CANCELABLE BIOMETRIC FILTERS FOR FACE RECOGNITION

Marios Savvides, B.V.K. Vijaya Kumar and P.K. Khosla
Electrical & Computer Engineering, Carnegie Mellon University, Pittsburgh PA 15213
msavvid@ri.cmu.edu, kumar@ece.cmu.edu, pkk@ece.cmu.edu

ABSTRACT

In this paper we address the issue of producing cancelable biometric templates; a necessary feature in the deployment of any biometric authentication system. We propose a novel scheme that encrypts the training images used to synthesize the single minimum average correlation energy) filter for biometric authentication. We show theoretically that convolving the training images with any random convolution kernel prior to building the biometric filter does not change the resulting correlation output peak-to-sidelobe ratios, thus preserving the authentication performance. However, different templates can be obtained from the same biometric by varying the convolution kernels thus enabling the cancelability of the templates. We evaluate the proposed method using the illumination subset of the CMU pose, illumination, expressions (PIE) face dataset. Our proposed method is very interesting from a pattern recognition theory point of view, as we are able to ‘encrypt’ the data and perform recognition in the encrypted domain that performs as well as the unencrypted case, regardless of the encryption kernel used; we show analytically that the recognition performance remains invariant to the proposed encryption scheme, while retaining the desired shift-invariance property of correlation filters.

1. INTRODUCTION

Biometric authentication systems such as face recognition systems [1] are being actively investigated for access control and security applications. However, there are many issues that need to be addressed to ensure the security of biometric templates. One such aspect is the cancelability of a biometric. For example, consider a scenario where a biometric template is stored on a card for authenticating a user. What happens when that card with the user’s biometric template is lost or stolen? How does one cancel the lost or stolen card and re-issue a new biometric card for that person? In order to protect the user’s biometric templates from possible hacking and to ensure cancelability, the templates must be encrypted. Then in case of theft or loss, a different encrypted biometric template can be issued from the same original biometric pattern. Recent work in using advanced correlation filters has shown promise for biometric verification Error! Reference source not found.Error! Reference source not found.Error! Reference source not found. Correlation filter methods offer advantages such as shift-invariance and graceful degradation. Employing standard encryption techniques can affect the correlation filters adversely degrading their some of the advantages. Soutar et al Error! Reference source not found. have shown how to use biometrics for encryption. In this paper, we propose a novel method to encrypt these biometric templates using random convolution kernels. We show theoretically that the minimum average correlation energy (MACE) filters Error! Reference source not found. used for biometric authentication produce identical performance even when the training images are convolved with a random kernel. This is the key to making cancelable biometric filters since it allows us to choose a different random convolution kernel when re-issuing biometric templates.

2. EXAMPLE SYSTEM ARCHITECTURE

We show in Fig.1 one such possible system architecture. During the enrollment, a few face images of the user are collected. These training images are then convolved with a random convolution kernel. How this kernel is generated can vary depending on the desired operation of the system. Here we assume a very simple scheme; the user is asked to provide a PIN number, and this PIN number is used as the ‘seed’ in a random number generator which is used to generate the random convolution kernel. The convolved training images are then used to generate a single biometric filter. We use the minimum average correlation energy (MACE) type correlation filters Error! Reference source not found. The inverse Fourier transform of this encrypted MACE filter will not be useful in extracting the original face images because of the convolution with random kernels.

Fig 1. Enrollment stage for encrypted filters
This resulting encrypted filter can be stored on a card and then used to authenticate the user’s identity. If the card is lost or stolen, the enrollment system simply generates a different convolution kernel to synthesize a different encrypted biometric filter. A perpetrator trying to reconstruct a person’s biometric from the stolen card needs to know the convolution kernel used in the enrollment stage. The attacker essentially has to perform image de-convolution to retrieve the original filter; which is extremely difficult without knowing the user’s PIN or the convolution kernel used.

In this scenario, during the authentication stage (shown in Fig. 2) the user will present his/her card and provide the PIN. That will generate the convolution kernel which will now be used to convolve with the test face images presented by the authentic user. The resulting convolved test images are then cross-correlated with the encrypted biometric filters, and the resulting correlation outputs are examined to perform authentication. The key point to note is that the authentication process is performed entirely in the encrypted domain. The metric we use when examining the output correlation output is the peak-to-sidelobe ratio (PSR) defined as (peak-mean)/std where the mean and the standard deviation are computed in an annular region centered at the peak Error! Reference source not found..

Fig 2. Authentication stage for Encrypted Filters ( denotes convolution and * correlation)

3. MACE FILTERS

Minimum Average Correlation Energy filters Error! Reference source not found. are among the most popular advanced correlation filters. There are many important differences between these advanced filters and the standard matched filter [6] (which is what many people think of when they hear the term “correlation filter”). A matched filter is made from a single training image. In contrast, a MACE filter is synthesized from many training images. Also MACE filters minimize the average correlation energy (ACE) effectively resulting in correlation outputs (for the true class) with sharp discernible peaks and values near zero elsewhere in the output correlation plane. This is very different from the matched filters that produce broad correlation output peaks, which do not exhibit good discrimination power. MACE filters in their efforts to produce sharp correlation peaks emphasize the higher spatial frequencies of the images, and thus are highly discriminative i.e., they do not produce any discernible peaks for images not belonging to the true class resulting in very low PSRs for the impostor classes.

The MACE filter formulation is given directly in the frequency domain as follows:

\[ h = D^{-1}X(X^*D^{-1}X)^{-1}c \]  

where \( X \) is an MxN matrix for N training images each with M=d1xd2 pixels where the image size is d1xd2. The 2-D Fourier transforms of training images are lexicographically re-ordered and placed as columns of \( X \). \( D \) is a MxM diagonal matrix containing the average power spectrum of all the training images along its diagonal. \( c \) is an Nx1 column vector containing the desired correlation values at the origin for each of the N training images. The resulting \( h \) is a column vector with M entries that needs to be re-ordered into a 2-D array to form the 2-D MACE filter.

3.1 PSR invariance to arbitrary convolution kernels

In this section, we prove that convolving the training images with any arbitrary convolution kernel to synthesize encrypted mace filters leads to identical output correlation plane energies as the un-encrypted mace filters. Thus the measured PSRs used for verification should be identical for both cases. The average correlation output energy \( E \) using Parseval’s theorem is given in the frequency domain as follows:

\[ E = h^*Dh \]  

where \( * \) denotes complex conjugate transpose. Convolving the training images in the spatial domain with a convolution kernel \( L \) is equivalent to multiplying the Fourier transform of the training images with the Fourier transform of the convolution kernel, i.e.,

\[ \hat{X}' = LX \]  

where \( \hat{X}' \) is a matrix of the same structure as \( X \) except that it contains the Fourier transforms of the encrypted training images, and \( L \) is a diagonal matrix of size MxM containing the Fourier transform of the convolution kernel \( L \) along its diagonal. Similarly we formulate the resulting pre-filtered MACE filter, noting however that the new average power spectrum is now of the following form:

\[ D' = (L^*DL) = (LDL^* \)  

yielding the pre-filtered MACE filter \( h' \) as

\[ h' = D'^{-1}X'(X'^*D'^{-1}X')^{-1}c \]
The energy resulting from the synthesized pre-filtered MACE filter is represented by $E'$ shown below.

$$E' = h^+D'h$$

(6)

Eq. (6) proves that convolving the training images with any arbitrary kernel does not affect the resulting energy minimization. Therefore the average correlation energy (ACE) $E'$ obtained with encrypted training images is the same as the $E$ average correlation energy of the original MACE filter. Thus any random convolution kernel can be used without affecting the resulting peak-to-sidelobe ratios. This is the key property that enables us to produce cancelable filters that provide identical verification performance, independent of what convolution kernel is used to encrypt the images.

4. EXPERIMENTS

In our experiments we used the illumination subset of the CMU PIE face dataset [7] for testing. We used the subset captured with no ambient background lighting, which contains the more challenging illumination variations. The dataset used consisted of 65 subjects with 21 illumination variations per person (100x100 pixels). We selected three training images per person, namely the extreme lighting variations (left shadow, frontal lighting and right shadow, example shown in Fig. 3) to synthesize a single MACE filter template for each person. Then we cross-correlated each of these filters with the whole dataset and measured peak-to-sidelobe ratios (PSR) for assessing the verification performance. Our results indicate 100% verification across all 65 people, i.e., there is a clear margin of separation between the PSRs of the authentic class and the 64 other impostors resulting from each filter for each of the 65 people. We show in Fig. 4 two different random convolution kernels. We can see in Fig. 5 the convolved training images from Fig. 3 with the random convolution kernel 1 from Fig 4. The encrypted training images in Fig.5 look nothing like the original images. Fig.6 shows the same training images convolved with random convolution kernel 2.

In Fig. 7 (left), we show the point spread function of the original MACE filter synthesized from 3 images of Person 2. Notice that we can see some facial features such as eyes, nose and mouth that are captured by the MACE filter. However in the point spread functions (Fig. 7 middle and right) of the MACE filter resulting from encrypted training images, we cannot make out any facial features. We also observe that MACE PSF 1 is different from PSF 2 as expected. However, both encrypted MACE filters, when cross-correlated with the training image 1, produce identical correlation outputs (See Fig. 8) with the same PSR, even though the training images used to design the two filters are completely different as they have been convolved with different kernels.

Fig. 3 (left) Image 3 (middle) Image 7 (right) Image 16 of Person 6 from the CMU PIE database.

Fig. 4. (left) Random convolution kernel 1 (right) Random convolution kernel 2

Fig. 5 Result of convolving with Kernel 1 (left) Image 3 (middle) Image 7 (right) and Image 16 of Person 6

Fig. 6 Result of convolving with Kernel 2 (left) Image 3 (middle) Image 7 (right) and Image 16 of Person 6

Fig. 7. (left) Point Spread Function of the MACE Filter 1. (middle) MACE PSF using convolution kernel 1. (right) MACE PSF using convolution kernel 2.
In this experiment we also cross-correlated all the original training images with the corresponding filters made from encrypted images and vice-versa, and observed that the correlation outputs do not produce any discernible peaks, but due to space limitations we have not shown those outputs here.

Fig. 9 shows a comparison of the PSRs from an encrypted (pre-filtered) MACE filter and original un-encrypted MACE filter for Person 2. We observe that the resulting PSRs are nearly identical. There is a small deviation from the original PSRs but we believe that is due to numerical quantization error involved with performing convolution of training images, as the same plot is obtained independent of the convolution kernel used.

Using this scheme, we are still able to achieve 100 % correct verification rates on all 65 people (we computed 65x65x21=88,725 correlations) using one filter per person designed from just 3 training images of that person achieving identical recognition performance to that of the experiment where we used the original raw images (with no encryption).

5. CONCLUSIONS

We have presented a novel approach to encrypting MACE correlation filters by using their invariance to linear pre-filtering. This property enables us to produce encrypted biometric filters that can be re-issued using a different convolution kernel. We have shown mathematically and through numerical experiments that an arbitrary random convolution kernel can be used, and that the resulting PSRs are the same. Thus verification performance is not affected by this pre-processing step. More importantly this method retains all the attractive properties of using correlation filters such as shift invariance and graceful degradation while allowing us to perform the resulting authentication directly in the encrypted domain (i.e., we do not at any point decrypt the images or filters during authentication). This helps to guard against the types of attacks where the attacker might try to intercept the decrypted filter during the verification stage as would be the case in standard encryption methods.

Finally, this paper has demonstrated cancelable MACE filters for face authentication, however this method can be applied to other biometrics such as fingerprints, iris image, etc. for the same purpose.

REFERENCES