the robust
watermark [14] ensures authenticity and can be extracted after manipulating the watermarked image. Semi-fragile watermark considered in this paper is satisfying a trade-off between both quality measuring the distortion introduced with watermark embedding, and robustness representing the resistance to different manipulations to watermarked images. Different optimization techniques have been proposed in intelligent watermarking literature to satisfy this trade-off between watermark quality and robustness. Optimization problem can be either formulated as Single Objective Optimization Problem (SOOP), or Multi-Objective Optimization Problem (MOOP) which is considered in this paper. Optimization problem aims to tune watermark embedding parameters to maximize both quality and robustness.

Intelligent watermarking of a stack of high resolution face grayscale images satisfying both watermark quality and robustness involves high computational complexity optimization problems. Intelligent watermarking a single high resolution grayscale face image can take several hours of processing, and thus increasing number of face images would threat the feasibility of this computationally expensive process in real life access control applications. In this paper, we present a novel formulation for the optimization problem of the stack of face grayscale images as single dynamic multi-objective optimization problem rather than series of static optimization problems. The optimization environment changes whenever a new face image is fed into the proposed watermarking system, and stays unchanged during optimizing embedding the watermark of this image. This novel formulation assumes that the stack of images to be watermarked has images of similar content and thus the optimization problems of these images has many similarities.

Experimental results show large computational complexity reduction to find near optimal solutions compared to much higher computational cost to find optimal solutions. The trade-off between the computational complexity and the quality of solutions produced is demonstrated in experiments for the proposed approach and the baseline system. The proposed formulation will have many applications in access control domain especially for systems involving recognition of large number of individuals using their high resolution face images. It can be generalized easily to color face images by applying the same formulation for different color channels.

The rest of the paper is organized as follows: Section 2 introduces different aspects of intelligent watermarking, bio-watermarking, multi-objective formulation, and incremental learning, then Section 3 describes the experimental methodologies, algorithms, metrics, and databases used for computer simulations. Section 4 shows the the experimental results along with analysis for these results, and finally Section 5 lists conclusions of this work and proposed future research directions.
Watermarking Stack of Grayscale Face Images as Dynamic Multi-Objective Learning

2 Intelligent Watermarking using Dynamic Multi-Objective Population Based Incremental Learning

Watermark quality and robustness are commonly measured using Weighted Peak Signal-To-Noise Ratio (wPSNR) and Normalized Correlation (NC) respectively. These metrics are defined as shown in equations 3 and 4. Peak Signal-To-Noise Ratio (PSNR) is first calculated in Equation 2 between original image $X$ and watermarked image $X_c$ of dimension $M \times N$ using the Mean Squared Error (MSE) as in Equation 1. Weighted PSNR uses an additional parameter called Noise Visibility Function (NVF) which is a texture masking function defined by Voloshynovskiy et al. [15]. NVF arbitrarily uses a Gaussian model to estimate how much texture exists in any area of an image. For flat and smooth areas, NVF is equal to 1, and thus wPSNR has the same value of PSNR, for any other textured areas, wPSNR is slightly higher than PSNR to reflect the fact that human eye will have less sensitivity to modifications in textured areas than smooth areas.

$$MSE_c = \frac{1}{M \cdot N} \sum_{i=1}^{M} \sum_{j=1}^{N} (X(i,j) - X_c(i,j))^2$$  \hspace{1cm} (1)

$$PSNR_c = 10 \log_{10} \left( \frac{255^2}{MSE_c} \right) \text{ (dB)} \hspace{1cm} (2)$$

$$wPSNR_c = 10 \log_{10} \left( \frac{255^2}{MSE_c \times NVF} \right) \text{ (dB)} \hspace{1cm} (3)$$

The Normalized Correlation (NC) is calculated between embedded watermark $W(i,j)$ and the extracted watermark from the attacked image $W'(i,j)$ using Equation 4, where both watermarks have the dimensions $M_W \times N_W$.

$$NC = \frac{\sum_{i=1}^{M_W} \sum_{j=1}^{N_W} W(i,j) W'(i,j)}{\sum_{i=1}^{M_W} \sum_{j=1}^{N_W} [W(i,j)]^2}$$  \hspace{1cm} (4)

Most digital watermarking techniques proposed for grayscale images use different transform domains to embed a watermark that minimizes the visual impact, and to deal with the uncorrelated coefficients in the transform domain. The most commonly used transform domains in watermarking literature are Discrete Cosine Transform (DCT) [13] and Discrete Wavelet Transform (DWT) [8]. Using DCT transform inheriting robustness against JPEG compression which is based on DCT transform as well, the host image is divided into small blocks of pixels (8x8 pixels), transformed to frequency domain, and watermark bits are distributed among these blocks by changing frequency bands coefficients of these blocks according to the value of the watermark bit to be embedded. Few authors have considered other transforms based on DFT [10] to improve robustness against geometric attacks since these transforms are more resistant to geometric manipulations.
Many authors have proposed aggregating both quality and robustness fitness into one objective for simplicity utilizing different aggregation weights for the objectives to resolve the issue of different scaling of these different types of objectives, and to favor one objective over the others using these weights. Shieh et al [13] have used Genetic Algorithm for optimizing the aggregated fitness for both quality and robustness, while Wang et al [16] have used Particle Swarm Optimization for optimization. Other authors [8] have proposed combining both GA and PSO for optimizing the aggregated fitness for quality and robustness. Different formulations for watermark embedding optimization have been evaluated and compared in literature [11]. Multi-objective formulation corresponds to the trade-off among different quality and robustness objectives. It provides multiple optimal non-dominated solutions (Pareto front) which gives a system operator the ability to choose among multiple solutions to tune the watermarking system resolving the challenge pointed out in [6].

Fig. 1. Intelligent watermarking using multi-objective optimization module with aggregation of different robustness objectives.

The optimization problem can be formalized in equation 5 and figure 1, where \( n \) represents the dimension of the optimization problem, \( m \) is the number of attacks considered for robustness objectives, and \( x_1, x_2, ... , x_n \) represent embedding frequency coefficient indices. The constraints considered ensures avoiding DC coefficient for embedding, and also avoiding repeating the same embedding coefficients for the same image block.
maximize Quality \((x_1, x_2, ..., x_n)\)

maximize Robustness_{eq} \((x_1, x_2, ..., x_n)\)

subject to constraints

\[63 > x_1, x_2, ..., x_n > 1\]

\[repeat_{in\_same\_block} (x_1, x_2, ..., x_n) = 0\] (5)

Different robustness objectives \(Robustness_1, Robustness_2, ..., Robustness_m\) are proposed to be aggregated into \(Robustness_{eq}\) objective using aggregation based on Chebychev [3] as shown in equation 6.

\[f_{eq}(x) = \max_{i=1,...,N_{obj}} (1 - w_i). (f_i(x) - F_i) + K \sum_{i=1}^{n} w_i.f_i(x)\] (6)

where \(f_i\) is the objective function number \(i\) of the multiobjective optimization problem, \(N_{obj}\) is the number of objectives in the multiobjective optimization problem, \(w_i\) is the weight associated with the objective function number \(i\), \(x\) is the decision vector, and \(F_i\) refers to a limit on the objective \(f_i\) under which the values of \(f_i\) are interesting for the decision maker. \(K\) is a tunable coefficient, and \(f_{eq}\) is the equivalent single objective function. However in the experimentation, only one robustness objective for JPEG compression attack is considered to prove the concept of dynamic optimization simply.

Population Based Incremental Learning method proposed by Baluja in 1994 is developed by combining GA and competitive learning to reduce the difficulties on the crossover and mutation operations in a GA, while retaining the stochastic search nature of the GA. The salient feature of this technique is the introduction of a real valued probability vector. The value of each element of the vector is the probability of having a 1 in that particular bit position of the encoded chromosome. Population Based Incremental Learning (PBIL) [11] has proved efficiency with intelligent watermarking problem where utilizing the previous experience in subsequent generations ensures better convergence properties. Bureerat and Sriworamas [1] proposed changes to PBIL algorithm to handle multi-objective optimization problems. In this algorithm the probability vector is replaced with probability matrix, where each row in this matrix represents the probability vector to create sub-population of individuals. An external archive is proposed to be used to store the non-dominated solutions found throughout iterations.

In the case of multiobjective optimization, there is a set of non-dominated solutions representing Pareto Optimal Front (POF) as shown in figure 2. A solution vector \(x\) is said to dominate the other solution vector \(y\) if the following two conditions are true: The solution \(x\) is no worse than \(y\) in all objectives; and the solution \(x\) is strictly better than \(y\) in at least one objective.

Farina et al [4] have categorized the multi-objective problems in dynamic environments into four different types as shown in figure 3. The multi-objective
optimization of digital watermarking of grayscale images can be considered of Type II where both optimal decision variables and optimal objective values change when a new image is fed into the watermarking system. The optimization environment is assumed to change whenever a new face image is fed into the intelligent watermarking system, and it stays unchanged during optimizing this face image. The optimization environment is expected to have cyclic changes which implies that face images of similar content are expected to re-occur at later stage in the stack of face images.

3 Experimental Methodology

The watermark embedding/extracting algorithm used in experiments is an algorithm proposed by Shieh et al [13]. This algorithm is based on Discrete Cosine
Watermarking Stack of Grayscale Face Images as Dynamic Multi-Objective Transform (DCT) which has better robustness against JPEG compression attacks compared to Discrete Wavelet Transform (DWT) because JPEG is based on DCT transform as well. The main research problem shall stay the same for both DCT and DWT based algorithms, the main challenge is the high computational complexity of optimizing embedding using static optimization techniques. In the considered algorithm proposed by Shieh et al [13] the original cover image is not required during extraction of the watermark, this reduces the required space needed to store the original cover images. Using this algorithm, the cover image $X$ to be watermarked of size $M \times N$ is splitted into 8x8 blocks and transformed into DCT domain where the resultant matrix $Y_{m,n}(k)$ for each image block has the upper left corner as DC co-efficient and the rest of matrix are the AC coefficients, where the DCT coefficients are ordered in zigzag order. The DCT transformed image $Y_{m,n}(k)$ is then used to get the ratio between DC and AC coefficients $R(i)$ using the equation 7

$$R(i) = \frac{\sum_{m=1}^{M/8} \sum_{n=1}^{N/8} \frac{Y_{m,n}(0)}{Y_{m,n}(i)}}{i \in [1, 63]}$$  \hspace{1cm} (7)$$

Then polarities $P$ are calculated using the equation 8. Next, the watermarked DCT coefficient $Y'$ is obtained using the equation 9 with coefficients modified $\in F$ with the watermark $W_{m,n}$ and finally the watermarked image $X_c$ is obtained using the inverse DCT for $Y'$

$$P_{(m,n)}(i) = \begin{cases} 
1 & \text{if } (Y_{m,n}(i) \cdot R(i)) \geq Y_{m,n}(0) \\
0 & \text{otherwise;}
\end{cases}$$  \hspace{1cm} (8)$$

$$Y'_{m,n}(i) = \begin{cases} 
Y_{m,n}(i) & \text{if } P_{(m,n)}(i) = W_{m,n}(i) \\
(Y_{m,n}(0)/R(i)) + 1 & \text{if } P_{(m,n)}(i) = 0, W_{m,n}(i) = 1 \\
(Y_{m,n}(0)/R(i)) - 1 & \text{otherwise}
\end{cases}$$  \hspace{1cm} (9)$$

The embedding optimization module is using multi-objective PBIL algorithm proposed by Bureerat and Sriworamas [1] and the face database used is PUT face database [7]. High resolution face images implies higher embedding capacity and thus larger data to be embedded as watermarks. PUT database is the only available face database with high resolution homogeneous face images similar to passport images. Stack of 70 Face images are used in experiments where they are converted to grayscale and then downsized to resolution 512x384 using matlab imresize, and the embedded logo is BancTec binary logo of resolution 128x128 shown in figure 4 with embedding capacity 8 bits per image block. Only JPEG compression attack with quality factor 80% is considered in experiments for simplicity to prove the concept. PBIL optimization was performed using 24
individuals, with maximum number of iterations equals to 80, external archive maximum size is 40, and convergence is assumed if the Pareto front produced is the same for 20 iterations. Binary representation is used to encode optimization individuals, where each individual have binary representation of embedding frequency bands per image 8x8 block multiplied by number of blocks in the host image. Each frequency band is represented by 6-bits to identify the AC frequency coefficient (0-63) to embed the watermark in.

Algorithm 1

Multi-objective PBIL adapted from [1] with simple change detection mechanism based on aggregated fitness change of optimization individuals.
1: Initialize empty external Pareto set, and probability matrix whose elements are equal to ’0.5’
2: while Iteration < Max Iteration do
3: Generate a sub population with each row in probability matrix.
4: while Sub-population < Max number of sub-populations do
5: Evaluate the corresponding objective values to the generated populations to populate current_fitness(individuals).
6: if Iteration == 1 AND (current_fitness − previous_fitness)/previous_fitness < 7.5% then
7: Utilize current optimization landscape and break from optimization.
8: else
9: Change is assumed and proceed with full optimization.
10: end if
11: Take non-dominated members sorted from the union set of the current population and the old external Pareto set as new external Pareto set, if the external Pareto set is full, remove some solutions using adaptive grid algorithm where members in most crowded solution regions is removed iteratively.
12: In updating each row of the probability matrix, generate m weighting factors randomly where the sum of weights equals to ’1’, the binary solution from union set of current population and external Pareto set which gives the minimum weighted sum using the m weights is chosen to update the row probability vector.
13: end while
14: Save objective fitness of optimization individuals of the population previous_fitness(individuals) from current_fitness(individuals)
15: The probability matrix and external Pareto set are improved iteratively until stopping criteria is reached.
16: end while

In the experiments, a simple change detection mechanism based on average fitness changes of optimization individuals is used within the multi-objective PBIL shown in Algorithm 1 and equation 11.
Watermarking Stack of Grayscale Face Images as Dynamic Multi-Objective

Fig. 4. BancTec logo used as watermark to be embedded in face images.

\[ \text{Quality Change} = \sum_{i=1}^{\text{population size}} \frac{|\text{Quality}_{\text{iter } N}(i) - \text{Quality}_{\text{iter } N+1}(i)|}{\text{Quality}_{\text{iter } N}(i) \times \text{population size}} \]  
\[ \text{Robustness Change} = \sum_{i=1}^{\text{population size}} \frac{|\text{Robustness}_{\text{iter } N}(i) - \text{Robustness}_{\text{iter } N+1}(i)|}{\text{Robustness}_{\text{iter } N}(i) \times \text{population size}} \]  
\[ \text{Aggregated Change} = w1 \times \text{Quality Change} + w2 \times \text{Robustness Change} \]

The change detection uses weighted sum for fitness change percentage for both quality and robustness objectives to consider both objectives in the change detection, where \(w1\) and \(w2\) are set experimentally to 0.2 and 0.8 respectively as shown in figure 9. A threshold of 7.5% of aggregated fitness difference percentage for all optimization individuals is used to detect changes in the optimization landscape. If the aggregated fitness change percentage is over 7.5%, full optimization is performed, otherwise the optimization landscape of the previous face image is utilized for the new face image fed into the system. This threshold is concluded from experimentation for the aggregated fitness change percentage as concluded from figure 6. The computational complexity is measured using number of optimization iterations. And finally to compare the multiple solutions representing Pareto Optimal Front (POF) of the proposed approach and the baseline system, it is proposed to set threshold for quality fitness and find a single solution using this threshold for quality. It is proposed to set quality threshold of wPSNR to 42 dB to imply that distortion cannot be detected using Human Visual System (HVS)[15].

4 Results and Analysis

Experiments show that the proposed approach reduce computational complexity significantly specially with stacks of larger number of face images as shown in figure 5, and table 1. The reduction percentage is increasing with the number of face images in stack to reach around 97% for a stack of 70 grayscale face images. This reduction results from replacing full static optimization for most of face images in the stack with only one iteration only to detect major changes in the face image content. Detecting a major change in face image content would trigger
Fig. 5. Computational complexity reduction using proposed approach represented by number of optimization iterations.

Table 1. Computational complexity reduction for stacks of grayscale face images of different sizes using proposed approach.

<table>
<thead>
<tr>
<th>Number of Face Images in Stack</th>
<th>Baseline System No. of Iterations</th>
<th>Proposed System No. of Iterations</th>
<th>Computational complexity reduction</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>641</td>
<td>89</td>
<td>86%</td>
</tr>
<tr>
<td>20</td>
<td>1295</td>
<td>99</td>
<td>92%</td>
</tr>
<tr>
<td>30</td>
<td>1868</td>
<td>109</td>
<td>94%</td>
</tr>
<tr>
<td>40</td>
<td>2404</td>
<td>119</td>
<td>95%</td>
</tr>
<tr>
<td>50</td>
<td>3083</td>
<td>129</td>
<td>96%</td>
</tr>
<tr>
<td>60</td>
<td>3679</td>
<td>139</td>
<td>96%</td>
</tr>
<tr>
<td>70</td>
<td>4336</td>
<td>149</td>
<td>97%</td>
</tr>
</tbody>
</table>
full optimization, and otherwise the final optimization environment landscape of
the previous face image is utilized in the next face image.

Using quality threshold of wPSNR equals to 42 dB, figures 7, and 8 show
the fitness produced by proposed system versus baseline system for quality and
robustness respectively. The quality of solutions produced by the proposed ap-
proach is compared to those of baseline system using the fitness difference per-
centage between the proposed approach and baseline system when setting quality
threshold wPSNR to 42 dB as shown in figure 9. This confirms the efficiency of
the proposed approach when gaining 97% of computational complexity reduction
for a stack of 70 grayscale face images, and loosing only less than 10% of quality
fitness and 2% of robustness fitness for grayscale face images in the stack.

As shown in figure 6, relaxing the threshold constraint to 7.5% results in con-
sidering the whole stream with no changes detected. Constraining this threshold
to 4.5% shall result in 5 changes in faces 4, 6, 27, 32, and 37 and thus 5 addi-
tional full optimization. Using the threshold of 4.5% shall result in additional
400 iterations for the total iterations for the stream, which shall decrease the
computational complexity reduction of the proposed system for the stream of
70 images from 97% to 87%. When considering the face images which is as-
sumed to have changes when using the threshold as 4.5% in figure 9, the fitness
difference for both robustness and quality between the full optimization in the
baseline system and the proposed system is less than 5% for quality fitness and
2% for robustness fitness, and thus the additional full optimization would not
be justified in this case.
Fig. 7. Quality fitness produced by proposed system versus baseline system

Fig. 8. Robustness fitness produced by proposed system versus baseline system
5 Conclusion and Future Work

This paper presented a novel formulation for intelligent watermarking of stack of grayscale face images as single dynamic multi-objective optimization problem rather than series of static optimization problems. Experimental results show significant computational complexity reduction up to 97% to produce near optimal solutions. The quality of solutions produced using the proposed approach is comparable with the quality of solutions produced from the baseline system, especially with robustness fitness. The proposed approach enables mass watermarking of grayscale face images which is widely used in access control applications involving mass population of people to be recognized. The following recommendations are proposed for future research directions:

1. More accurate metric for computational complexity: The computational complexity is proposed to be measured using number of fitness evaluations, as optimization iterations contain different number of fitness evaluations depending on the number of non-dominated solutions stored in the external archive shown in algorithm 1. As shown in figure 10, the archive contents varies along iterations for the first image from 4 to 10 solutions. In the experimentation described in section 3, the impact of changing this metric for computational complexity would mainly affect the first face image which involves full optimization, and the rest of face images in the stack will involve only fitness evaluations for optimization population for detecting changes.
2. **Better change detection mechanism based on Pareto front metrics:** Most of literature in dynamic optimization for single objective is based on sentry particles/individuals as change detection mechanism where change is assumed when the fitness of these sentry particles/indivduals is varying. In multi-objective optimization in a dynamic environment, sentry particles becomes in-accurate in case of problems where the Pareto front in decision space is varying like problems of Type II and III, while this can be applied to dynamic multi-objective optimization of Type I and II as proposed by Zheng [18] and also Greeff and Engelbrecht [5]. For Dynamic Multi-Objective Optimization Problems (DMOOP) of Type II and III, some authors have considered other change detection with regards to changes in the Pareto set using some proposed metrics for the Pareto set like hypervolume and generational distance like the approaches proposed by Camara *et al* [2] and Li *et al* [9] respectively.

3. **Apply changes for PBIL to improve its efficiency in dynamic environments:** As proposed by Yang and Yao [17] different changes are applied to PBIL to improve its efficiency in dynamic environments like random immigrants, dual PBIL, and associative memory approaches. The most efficient approach for dynamic environments of cyclic changes is associative memory where the optimization environment landscape is recalled at later stage. Probability vectors can easily represent the optimization landscape, and thus can be easily stored in associative memory for later recall when a face image of similar content re-occur in the stack.

6 **Acknowledgment**

This work was supported by the Natural Sciences and Engineering Research Council of Canada and BancTec Inc.
References


