Picture ID Authentication Using Invisible Watermark and Facial Recognition Features

Wensheng Zhou[1] and Hua Xie[2]

[1] Information Systems Sciences Lab, HRL Laboratories, LLC, 3011 Malibu Canyon Road, Malibu, CA 90265, USA

[2] Signal and Imaging Processing Institute, Department of Electrical Engineering, University of Southern California, Los Angeles, CA 90089, USA

Abstract. Picture ID authentication is very important for any identification verifications and extremely critical for homeland security. Here we propose a unique picture ID authentication apparatus which combines invisible watermark embedding and detection technology with facial recognition techniques. To demonstrate this apparatus, we implemented a system that is capable of fast and secure verification on the integrity and authenticity of ID documents with face images for Boeing. The proposed invisible watermarks tolerate most-common attacks such as recompression. We believe with only minor improvement this picture ID authentication system can be deployed in real environment at airports and country borders.

1 Introduction and Motivation

As technology advances, more and more digital equipments are readily available to provide easy and convenient ways to generate, manage and distribute digital contents and information. However, digital-format contents are easily modified without notice. As a result, seeing is no longer absolutely a believing [1]. How to protect the copyright and integrity of the digital content is becoming increasingly important and challenging, not only for digital content providers, but also for digital content consumers.

Besides, broadband networks, such as next-generation satellite system, also provide an ideal platform to achieve the cost effective delivery of large volume of digital data. The Digital Cinema (DC) project [2,3] that targets to deliver high-resolution movies to theaters is a prime example of such endeavor. However, it lacks the key security component to protect the authenticity of the distributed data from video frame swapping and image editing and to deter and track illegal pirating.

This lack of security not only causes huge financial loss in commercial world, but also becomes serious security issue in identification documents. In fact, identity theft and fraud have been growing rapidly worldwide. There were over 700,000 cases of identify theft in 2002. After 9.11, from homeland security point of view, identification verification becomes even more urgent. Each identity contains personal informa-

Zhou W. and Xie H. (2005).
Picture ID Authentication Using Invisible Watermark and Facial Recognition Features.
In *Proceedings of the 5th International Workshop on Pattern Recognition in Information Systems*, pages 12-21
DOI: 10.5220/0002579100120021

tion, identity photo, and so on. The original identity needs to be protected from alterations, and at the same time, the identity needs to be authenticated. It is a challenge to come up with smart and secure ID cards and passports to make sure that terrorists can't fool security staffs at the borders, airports and any entry to the country that requires identity checkups.

So in this paper, we designed and implemented a face image content authentication protection apparatus and an automatic face verification and restoration system. It provides content integrity preservation, verification, and protection, especially for video and image contents. The technology is also applicable to intrusion detection system to detect any content modification, identification authentication, copy tracking and unauthorized usages. This work applies security and digital copy management with state of the art watermark technologies to correct these problems. The homeland security will see this work very useful because it is created to protect the true content of the identity photos. Under any case, for any the fraudulent IDs, there is a watermark which is corresponding to the true identity and it helps to detect out the fraudulent ID.

The paper is organized as follows. Section 2 presents the related work on the subject and gives a brief introduction of the contribution of this work. Section 3 characterizes the proposed authentication service and authentication algorithm. In particular, facial recognition features using Eigenface as an invariant property of authentication, and an indication of how authentication algorithm embedding are presented. The design of the authentication detection system is given in Section 4. Experiment results and discussion are given in Section 5. Section 6 concludes the paper.

2 Related Work and Contribution

2.1 Related work

Traditional digital signatures, which utilize cryptographic hashing and public key techniques, have been used to protect the authenticity of traditional data and documents [4]. However, such schemes protect every bit of the data and do not allow any data manipulation or processing, and it is also hard to tolerate printing and scanning, which are critical procedures for ID creations.

Paper [1] surveyed the most current multimedia authentication technologies and their applications. Hard authentication rejects any modification to a multimedia signal, which is apparently suitable for applications in ID documents that involve A/D signal conversions. However, multimedia signals that are modified yet retain their original perceptual quality and/or semantic content are desired in such applications. Zhu et. al. [5] describes algorithms that accept only manipulations that preserve the perceptual quality. Papers [6-10] address the content-based authentication by using computable feature vector that can capture the major content characteristics from a human perspective. However, all these papers use very heuristic features to represent the semantic content of the original multimedia content, such as block histograms [6], averages [7], lower-order moments [8] or image edges [8,9] and zero-crossings [10]. None of their methods addresses the content-based authentication by preserving both perceptual and semantic contents yet, especially for ID documents. Wu [11] presented a content-based multimedia authentication system by combining some of the best features of the feature-based and hash-based authentication algorithms. Bartolini et. al. [12] studied the image authentication techniques for surveillance applications.

2.2 Contribution of this work

Our proposed work develops an authentication watermark algorithm that is designed to verify the integrity of the cover digital content in which it is embedded. Here we especially try to embed authentication watermark to protect the ID documents, such as passport and other personal ID for enhancing homeland security, and student ID and drivers' licenses for verification applications. We are the first to take the novel approach to combine the facial recognition technique with identification document content protection mechanism. The uniqueness and invariant property of Eigenvectors of the Eigenfaces make them perfect to serve as authentication watermark key. The invisible watermark embedding/detection using this novel technique tolerates most-common attacks.

This technique differs from traditional digital signatures and some of the pervious image authentication algorithms in that (1) It uses invisible watermarking, which is imperceptible to human eyes and becomes an integral part of the image, rather than an external signature. (2) It incorporates facial features for unique watermark embedding for each specific face in ID documents. It can also combine other biometric information (i.e., handwriting and finger-printings) with watermarking for additional security. (3) It provides robustness. It allows some predefined acceptable manipulations which don't hurt any facial recognition. Also the watermark is robust in printing and scanning processes. (4) It is a secure authentication. Each authentication watermark is identified with a unique secret key. (5) It provides flexible verification method and can automatically recover the corrupted face image for ID documents. This developed system has flexible and self- verification capabilities, and could conduct both machine readable verification using advanced digital camera and scanners, and Network-based verification via databases and servers.

3 Digital ID Document Authentication System

ID Documents are a hybrid of text, pictures, images and graphics. Fig. 1 depicts a digital document authentication system that protects digital contents in either standalone or distributed environment. This authentication method for ID images mainly has two distinguished features: (1) it protects the content of the standard face images for ID documents; and (2) it supports the robust and accurate authentication verification of the protected content even after IDs are scanned or reprinted. The first character requires effective face recognition feature vector extraction method for image content protection. The second character requires robust and effective watermark embedding and detection methods.

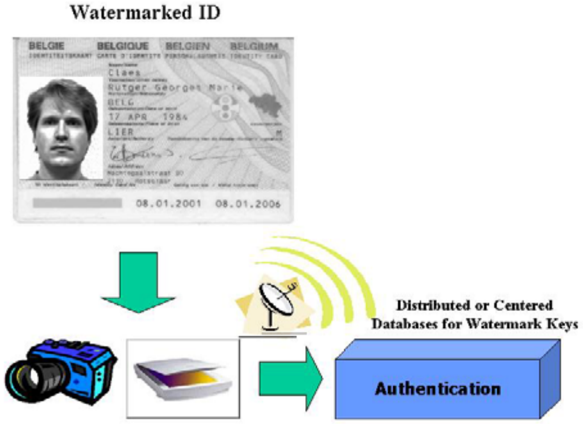


Fig. 1. Digital Document Authentication System which protects generated and distributed digital contents

3.1 Eigenface vector extraction

Eigenface is a well-known Principle Component Analysis (PCA) based face recognition algorithm developed by researchers at MIT [13]. The calculus of the Eigenface is supported on the statistical method of **principal components**. The analysis tries to generate new variables, using an initial data matrix as a point of departure in such a way that these variables can express more structural variability of the first matrix. Specifically, the matrix of the resultant variables is now orderly, so that all the variables are not correlated. The first variable contains the most variability of the initial group, and the second variable has the second most variability and so on. It can be proved that the transformation of the initial matrix that is required for the fulfillment of these conditions depends on the matrix of Eigenvectors that are associated with the Eigenvalues of the original data matrix. It means that the matrix of Eigenvectors determines the rotation to which the initial variables have to conform in order to perform the previous conditions.

Though the mathematical underpinnings of Eigenfaces are complex, the entire algorithm is simple and has a structure quite amenable to streaming. Training images are represented as a set of flattened vectors and assembled together into a single matrix. The Eigenvectors of the matrix are then extracted and stored in a database. The training face images are projected onto a feature space, called *face space*, defined by the Eigenvectors. This captures the variation between the set of faces without emphasis on any single facial region such as eyes or nose. The projected face space representation of each training image is also saved to a database. To identify a face, the test image is projected to face space using the saved Eigenvectors. The projected test image is then compared against each saved projected training image for similarity. The identity of the person in the test image is assumed to be the same as the person depicted in the most similar training image. An example of face Eigenfeature extraction is shown in Fig. 2. A re-implementation of the Eigenfaces algorithm from researchers at Colorado State University [14] was used in this research.

Once eignefaces *E[e$_1$, e$_2$, …e$_n$]* are established, we can always decompose a face into a projection vector over the Eigenspace, v_i=<*I*, e_i>, and *V=[v$_1$, v$_2$, …, v$_n$]* is the Eigenvector of the face image over the Eigenfaces.

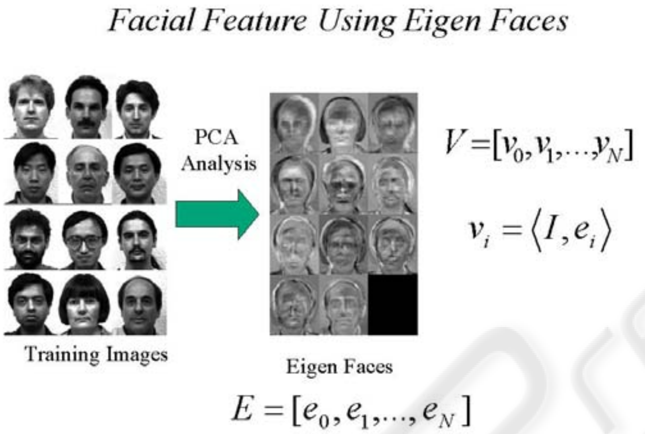

Facial Feature Using Eigen Faces
PCA Analysis
Training Images
Eigen Faces
$V=[v_0, v_1, \ldots, v_N]$
$v_i = \langle I, e_i \rangle$
$E = [e_0, e_1, \ldots, e_N]$

Fig. 2. Facial feature using Eigenfaces

Because Eigenfaces serve as basic elements of original faces, which allows each face to project itself to the Eigenfaces and the generated Eigenvectors have invariant properties of each face, we can use the Eigenface vectors as watermark keys of each identification card. In this work, we used the quantized facial features to serve as watermark keys, and embedded the watermark keys into the wavelet transformed face images for authentication purpose with joint wavelet compression and authentication watermark [15, 16, 17]. The invariant Eigenface and Eigenface vector properties provide a solution to two major challenges in developing authentication watermarks (a.k.a., integrity watermarks): how to extract short, invariant, and robust information to substitute fragile hash function; and how to embed information that is guaranteed to survive quantization-based lossy compression to an acceptable extent. Furthermore, the authentication watermarks not only serve as authentication purpose to verify the integrity of the face images, but also serve as the recovery bits for recovering approximate face values in corrupted IDs. This authenticator utilizes the compressed bitstream, and thus avoids rounding errors in reconstructing transform domain coefficients. At applications, the watermark can be embedded while the IDs are created. When the IDs or any other authenticated documents are distributed through network or other medias, an authentication verifier can automatically detect the face's Eigenface vectors, and compare them with watermark embedded somewhere in the image. If they are matched, the ID is authentic. Otherwise, the original face image can be restored from the face database based on the watermark key. The key point here is that we can embed invariant watermark bits in interesting locations that are specific to the quality of the image to allow convenient and robust watermark detection.

3.2 Watermarking embedding method with facial features

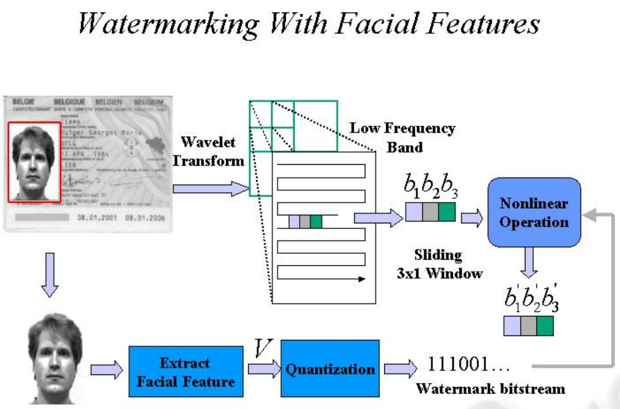


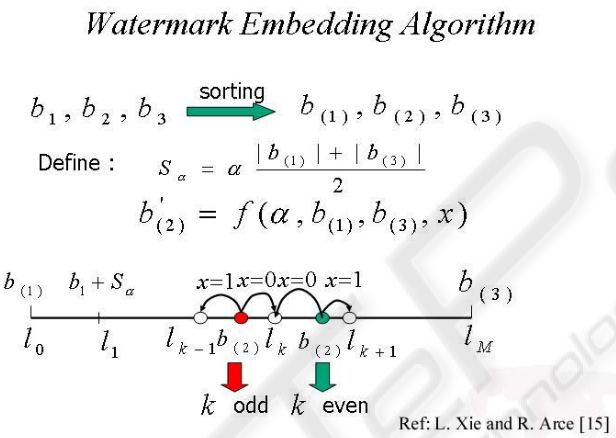
Fig. 3. Watermark key extraction via Eigenface vectors for photo ID authentication

In this demonstrable authentication system, we utilized cutting-edge face recognition technologies to help us to protect the most important features of the human being faces. We extracted facial features by decomposing the face picture into Eigenvectors over the Eigenfaces in the view-based and modular Eigenspaces for face recognition. Then we quantized these features into digital values to be embeded to watermark. HRL-developed watermark technologies [3] can be used as watermark embedding and detection method within any other *spaces of* the picture ID, such as signature area to demonstrate its effectiveness for verification and robustness against several attacks. Each watermark pattern is unique and robust to the specific face; and the watermark bits are embedded in the special features of DWT (Discrete Wavelet Transform) magnitude domain of the original image due to the advantages of rotation and scaling invariance. The mechanism is novel in that watermark created in the DWT domain for digital images allows robust detection and self-verification. Uniqueness of the watermark means that given a digital picture ID, the watermark can be identified as a unique label of the ID. We designed the watermark payload to be big enough to satisfy the uniqueness of watermark in digital picture ID protection applications. Besides, the wavelet-based watermark can be created dynamically according to the time and places of display so that the digital watermark can protect the multimedia content. Furthermore, watermark detection can be oblivious without original data: if the picture was detected as unauthentic, the possible authentic picture can be reconstructed out from the extracted watermark information and the engenspaces trained from existing face databases. Watermark Embedding Algorithm includes the following steps:

1). Extract facial features as described in section 3.1.

2). Conduct Feature quantization. Currently we are using uniform quantization (8-bits), and it can be improved by optimizing quantization with minimizing quantization error. Normally, increasing information rate (payload) for watermarking will increase watermark bits that are embedded, and thus make it more robust to printing and scanning processes, which is very important for watermark verifications using digital cameras and making picture IDs with our current watermarking authentication technology.

3). Apply the blind wavelet based digital signature for image authentication method. Here we used methods in [2, 3], and we also applied the method developed by Xie, et. al. [15, 16, 17] and the procedure is shown in Figures 3 and 4 and described next. Refer to paper [15, 16, 17] for more details.


Watermark Embedding Algorithm
$b_1, b_2, b_3 \xrightarrow{\text{sorting}} b_{(1)}, b_{(2)}, b_{(3)}$
Define :
$S_\alpha = \alpha \frac{|b_{(1)}| + |b_{(3)}|}{2}$
$b'_{(2)} = f(\alpha, b_{(1)}, b_{(3)}, x)$
$b_{(1)}$
$b_1 + S_\alpha$
x=1 x=0 x=0 x=1
$b_{(3)}$
l_0
l_1
l_{k-1} $b_{(2)}$ l_k $b_{(2)}$ l_{k+1}
l_M
k odd
k even

Ref: L. Xie and R. Arce [15]

Fig. 4. The watermark engraving structure

To assure robustness, the watermark bit sequence is embedded into the low-frequency band of the wavelet image representation with a sliding and non-overlapping *3x1* running window as illustrated in Fig. 3 and 4. A watermark bit is etched at each sliding location. Elements within the window are denoted as b_1, b_2, b_3, which are the coefficient values at locations with coordinates (*i - 1; j*), (*i; j*), (*i + 1; j*). The corresponding rank-ordered coefficients are denoted as $b_{(1)}$ <=$b_{(2)}$ <= $b_{(3)}$. Then a nonlinear Rank-order based transformation algorithm [15, 16, 17]is used that changes the median of these coefficients in the window area to $b'_{(2)} = f(\alpha, b_{(1)}, b_{(3);}\ x)$, where x is the watermark bit to be embedded, and the remaining coefficients are the same. To determined $b'_{(2)}$, as shown in Fig. 4, we first divided the range [$b_{(1),}$ $b_{(3)}$] into M intervals with interval step to be S_α with α as a tuning value, and $MS_\alpha > b_{(3)} - b_{(1)}$. As $b_{(2)}$ falls into the region [l_{k-1}, l_k], then $b'_{(2)} = l_{k-1}$ when k is odd and $x=1$ or k is even and $x= 0$; or $b'_{(2)} = l_k$ when k is even and $x=1$ or k is odd and $x= 0$.

4 Watermark Detection and Image Authentication Verification

At the detection or receiver side, watermark extraction procedure is shown in Fig. 5, and it is an inverted process of Section 3.2. A *3x1* window is shifted through the received wavelet transformed image, and a sequence with elements: $B_{(1),}$ $B_{(2)}$ and $B_{(3)}$ is obtained. The watermarked bit associated with the window at each location is extracted as: $x = arg\ min \mid B_{(2)} - f(a;\ b_{(1);}\ b_{(3)};\ x)\mid$ where x is within $(0,1)$ and is the possible value of the watermark sample and $B_{(1)} = b_{(1),}$, $B_{(3)} = b_{(3).}$ The need of the original image for retrieving the signature is removed since the invariance of rank-ordering is utilized to memorize the hidden information bit. Shifting the decoding window throughout the entire watermarked image, the entire embedded watermark sequence *V'* is retrieved. The received image is also needed to calculate the Eigenvector features *V* of the face image on the ID as described in Section 3.1. Authentication verification is executed by comparing it with the message bits carried by the watermark. Threshold is experimentally chosen as to maximize the detection accuracy of the authentication performance.

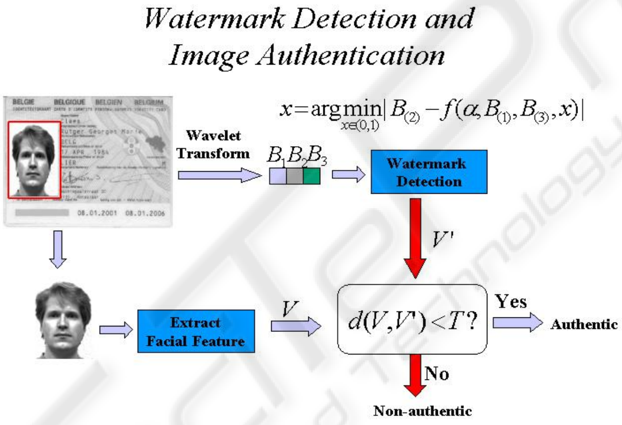


Fig. 5. Watermark detection and face ID authentication

5 Experimental Tests and Discussion

Using the method described in Section 3 and 4, we have an automatic verifiable ID system. If any watermark does not match with the intrinsic face image Eigenvector feature, we may use the detected watermark that should be equivalent to Eigenvector values to get the true face image restored, and it is as shown in Figure 6.

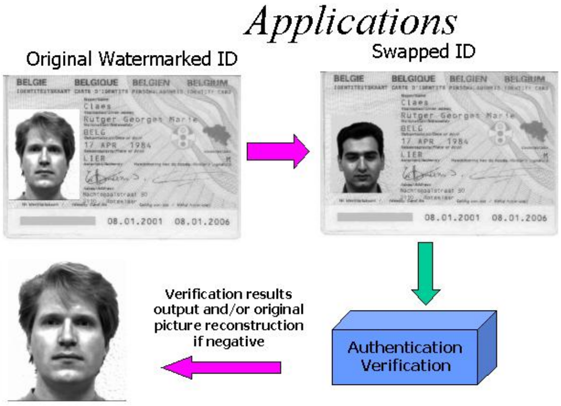

Applications
Original Watermarked ID
Swapped ID
Verification results output and/or original picture reconstruction if negative
Authentication Verification

Fig. 6. Watermark detection and face ID authentication

In this research, we first trained the system with about 100 sample faces with slightly angled face images. After watermark embedding, we did two types of test. First we switched the face image on the photo with no angle at all, and then we switched the face image to a different person's photo with no angle, and the system can recognize the right person's image, authenticate the ID and restore the corrupted one with a right face 100% under no further deterioration of the ID image's quality. Our system works for common attacks in digital image watermarks such as JPEG image recompression. However, we need to further validate our proposed algorithm and system with other attacks in digital image watermarks, image resizing, cropping, scaling and so on. Our demo and experiments show that our watermarking can survive some attacks up to such a promising level that the altered picture ID will inevitably be unacceptable.

6 Conclusion

In summary, we have developed a picture ID image authentication prototype using watermark to further protect multimedia content. The main novelty of our technology is to combine biometric information (face recognition techniques) with watermarking for secure ID document authentication. The decision rule of the watermark signature, which is uniquely assigned to the whole image based on the face image's unique and invariable feature vectors, makes the detection of the authentication watermark and the restoration of damaged face image robust. There are a wide variety of valuable applications for our watermark techniques. For example, watermarking techniques can also be used for stegnography and stegnoanalysis, covered channel communications and other security issues in secure information dissemination and homeland security applications. In the future, we will further study the robustness of this technique against A/D and D/A conversion.

References

1. B. B. Zhu, M D. Swanson, and A. H. Tewfik, "When seeing isn't believing," IEEE Signal Proceeding Magazine, March, 2004.
2. P. Sagetong and W. Zhou, "Dynamic Wavelet Feature-based Watermarking for Copyright Tracking in Digital Movie Distribution Systems," the IEEE International Conference of Imaging Processing, Rochester, NY, September, 2002.
3. W. Zhou, T. Rockwood and P. Sagetong, "Non-repudiation Oblivious Watermarking Schema for Secure Digital Video Distribution," the IEEE International Workingshop for Signal Processing, Virgin Island, December, 2002.
4. W. Diffle and M. E. Hellman, "New Directions in Cryptography," IEEE Trans. on Information Theory, Vol. 22, No. 6, pp-644-654, Nov 1976.
5. B. Zhu, M.D. Swanson, and A.H. Tewfik, "A transparent authentication and distortion measurement technique for images," in Proc. 7th IEEE Digital Signal Processing Workshop, Loen, Norway, Sept. 1996, pp. 45–48.
6. M. Schneider and S.-F. Chang, "A robust content based digital signature for image authentication," in Proc. IEEE Int. Conf. Image Processing, 1996, vol. 3, pp. 227–230.
7. D.-C. Lou and J.-L. Liu, "Fault resilient and compression tolerant digital signature for image authentication," IEEE Trans. Consumer Electron., vol. 46, no. 1, pp. 31–39, 2000.
8. M.P. Queluz, "Content-based integrity protection of digital images," in Proc. SPIE Conf. Security Watermarking Multimedia Contents, Jan. 1999, vol. 3657, pp. 85–93.
9. J. Dittmann, A. Steinmetz, and R. Steinmetz, "Content-based digital signature for motion pictures authentication and content-fragile watermarking," IEEE Int. Conf. Multimedia Computing and Systems, 1999, vol. 2, pp. 209–213.
10. C.-T. Li, D.-C. Lou, and T.-H. Chen, "Image authentication and integrity verification via content-based watermarks and a public key cryptosystem," in Proc. IEEE Int. Conf. Image Processing, 2000, vol. 3, pp. 694–697.
10. S. Bhattacharjee and M. Kutter, "Compression tolerant image authentication," in Proc. IEEE Int. Conf. Image Processing, 1998, vol. 1, pp. 435–439.
11. Chai Wah Wu. On the design of content-based multimedia authentication systems. IEEE Transaction on Multimedia, Vol. 4, No. 3, September, 2002.
12. F. Bartolini, A. Tefas, M. Barni and I. Pitas. Image Authentication Techniques for Surveillance Applications. Proceedings of the IEEE, Vol. 89, No. 10, October, 2001.
13. Turk, M., and Pentland, A. Face recognition using Eigenfaces. In *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR)* (June 1991), pp. 586-591.
14. D. Bolme, R. Beveridge, M. T., and Draper, B. The CSU face identifichation evaluation system: Its purpose, features and structure. In International Conference on Vision Systems *(April 2003), pp. 304-311.*
15. G. Arce L. Xie. "A joint wavelet compression and authentication watermarking," In IEEE International Conference on Image Processing, Chicago, IL, Oct 1998.
16. G. R. Arce L. Xie, "A blind wavelet based digital signature for image authentication," Proceedings of the EUSIPCO-98, Sept. 1998.
17. G. R. Arce L. Xie. "A blind content based digital image signature," Proceedings of the 2nd Annual Fedlab Symposium on ATIRP, Feb. 1998.