Impact of Watermarking on Offline Signature Verification in Intelligent Bio-Watermarking Systems

Bassem S. Rabil, Robert Sabourin, Eric Granger
Laboratoire d' Imagerie, de Vision, et d'Intelligence Artificielle
École de Technologie Superiéure (ÉTS), University of Quebec
1100, rue Notre-Dame Ouest, Montreal, Canada, H3C 1K3
bguendy@livia.etsmtl.ca, Robert.Sabourin@etsmtl.ca and Eric.Granger@etsmtl.ca

***Abstract*—Bio-watermarking systems were introduced as the synergistic integration of biometrics and digital watermarking to assure the integrity, authenticity and confidentiality of digitized image documents, and biometric templates. In this paper, the impact of watermarking attacks on the performance of offline signature verification is assessed in the context of intelligent bio-watermarking systems. The considered system is based on incremental learning computational intelligence, and multi-objective formulation that allows optimizing parameters according to watermark quality and robustness simultaneously. In this study, Extended Shadow Code features are extracted from digitized offline signatures, collected into feature vectors, and discretized into binary watermarks prior to being embedded into high resolution grayscale face image. The impact on biometric verification performance of quantization and different intensities of attacks are considered, and also observed the impact of using only certain areas of face images of higher texture Region Of Interest (ROI) for embedding the watermark. Experimental results conclude the optimal discretization, and better watermark fitness and verification performance when embedding in ROI. To improve the performance in future research, the authors propose to embed more reference signatures, use efficient ROI identification techniques, and finally novel formulation to add biometrics verification fitness to the watermark quality and robustness fitness during embedding optimization. The proposed system can be applied for verifying individuals crossing borders using offline signatures, or protecting biometric templates.**

***Index Terms*—biometrics, intelligent digital watermarking, incremental learning, offline signature verification, bio-watermarking**

I. Introduction

With rapid development of information technology, growing number of digital documents are transmitted and exchanged via the Internet. It has created an environment where digital information is easily distributed, duplicated and modified, leading to the need for effective copyright protection techniques. In addition the digitization of documents allows the rapid dissemination of data in distributed systems and post processing on computerized resources. Out of the main challenges consists in assuring the integrity, authenticity, and confidentiality of these digitized documents images. Various digital watermarking schemes have been developed to address these issues.

Digital watermarking is deployed in many domains to assure integrity and authenticity of the original signal via fragile and robust watermarking respectively. Digital watermarking is the process of embedding information into a digital signal. The signal may be audio, pictures or video. If the signal is copied, then the information is also carried in the copy. Biometrics and cryptography can be integrated with watermarking framework to assure confidentiality. A fragile watermark [20] is a type of watermark to ensure integrity, but it is broken if the watermarked image is manipulated or altered, while the robust watermark [20] ensures authenticity and can be extracted after manipulating the watermarked image. Semi-fragile watermark [8] is satisfying a trade-off between both quality and robustness and combines properties of fragile and robust watermark, semi-fragile watermarking systems are designed such that the protected image can undergo some image processing operations while it is possible to detect malevolent alterations and to locate and restore image regions that have been altered. Some authors have proposed using multiple watermarks [23] to handle integrity and authenticity separately.

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 against tampering, manipulation and attacks to ensure authenticity and integrity of the templates, also to hide biometric traits invisibly inside other biometric templates.

Offline signature based bio-watermarking systems have been studied by few authors in literature. Low *et al* [14] have used offline signature extracted features discretized as binary watermark to study the impact of watermarking attacks on watermark quality and robustness fitness only, while Bhattacharyya *et al* [4] have used offline signature images as watermarks to improve robustness against watermark removal attacks. The impact of watermarking attacks on the biometric verification system have been considered by Dong and Tan [7]

for iris template images, and Huang *et al* [9] for 3D face model authentication images. Also Dong and Tan [7] have considered the impact of watermarking attacks when embedding iris templates as watermarks. None of these bio-watermarking systems was based on computational intelligence techniques to optimize watermark embedding to maximize fitness of watermark quality and robustness.

The impact of watermarking attacks on biometric verification system is important specially if the watermark represents biometric trait where the performance of the overall system is affected when integrating biometric verification system with bio-watermarking framework. There is a trade-off between quality and robustness fitness, and the performance of the verification system because adding more bits improving the accuracy of discretization or increasing the size of feature vectors improves the performance of the biometric verification system, however this degrades the fitness for both quality and robustness due to increasing the embedding capacity.

In this paper, we present a study for the impact of watermarking attacks on biometric offline signature verification systems and its relation with the impact on the quality and robustness fitness of the watermark. Offline signature feature vectors are discretized into binary stream, and embedded as binary watermarks into grayscale face images of high resolution which have high embedding capacity and better face recognition verification rates. Watermark embedding is optimized using computational intelligence optimization method which is Population Based Incremental Learning (PBIL) for faster convergence as it employs previous optimization experience in subsequent generations. The impact of quantization and watermarking attack of different intensities is considered. Also the impact of using only region of interest (ROI) of higher texture for embedding watermarks rather than other smooth texture areas is studied for this class of face grayscale images. Also recommendations for proposed research directions to improve the overall intelligent bio-watermarking system for offline signature are described at the end of this paper.

The proposed intelligent bio-watermarking system for offline signature can be used to verify individuals crossing borders using their face images with their offline signatures features embedded as invisible watermarks, and verified from border filled forms. Also the proposed system can be used to protect biometric templates for both cover images representing face images, and the offline signature features which is embedded as invisible watermark where intruders are not aware of existing embedded features given good watermark embedding quality with minimal visual distortion.

The rest of the paper is organized as follows: Section II provides a background on intelligent watermarking, population based incremental learning and bio-watermarking, then Section III describes the experimental methodology used for computer simulations, and Section IV lists experimental results along with analysis, and finally Section V describes conclusion and recommendations for future research directions.

II. Intelligent Bio-Watermarking with Multi-Objective Population Based Incremental Learning Using Offline Signature Feature Vectors

Intelligent watermarking [20] was introduced to resolve the trade-off between watermark robustness and quality using non-conventional methods as computational intelligence methods like Genetic Algorithms and Particle Swarm Optimization which have proved efficiency with resolving such optimization problems. The optimization problem is formulated to maximize the fitness for both quality represented by Peak Signal to Noise Ratio (PSNR) and robustness represented by Normalized Correlation (NC) between the original watermark and the extracted watermark after manipulating the watermarked image. These metrics are calculated using equations 1, 2, and 3.

$$MSE_c = \frac{1}{M.N} \sum_{i=1}^{M} \sum_{j=1}^{N} \left(X\left(i,j\right) - X_c\left(i,j\right) \right)^2 \quad (1)$$

$$PSNR_c = 10log_{10}. \left(\frac{255^2}{MSE_c} \right) (dB) \quad (2)$$

$$NC = \frac{\sum_{i=1}^{M_W} \sum_{j=1}^{N_W} \left[W\left(i,j\right) W'\left(i,j\right) \right]}{\sum_{i=1}^{M_W} \sum_{j=1}^{N_W} \left[W\left(i,j\right) \right]^2} \quad (3)$$

where X is the original cover image of dimension MxN, X_c the watermarked cover image, the embedded watermark $W(i,j)$ of dimension M_WxN_W, and the extracted watermark from the attacked image $W(i,j)'$

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) [19] and Discrete Wavelet Transform (DWT) [12]. 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 [13] 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* [19] have used Genetic Algorithm for optimizing the aggregated fitness for both quality and robustness, while Wang *et al* [21] have used Particle Swarm Optimization for optimization. Other authors [12] 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 [15]. Multi-objective formulation [6], [17] 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 [8].

Population Based Incremental Learning method proposed by Baluja [2] 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. Initially, all the values of the probability vector are set to 0.5 and sampling from this vector produces a uniform distribution of the initial population on the feasible parameter space, as there is equal likelihood in the generation of 1 or 0 for each binary bit of the solution chromosome in this case. In every generation, this probability vector is used to generate a new population in such a way that the probability for the ith bit of a chromosome to become 1 is proportional to the value of the ith element of this probability vector. After evaluating the objective functions of the new population, this probability vector is updated by using only the best individual of the current population to help it shifting towards the chromosome of this new individual. As the search progresses, the probability vector is expected to shift gradually to correspond to solutions with the highest fitness values. Population Based Incremental Learning (PBIL) [15] has proved efficiency with intelligent watermarking problem where utilizing the previous experience in subsequent generations ensures better convergence properties.

Bureerat and Sriworamas [5] 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. The detailed algorithm is described in Algorithm 1.

The multi-objective PBIL component of the proposed bio-watermarking system for offline signature is shown in Figure 1, where quality objective and robustness against different attacks objectives are optimized simultaneously without favoring one objective over the other. This proposed mechanism provides multiple non-dominated solutions (Pareto front), which helps the operator to tune the watermarking system to be robust against certain attacks without computationally expensive re-optimization. This can be easily accomplished by choosing the best solution with regards to robustness against certain attack to be the optimal embedding to be used for the digitized document images.

Biometric watermarking was first proposed by Jain in 2002, where Jain and Uludag [10] suggested an amplitude modulation-based biometric watermarking. Bio-watermarking systems can be categorized into the following categories [14]:

1) *Watermarked biometrics:* For watermarked biometrics the host is a biometrics, whereas the watermark can either be a biometrics, or other proprietary notice. Intruders might not be aware of invisibly embedded traits.
2) *Biometric watermarking:* For biometric watermarking the biometrics are employed as the watermark, whereas the host can be any copyrighted documents.

In this paper, the proposed bio-watermarking is considered of the first category where the cover image is representing biometric face template, and the watermark is extracted features of another biometric trait which is offline signature.

The most significant advantage of handwritten offline signature over other biometric attributes is that it has traditionally

Algorithm 1 Multi-objective PBIL adapted from [5].

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.
6: 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.
7: 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
8: **end while**
9: The probability matrix and external Pareto set are improved iteratively until stopping criteria is reached.
10: **end while**

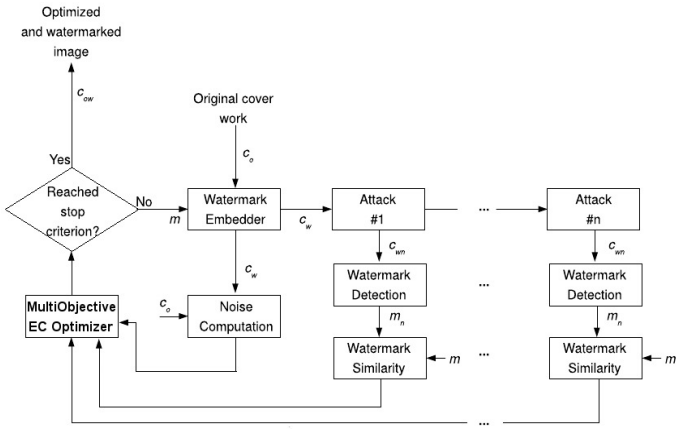

Fig. 1. Block diagram for multi-objective optimization component in the intelligent bio-watermarking system.

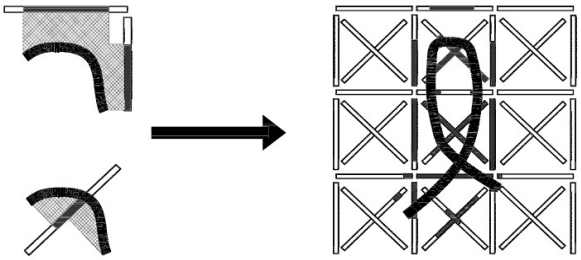

Fig. 2. Projection definition in Extended Shadow Code [16].

been used for authenticating official documents and thus it is socially accepted and widely used in many domains. Extended Shadow Code (ESC) [16] is a global shape factor for offline signature which is used in the signature verification problem because it permits the local projection of the handwriting without losing the knowledge of the location of measurements in the 2D space as shown in Figure 2. That is why ESC seems to be a good compromise between global features related to the general aspect of the signature, and local features related to measurements taken on specific parts of the signature without requiring the low-level segmentation of the handwriting into primitives. ESC resolution represents number of row cells and column cells respectively used for projection, for example in Figure 2 ESC resolution is 3x3.

Extended Shadow Codes (ESC) consists in the superposition of bar mask array over the binary image of a handwritten signature as depicted by Figure 3. Each bar is assumed to be a light detector related to a spatially constrained area of the 2D signal. A shadow projection is defined as the simultaneous projection of each black pixel into its closest horizontal, vertical and diagonal bars. A projected shadow turns on a set of bits distributed uniformly along the bars. After all the pixels of a signature are projected, the number of on bits in each bar is counted and normalized to the range of [0, 1] before features are extracted. Given a virtual grid composed of I rows by J columns, the cardinality of the ESC feature vector is calculated using equation 4. For example resolution 2x3 which is considered in this paper corresponds to cardinality equals to 29.

$$Cardinality = 4IJ + I + J \tag{4}$$

Extended Shadow Code (ESC) features are discretized to be converted to binary stream to be embedded as binary watermarks. The more bits used for discretization, the more accuracy is achieved for biometric verification, on the other hand this degrades the fitness for watermark quality and robustness by adding more bits to be embedded in the payload increasing the watermark capacity. Other authors [8] described using cryptographic digital signature as watermarks. Digital signatures aims to sign a document in its electronic form, such that the signature can be transmitted electronically with the signed documents. One of the methods to add the digital signature to the digitized document is discretizing the signature

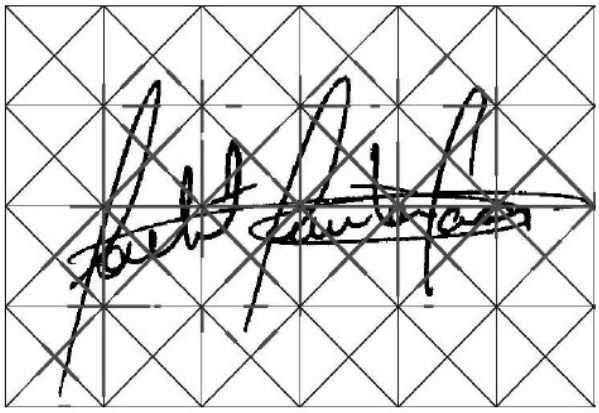

Fig. 3. Extended Shadow Code for Offline Signature Binary Image [3].

into binary watermarks to be embedded in original documents to be signed. However in this paper, the main focus will be on offline signature rather than digital signature and use extracted features as binary watermarks.

III. Experimental Methodology

The watermark embedding/extracting algorithm used in experiments is an algorithm proposed by Shieh *et al* [19]. In this algorithm 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 MxN 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 5

$$R\left(i\right) = \sum_{m=1}^{M/8} \sum_{n=1}^{N/8} \left(\frac{Y_{m,n}\left(0\right)}{Y_{m,n}\left(i\right)} \right), i \in [1, 63] \tag{5}$$

Then polarities P are calculated using the equation 6. Next, the watermarked DCT coefficient Y' is obtained using the equation 7 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'

$$P_{(m,n)}(i) = \begin{cases} 1 & if(Y_{(m,n)}(i).R(i)) \geq Y_{(m,n)}(0) \\ & i \in F \\ 0 & otherwise; \end{cases} \tag{6}$$

$$Y'_{(m,n)}(i) = \begin{cases} Y_{(m,n)}(i) & if P_{(m,n)}(i) = W_{(m,n)}(i) \\ & i \in F \\ (Y_{(m,n)}(0)/R(i)) + 1 & if P_{(m,n)}(i) = 0 \\ & W_{(m,n)}(i) = 1 \\ & i \in F \\ (Y_{(m,n)}(0)/R(i)) - 1 & otherwise \end{cases} \tag{7}$$

Fig. 4. Face images used in experiments as host grayscale images [11] of resolution 2048x1536.

Fig. 5. Signatures used in experiments whose feature vectors are embedded as watermarks [3].

The bio-watermarking system used in experiments is shown in Figure 6, where the embedding optimization module is using multi-objective PBIL algorithm proposed by Bureerat and Sriworamas [5] and the offline signature verification system proposed by Bertolini *et al* [3]. The databases used are PUT face database [11], and offline signature database proposed by Bertolini *et al* [3].

The offline signature verification system proposed by Bertolini *et al* [3] deploys multi-modal verification and decision fusion for the biometric trait achieving better performance than uni-modal verification systems. It also addresses the challenges of offline signature verification systems which are: the large number of users, the large number of features, the limited number of reference signatures for training, the high intrapersonal variability of the signatures and the unavailability of forgeries as counterexamples.

Binary representation is used to encode 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. The optimization problem to maximize quality and robustness fitness has high dimension as the metrics of both quality and robustness are calculated for the whole image while being dependent on the selection of embedding bands in each and every image block which have to be represented in each optimization individual. The best non-dominated solution from Pareto front with regards to robustness fitness is chosen as the optimal solution representing the optimal embedding bands for the host image.

was

In the experiments the face images used as host images are converted to grayscale, and then downsized 50% to resolution 1024x768. The offline signatures feature vectors used in experiments as watermarks are Extended Shadow Code (ESC) features extracted by the system proposed by Bertolini *et al* [3]. ESC feature vectors of resolution 2x3 producing feature vectors of size 29 features are discretized using different

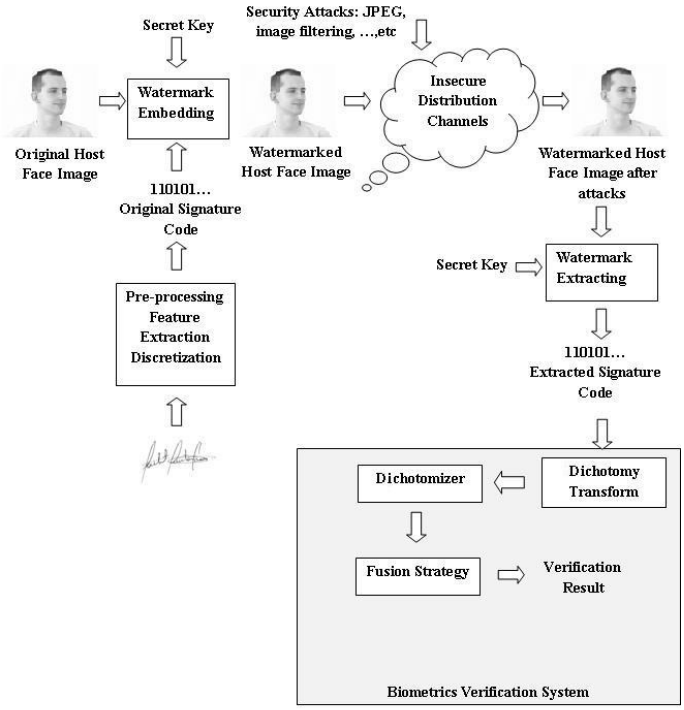

Fig. 6. Block diagram for bio-watermarking system with integrated verification system used in experiments [14], [11], [3].

number of bits to be used as binary watermarks with different accuracy levels.

The face images and signatures used in experiments are shown in Figures 4 and 5. The first 10 writers signatures feature vectors from the signatures database are embedded as watermarks in the first 10 persons face images from face images database respectively. The verification for the signature is performed against 39 signatures of the same writer as genuine samples and 39 signatures of random forgeries from other writers as negative samples for simplicity. Then the Genuine Accept Rate (GAR) and False Accept Rate (FAR) are calculated as metrics to measure the performance of the biometric verification system along with Equal Error Rate (EER), and Area Under Curve (AUC) at FAR equals to 0.05 to consider the system performance with maximum 5% falsely accepted samples. Receiver Operating Characteristics (ROC) curve is used to represent these metrics graphically.

First experiment shows the impact of discretization of ESC feature vectors on the biometric verification system, where different accuracy levels are experimented for discretizing feature vectors into binary string to be embedded as binary watermark into grayscale face images. In this experiment, the impact on the biometric verification system represented graphically using DET (Detection Error Trade-off) curve is studied for discretization using 6, 8, 10, and 12 bits. From this experiment, the best number of bits needed for discretization to be used in subsequent experiments is concluded. In this experiment, neither watermarking nor attacks is involved to isolate the impact of the quantization only.

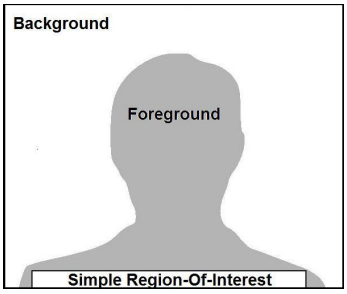

Fig. 7. Region Of Interest (ROI) used for experiments for face grayscale images.

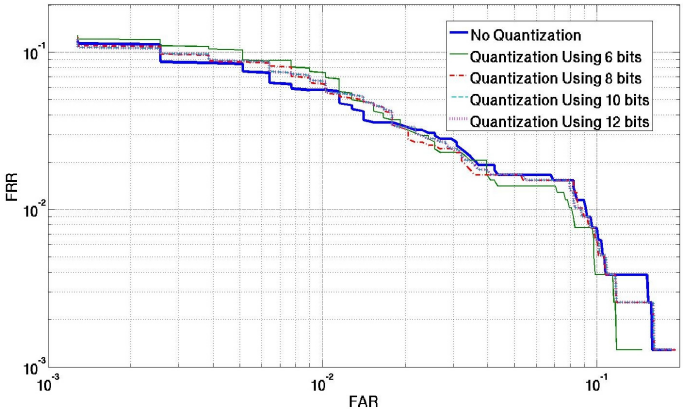

Fig. 8. DET curve for quantization of ESC 2x3 feature vectors using 6, 8, 10, and 12 bits representing the impact on the biometric verification system for different accuracy levels.

Second experiment shows the impact of JPEG compression attack with different quality factors 100%, 80% and 60% on the biometric verification system along with the impact on the watermark fitness for both quality and robustness.

In this application domain, the embedded features bits could be less than the number of image blocks, and consequently the embedding algorithm has to take into consideration the choice of suitable image blocks for embedding. And thus, the third experiment shows the impact of JPEG compression attack of quality factor 80% on the verification system when embedding the watermark in the foreground which is the profile of the face image rather than the smooth background to maximize the watermark fitness. A simple region of interest used for embedding the watermark at the bottom of the foreground as shown in Figure 7.

IV. Results and Analysis

Figures 8 shows graphically the impact of quantization on the biometric verification system performance for ESC of resolution 2x3 feature vectors using 6, 8, 10, and 12 bits. The results show minimal impact for quantization on the biometric verification system performance, also the results show that using 10 bits have the most similar DET curve to that of using no quantization. Using more than 10 bits have nearly identical DET curve of using 10 bits. The area under the curve for ROC curves when FAR=0.05 equals to 0.0481, 0.0479, 0.0480, 0.0480, and 0.0480 for no quantization, 6, 8, 10, and 12-bits quantization respectively.

Table I shows the impact of watermark attack of different intensities on the quality and robustness fitness and verification system performance, when embedding ESC feature vectors of resolution 2x3 using 10 bits for discretization. The impact on the biometric verification system efficiency is graphically represented using ROC curve in Figure 9, where the area under the curve for ROC curves when FAR=0.05 equals to 0.0451, 0.0433, and 0.0424 for quality factors 100%, 80%, and 60% respectively. The results show that the fitness changes for quality and robustness are minimal, while the impact on the verification system performance represented by AUC and EER is more significant. This proves the importance of this study.

Table II shows the impact of using region of interest to embed the watermark on the quality and robustness fitness and verification system performance, when embedding ESC feature vectors of resolution 2x3 using 10 bits for discretization. The impact on the biometric verification system efficiency is graphically represented using ROC curve in Figure 10, where the area under the curve for ROC curves when FAR=0.05 equals to 0.0433, and 0.0450 for embedding the watermark in random region, and embedding in ROI respectively. The results show slight improvement in the fitness for both quality and robustness and significant improvement for verification system performance represented by AUC and EER. Also the results show that the extracted watermark is affected by the watermarking attack for few users, meanwhile the impact of the attack is significant on the verification system performance compared to the effect of the discretization process, this means that the affected bits of the watermark were towards the Most Significant Bits (MSB), and thus the impact was severe on the values of feature vectors which degrades the verification system performance as Normalized Correlation (NC) representing the robustness is concerned with only the

TABLE I
JPEG COMPRESSION ATTACK IMPACT WITH DIFFERENT QUALITY FACTORS WHEN EMBEDDING ESC 2X3 FEATURE VECTORS USING 10 BITS FOR DISCRETIZATION.

Q.F.	**100%**		**80%**		**60%**	
Fitness /User	**PSNR**	**NC**	**PSNR**	**NC**	**PSNR**	**NC**
1	86.1	0.99	84.1	1.0	82.8	0.99
2	84.5	1.0	84.3	1.0	84.7	1.0
3	83.9	1.0	82.3	1.0	80.8	1.0
4	83.5	1.0	83.4	1.0	83.8	1.0
5	85.1	0.96	86.9	0.96	85.9	0.95
6	82.8	1.0	85.5	1.0	81.8	1.0
7	82.6	1.0	82.0	1.0	82.3	1.0
8	84.9	1.0	87.4	0.99	85.6	1.0
9	83.9	1.0	84.0	1.0	86.3	0.98
10	83.2	1.0	83.7	1.0	82.6	1.0
Mean	**84.1**	**1.0**	**84.3**	**1.0**	**83.7**	**0.99**
EER	**0.0436**		**0.0577**		**0.0526**	
AUC_0.05	**0.0451**		**0.0433**		**0.0424**	
No Quantization + No Attack EER=0.0282 and AUC_0.05=0.0481						

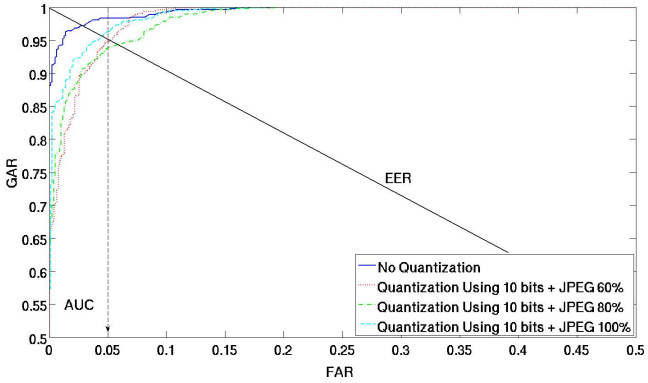

Fig. 9. ROC curve for JPEG compression attack impact with different quality factors when embedding 2x3 feature vectors using 10 bits for discretization.

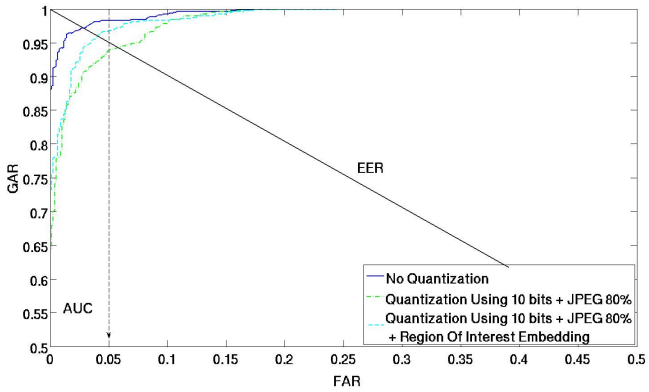

Fig. 10. ROC curve for the impact of JPEG compression attack with quality factor 80 while embedding the watermark in region of interest of higher texture when embedding ESC 2x3 feature vectors using 10 bits for discretization.

TABLE II
IMPACT OF JPEG COMPRESSION ATTACK WITH QUALITY FACTOR 80% WHILE EMBEDDING THE WATERMARK IN REGION OF INTEREST WHEN EMBEDDING ESC 2X3 FEATURE VECTORS USING 10 BITS FOR DISCRETIZATION.

ROI	**No**		**Yes**	
Fitness /User	**PSNR**	**NC**	**PSNR**	**NC**
1	84.1	1.0	82.0	1.0
2	84.3	1.0	85.2	1.0
3	82.3	1.0	85.3	1.0
4	83.4	1.0	84.7	1.0
5	86.9	0.96	86.6	0.96
6	85.5	1.0	83.5	1.0
7	82.0	1.0	82.6	1.0
8	87.4	0.99	85.3	1.0
9	84.0	1.0	84.4	1.0
10	83.7	1.0	85.4	1.0
Mean	**84.3**	**1.0**	**84.5**	**1.0**
EER	**0.0577**		**0.0397**	
AUC_0.05	**0.0433**		**0.0450**	
No Quantization + No Attack EER=0.0282 and AUC_0.05=0.0481				

percentage of correct bits.

V. CONCLUSIONS AND RECOMMENDATIONS

This paper presented a study for watermarking attacks on biometric offline signatures verification in intelligent bio-watermarking systems. Experiments clarified that using watermark fitness metrics is not sufficient to measure the overall performance of the bio-watermarking system. Also experiments showed minimal impact of quantization process on the biometric offline signature verification system, and the optimal quantization is achieved using 10 bits. The impact of watermark attack JPEG compression of different quality factors on the watermark fitness and the biometric verification system has been studied and the least impact on offline signature verification system is noticed for quality factor 100% and the most for 60%. Using region of interest of face images for embedding the watermark has proved better performance for the biometric offline signature verification system.

To improve the efficiency of the proposed intelligent bio-watermarking system using offline signature as embedded biometric trait, the following directions are proposed:

1) *More robust signature verification :* In the experiments, simplified experimental protocol for signature verification is used as a proof of concept. More robust results can be achieved when considering other types of forgeries like simple and skilled forgeries, use selected features from multiple ESC resolutions for more discriminant extracted features, consider the impact of the watermarking on all genuine signatures for writer instead of only one genuine reference signature, and finally increasing the number of writers for better generalization.
2) *Embed more than one reference signature into face images:* In the experiments only one reference feature vectors per writer has been embedded in grayscale high resolution face images. The performance of the verification system could be dramatically improved if more than reference signature for the same writer are embedded in the same face image. For better verification results with more discriminant features accomplished by several hundreds of features [3], high resolution grayscale face images would be sufficient for around 4 reference signatures. Confidence level fusion can be used with these multiple reference signatures.
3) *Use efficient Region-Of-Interest identification technique:* In the experiments a simple region of interest is chosen to ensure belonging to the foreground of the face grayscale image. More efficient region of interest mechanisms could be used to identify the suitable image blocks to embed the watermark, and also identify the suitable image blocks for increasing watermark embedding capacity. Local Binary Patterns have been proposed for face detection [1], it would improve the performance of the proposed system to use such efficient technique for detecting region of interest of face grayscale images. Another simple thersholding [18] mechanisms can be used in the case of grayscale images like Otsu method

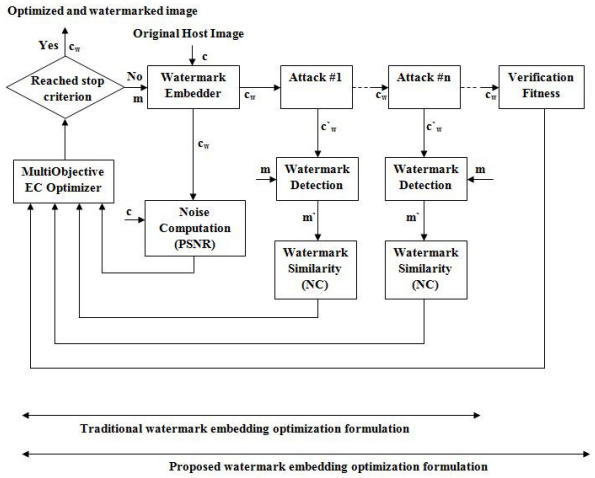

Fig. 11. Proposed optimization formulation compared to traditional formulation [19].

which can be used to identify the silhouette of face images, this method assumes that the image contains two classes of pixels foreground and background, then it calculates the optimum threshold separating those two classes so that their combined spread representing intra-class variance is minimal.

4) *Better formulation for watermark embedding optimization problem:* In the experiments it was clearly demonstrated that in most of the cases the watermark fitness including PSNR and NC, and biometric verification system performance are conflicting objectives which makes it hard to find a compromise between them.
The traditional formulation is not considering the impact on the biometric verification system during the embedding optimization phase, and this degrades the verification rate because NC is representing only the percentage of correct bits in the extracted watermark representing feature vectors of the biometric trait. The verification system is more sensitive to the position of the correct bits in the extracted watermark rather than the percentage. For example, the affected LSB will have minimal impact on the verification system, and vice versa with MSB. In the case of other encoding scheme like Gray code encoding, the sensitivity of the verification system is towards discriminant features bits. To resolve this issue, it is proposed to add verification system fitness to the optimization process beside quality and robustness objectives as shown in Figure 11. The fitness could be represented by the confidence value/score of the verification system. In this proposed formulation robustness fitness and verification fitness will complement each other as the robustness fitness minimizes the number of affected bits and meanwhile the verification fitness optimizes the position of affected bits (if any).

ACKNOWLEDGMENT

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

REFERENCES

[1] Ahonen T., Hadid A., and Pietikinen M., "Face description with local binary patterns: Application to face recognition.", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 28(12):2037–2041, 2006
[2] Baluja S., "Population-Based Incremental Learning: A method for integrating genetic search based function optimization and competitive learning.", Technical report, CMU, 1994.
[3] Bertolini D., Oliveira L.S., Justino E., and Sabourin R., "Reducing Forgeries in Writer-independent Off-line Signature verification through ensemble of classifiers.", *Pattern Recognition*, 43(1):387–396, January 2010.
[4] Bhattacharyya D., Bandyopadhyay S. K., and Das P., "Handwritten Signature Watermarking and Extraction Technique Inspired by Principle of Segregation.", *International Journal of Security and Its Application*, 1(1):35-44, July 2007
[5] Bureerat S., and Sriworamas K., "Population-Based Incremental Learning for Multiobjective Optimization.", *Soft Computing in Industrial Applications*, 39:223-232, 2007.
[6] Diaz D.S., and Romay M.G., "Introducing a Watermarking with a Multi-objective Genetic Algorithm.", In *GECCO*, 2005.
[7] Dong J., and Tan T., "Effects of Watermarking on Iris Recognition Performance.", *International Conference on Control, Automation, Robotics and Vision*, pages 1156-1161, Vietnam, December 2008
[8] Haouzia A., and Noumeir R., "Methods for Image Authentication: A survey.", *MultiMed Tools Appl*, 39:1-46, 2008.
[9] Huang W., Niu X., Song W., and Lu M., "Digital Watermark for 3D Face Model Authentication and EER Performance Analysis.", *Eighth International Conference on Intelligent Systems Design and Applications*, pages 550-554, 2008
[10] Jain A.K., and Uludag U., "Hiding Biometric Data.", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 25(11):1494-1498, 2003.
[11] Kasinski A., Florek A., and Schmidt A., "The PUT Face Database.", *Image Processing & Communications*, 13(3-4):59-64, 2008.
[12] Lee Z.J., Lin S.W., Su S.F., and Lin C.Y., "A hybrid watermarking technique applied to digital images.", In *Applied Soft Computing*, 8:798-808, 2008.
[13] Licks V., and Jordan R., "Geometric Attacks on Image Watermarking Systems.", In *IEEE Multimedia, IEEE Computer Society*, July-September 2005.
[14] Low C-Y., Teoh A., and Tee C., "Fusion of LSB and DWT Biometric Watermarking using Offline Handwritten Signature for Copyright Protection.", In *ICB2009*, pages 786-795, 2009.
[15] Rabil B.S., Sabourin R., and Granger E., "Multi-Objective Intelligent Watermarking with Population Based Incremental Learning.", *IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, October 2010.
[16] Sabourin R., "Off-Line Signature Verification: Recent Advances and Perspectives.", *Brazilian Symposium on Document Image Analysis-BSDIA*,1997.
[17] Sal D., Grana M., and Anjou A.D., "A moga to place the watermark in an hyperspectral image.", In *International Geoscience and Remote Sensing Symposium*, pages 774-777, Denver, USA, August 2006.
[18] Sezgin M., and Sankur B., "Survey over image thresholding techniques and quantitative performance evaluation.", In *Journal of Electronic Imaging*, 13(1):146-165, 2003.
[19] Shieh C-S., Huang H-C., Wang F-H., and Pan J-S., "Genetic Watermarking Based on Transform-domain Techniques.", *Pattern Recognition*, 37:555-565, 2004.
[20] Vellasques E., Granger E., and Sabourin R., "Intelligent Digital Watermarking of Document Images.", *in Handbook of Pattern Recognition and Computer Vision*, ed., C.H. Chen, 4th edition, 2010, pages 687-724.
[21] Wang Z., Sun X., and Zhang D., "A novel watermarking scheme based on PSO algorithm.", *in LSMS*,4688:3017-314, 2007.
[22] Wu M., *"Multimedia Data Hiding."*, PhD thesis, Princeton University, 2001.
[23] Wu M., Yu H., and Liu B., "Data hiding in image and video: Part II - Designs and Applications.", *IEEE Transactions on Image Processing.*, 12(6):696-705, June 2003.