Visual Cryptography for Biometric Privacy

Arun Ross, *Senior Member, IEEE*, and Asem Othman, *Student Member, IEEE*

***Abstract*—Preserving the privacy of digital biometric data (e.g., face images) stored in a central database has become of paramount importance. This work explores the possibility of using visual cryptography for imparting privacy to biometric data such as fingerprint images, iris codes, and face images. In the case of faces, a private face image is dithered into two host face images (known as sheets) that are stored in two separate database servers such that the private image can be revealed only when both sheets are simultaneously available; at the same time, the individual sheet images do not reveal the identity of the private image. A series of experiments on the XM2VTS and IMM face databases confirm the following: 1) the possibility of hiding a private face image in two host face images; 2) the successful matching of face images reconstructed from the sheets; 3) the inability of sheets to reveal the identity of the private face image; 4) using different pairs of host images to encrypt different samples of the same private face; and 5) the difficulty of cross-database matching for determining identities. A similar process is used to de-identify fingerprint images and iris codes prior to storing them in a central database.**

***Index Terms*—De-identification, face, fingerprint, IrisCodes, privacy, visual cryptography.**

I. Introduction

BIOMETRICS is the science of establishing the identity of an individual based on physical or behavioral traits such as face, fingerprints, iris, gait, and voice [1]. A biometric authentication system operates by acquiring raw biometric data from a subject (e.g., face image), extracting a feature set from the data (e.g., eigen-coefficients), and comparing the feature set against the templates stored in a database in order to identify the subject or to verify a claimed identity. The template of a person in the database is generated during enrollment and is often stored along with the original raw data. This has heightened the need to accord privacy[1] to the subject by adequately protecting the contents of the database.

For protecting the privacy of an individual enrolled in a biometric database, Davida *et al.* [2] and Ratha *et al.* [3] proposed storing a transformed biometric template instead of the original biometric template in the database. This was referred to as a private template [2] or a cancelable biometric [3]. Feng *et al.* [4] proposed a three-step hybrid approach that combined the advantages of cryptosystems and cancelable biometrics. Apart from these methods, various image hiding approaches [5]–[7] have been suggested by researchers to provide anonymity to the stored biometric data.

For according privacy to face images present in surveillance videos, Newton *et al.* [8] and Gross *et al.* [9] introduced a face de-identification algorithm that minimized the chances of performing automatic face recognition while preserving details of the face such as expression, gender, and age. Bitouk *et al.* [10] proposed a face swapping technique which protected the identity of a face image by automatically substituting it with replacements taken from a large library of public face images. However, in the case of face swapping and aggressive de-identification, the original face image can be lost. Recently, Moskovich and Osadchy [11] proposed a method to perform secure face identification by representing a private face image with indexed facial components extracted from a public face database.

In this paper, the use of visual cryptography is explored to preserve the privacy of biometric data (viz., raw images) by decomposing the original image into two images in such a way that the original image can be revealed only when both images are simultaneously available; further, the individual component images do not reveal any information about the original image. Figs. 1 and 2 show block diagrams of the proposed approach for three biometric modalities. During the enrollment process, the private biometric data is sent to a trusted third-party entity. Once the trusted entity receives it, the biometric data is decomposed into two images and the original data is discarded. The decomposed components are then transmitted and stored in two different database servers such that the identity of the private data is not revealed to either server. During the authentication process, the trusted entity sends a request to each server and the corresponding sheets are transmitted to it. Sheets are overlaid (i.e., superimposed) in order to reconstruct the private image thereby avoiding any complicated decryption and decoding computations that are used in watermarking [5], [6], steganography [7], or cryptosystem [12] approaches. Once the matching score is computed, the reconstructed image is discarded. Further, cooperation between the two servers is essential in order to reconstruct the original biometric image.

For irides and fingerprints, as shown in Fig. 1, the biometric image is decomposed by the visual cryptography scheme and two noise-like images known as sheets are produced. In the case of securing an iris template, the iris code is encrypted instead of the iris image.

For faces, as shown in Fig. 2, each private face image is decomposed into two independent public host images. In this scenario, the private image can be viewed as being encrypted into two host face images.

Manuscript received June 28, 2010; revised September 24, 2010; accepted November 02, 2010. Date of publication December 06, 2010; date of current version February 16, 2011. This work was supported by U.S. NSF CAREER Award IIS 0642554. A preliminary version of this work was presented at the SPIE 2010 Conference, Orlando, FL. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Ajay Kumar.

The authors are with the Lane Department of Computer Science and Electrical Engineering, West Virginia University, Morgantown, WV 26506-6109 USA (e-mail: arun.ross@mail.wvu.edu; asem.othman@mail.wvu.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2010.2097252

[1]The term "privacy" as used in this paper refers to the de-identification of biometric data.

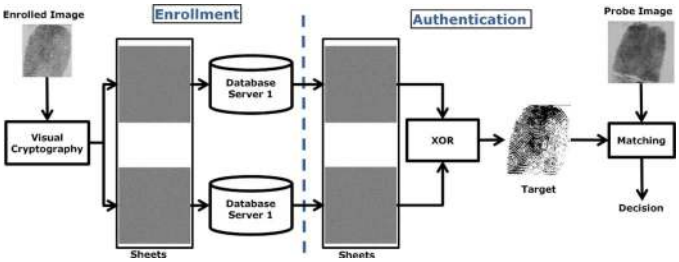

Fig. 1. Proposed approach for de-identifying and storing a fingerprint image. A similar technique is used for iris codes.

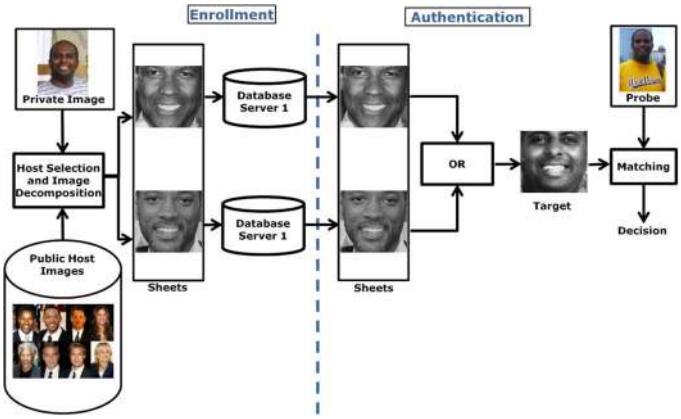

Fig. 2. Proposed approach for de-identifying and storing a face image.

The use of face images as hosts for a private face image (as opposed to using random noise or other natural images) has several benefits in the context of biometric applications. First, the demographic attributes of the private face images such as age, gender, ethnicity, etc. can be retained in the host images thereby preserving the demographic aspects of the face while perturbing its identity. Alternately, these demographic attributes, as manifested in an individual's face, can also be deliberately distorted by selecting host images with opposite attributes as that of the private image. Second, a set of public face images (e.g., those of celebrities) may be used to host the private face database. In essence, a small set of public images can be used to encrypt the entire set of private face images. Third, using nonface images as hosts may result in visually revealing the existence of a secret face as can be seen in Fig. 4. Finally, while decomposing the face image into random noise structures may be preferable, it can pique the interest of an eavesdropper by suggesting the existence of secret data.

Additionally, the proposed approach addresses the following template protection requirements [12]–[14]. **1) Diversity:** Since different applications can adopt different sets of host images for encrypting the same private face image, cross-matching across applications to reveal the identity of a private face image will be difficult. For iris codes and fingerprints, the sheets appear as random noise making it difficult to match them across databases. **2) Revocability:** If the private data is deemed to be compromised, then it can be decomposed again into two new sheets based on new host images. However, in reality, break-ins to a server are very hard to detect when the attacker simply steals certain information without modifying the stored data. To strengthen security, the decomposing operation can be periodically invoked at regular time intervals. **3) Security:** It is computationally hard to obtain the private biometric image from the individual stored sheets due to the use of visual cryptography. Furthermore, the private image is revealed only when both sheets are simultaneously available. By using distributed servers to store the sheets, the possibility of obtaining the original private image is minimized. There have been numerous efforts in the literature to guarantee that the data stored in distributed databases are protected from unauthorized modification and inaccurate updates (e.g., [15]) **4) Performance:** As will be shown in the experiments section, the recognition performance due to the reconstructed image is not degraded after decryption.

The rest of the paper is organized as follows. In Section II a basic introduction to visual cryptography and its extensions are presented. Sections III and IV discuss the proposed approach for securing iris, fingerprint, and face images. Section V reports the experimental results and Section VI concludes the paper.

II. Visual Cryptography

One of the best known techniques to protect data such as biometric templates [16] is cryptography. It is the art of sending and receiving encrypted messages that can be decrypted only by the sender or the receiver. Encryption and decryption are accomplished by using mathematical algorithms in such a way that no one but the intended recipient can decrypt and read the message. Naor and Shamir [17] introduced the visual cryptography scheme (VCS) as a simple and secure way to allow the secret sharing of images without any cryptographic computations. VCS is a cryptographic technique that allows for the encryption of visual information such that decryption can be performed using the human visual system. The basic scheme is referred to as the k-out-of-n VCS which is denoted as (k, n) VCS [17]. Given an original binary image T, it is encrypted in n images, such that

$$T = S_{h_1} \oplus S_{h_2} \oplus S_{h_3} \oplus \cdots \oplus S_{h_k} \tag{1}$$

where $\oplus$ is a Boolean operation, S_{h_i}, $h_i \in 1, 2, \ldots, k$ is an image which appears as white noise, $k \leq n$, and n is the number of noisy images. It is difficult to decipher the secret image T using individual S_{h_i}'s [17]. The encryption is undertaken in such a way that k or more out of the n generated images are necessary for reconstructing the original image T.

In the case of (2, 2) VCS, each pixel P in the original image is encrypted into two subpixels called shares. Fig. 3 denotes the shares of a white pixel and a black pixel. Note that the choice of shares for a white and black pixel is randomly determined (there are two choices available for each pixel). Neither shares provide any clue about the original pixel since different pixels in the secret image will be encrypted using independent random choices. When the two shares are superimposed, the value of the original pixel P can be determined. If P is a black pixel, we get two black subpixels; if it is a white pixel, we get one black subpixel and one white subpixel. Therefore, the reconstructed image will be twice the width of the original secret image and

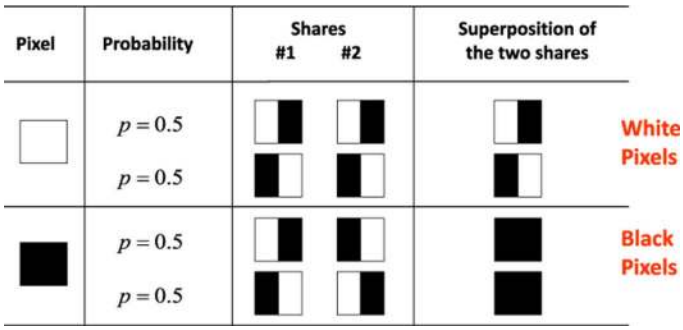

Fig. 3. Illustration of a 2-out-of-2 VCS scheme with 2 subpixel construction.

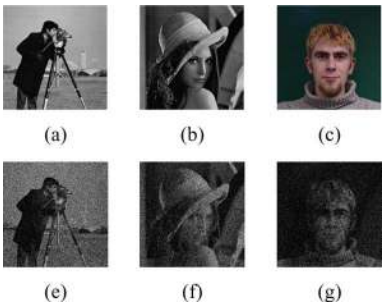

Fig. 4. Encryption of a private face image in two standard host images. (a) Host 1: Cameraman image. (b) Host 2: Lena image. (c) A private face image. (e) and (f) The two host images after visual encryption (two sheets). (g) Result of superimposing (e) and (f).

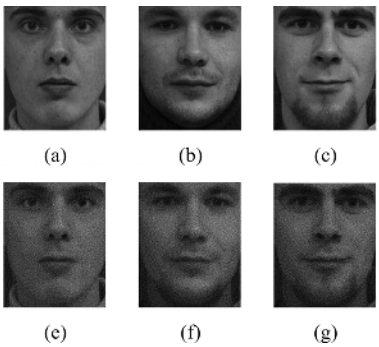

Fig. 5. Encryption of a private face image in two prealigned and cropped face images. (a) and (b) are two host images. (c) is a private face image. (e) and (f) are the host images after visual encryption (two sheets). (g) is the result of overlaying (e) and (f).

there will be a 50% loss in contrast [17]. However, the original image will become visible.

In 2002, Nakajima and Yamaguchi [18] presented a 2-out-of-2 extended VCS for natural images. They suggested a theoretical framework for encoding a natural image in innocuous images as illustrated in Figs. 4 and 5. This is known as the gray-level extended visual cryptography scheme (GEVCS). In this work, the basic VCS is used to secure iris codes and fingerprint images and the extended VCS for grayscale images is used to secure face images. The basic VCS and its extension (GEVCS) are discussed in detail below.

A. Visual Cryptography Scheme (VCS)

There are a few basic definitions which need to be provided before formally defining the VCS model and its extensions. **1) Secret image** (O): The original image that has to be hidden. In our application, this is the private biometric image. **2) Hosts** $(H's)$: These are the face images used to encrypt the secret image using the GEVCS. In our application, these correspond to the face images in the public dataset. **3) Sheets** $(S's)$: The secret image is encrypted into n sheet images which appear as random noise images (in the case of (k,n) VCS) or as a natural host image (in the case of GEVCS). **4) Target** (T): The image reconstructed by stacking or superimposing the sheets. **5) Subpixel:** Each pixel P is divided into a certain number of subpixels during the encryption process. **6) Pixel Expansion** (m): The number of subpixels used by the sheet images to encode each pixel of the original image. **7) Shares:** Each pixel is encrypted by n collections of m black-and-white subpixels. These collections of subpixels are known as shares. **8) Relative Contrast** (α): The difference in intensity measure between a black pixel and a white pixel in the target image. **9)** OR**-ed** m**-vector** (V): An $n \times m$ matrix is transformed to an m-dimensional vector by applying the Boolean OR operation across each of the m columns. **10) Hamming weight** $(H(V))$: The number of "1" bits in a binary vector V.

The k-out-of-n VCS deals with binary images. Each pixel is reproduced as n shares with each share consisting of m subpixels. This can be represented and described by an $n \times m$ Boolean matrix $B = [b_{ij}]$ where $b_{ij} = 1$ if and only if the jth subpixel in the ith share is black. The B matrix is selected randomly from one of two collections of $n \times m$ Boolean matrices C_0 and C_1; the size of each collection is r. If the pixel P in the secret image is a white pixel, one of the matrices in C_0 is randomly chosen; if it is a black pixel, a matrix from C_1 is randomly chosen. Upon overlaying these shares, a gray level for the pixel P of the target image becomes visible and it is proportional to the Hamming weight, $H(V)$, of the OR-ed m-vector V for a given matrix B. It is interpreted visually as black if $H(V) \geq d$ and as white if $H(V) < d - \alpha m$ for some fixed threshold $1 \leq d \leq m$ and relative difference $\alpha > 0$. The contrast of the target is the difference between the minimum $H(V)$ value of a black pixel and the maximum allowed $H(V)$ value for a white pixel, which is proportional to the relative contrast (α) and the pixel expansion (m). The scheme is considered valid if the following three conditions are satisfied. **Condition 1**: For any matrix B in C_0, the OR operation on any k of the n rows satisfies $H(V) < d - \alpha m$. **Condition 2**: For any matrix B in C_1, the OR operation on any k of the n rows satisfies $H(V) \geq d$. **Condition 3**: Consider extracting q rows, $q < k$, from two matrices, $B_0 \in C_0$ and $B_1 \in C_1$ resulting in new matrices B_0' and B_1'. Then, B_0' and B_1' are indistinguishable in that there exists a permutation of columns of B_0' which would result in B_1'. In other words, any $q \times m$ matrix $B_0 \in C_0$ and $B_1 \in C_1$ are identical up to a column permutation.

Conditions 1 and 2 define the image contrast due to VCS. Condition 3 imparts the security property of a (k,n) VCS which states that the careful examination of fewer than k shares will not provide information about the original pixel P. Therefore, the important parameters of the scheme are the following. First, the number of subpixels in a share (m); this parameter represents the loss in resolution from the original image to the resultant target image and it needs to be as small as possible such that the

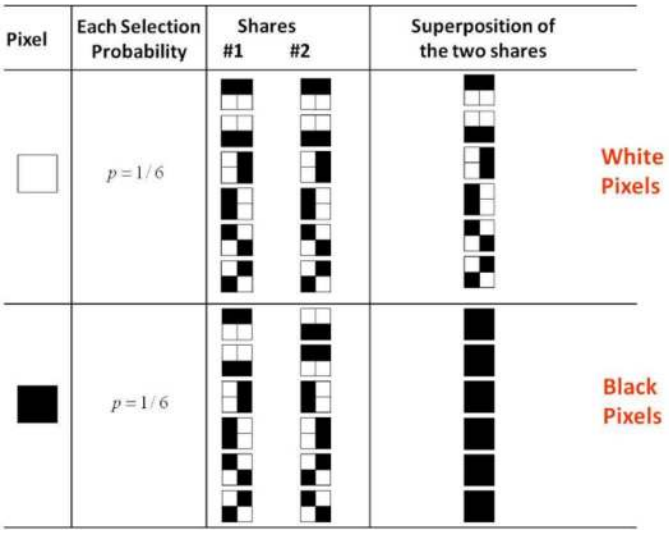

Fig. 6. Illustration of a 2-out-of-2 scheme with 4 subpixel construction.

target image is still visible. In addition, the m subpixels need to be in the form of a $v \times v$ matrix where $v \in \mathbb{N}$ in order to preserve the aspect ratio of the original image. Second, α, which is the relative difference in the Hamming weight of the combined shares corresponding to a white pixel and that of a black pixel in the original image; this parameter represents the loss in contrast and it needs to be as large as possible to ensure visibility of the target pixel. Finally, the size of the collection of C_0 and C_1, r, which represents the number of possibilities for B. This parameter does not directly affect the quality of the target image.

The scheme can be illustrated by a (2, 2) VCS example which is shown in Fig. 6. One pixel of the original image corresponds to four pixels in each share. Therefore, six patterns of shares are possible. Based on this, the following collection of matrices are defined:

$$C_0 = \left\{ \text{all the matrices obtained by permuting the columns of } \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix} \right\}$$

$$C_1 = \left\{ \text{all the matrices obtained by permuting the columns of } \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} \right\}.$$

This 2-out-of-2 VCS has the parameters $m = 4$, $\alpha = 1/2$, and $r = 6$. A secret image is encrypted by selecting shares in the following manner. If the pixel of the secret binary image is white, the same pattern of four pixels for both shares is randomly selected which is equivalent to randomly selecting a Boolean matrix B from the collection C_0. If the pixel of the original image is black, a complementary pair of patterns is randomly picked which is equivalent to selecting a Boolean matrix B from the collection C_1. Conditions 1 and 2 can be easily tested to validate this (2, 2) VCS. The last condition which is related to the security of the scheme can be verified by taking any row from $B_0 \in C_0$ and $B_1 \in C_1$ and observing that they have the same frequency of black and white values.

B. Gray-Level Extended Visual Cryptography Scheme (GEVCS)

VCS allows one to encode a secret image into n sheet images, each revealing no information about the original. Since these sheets appear as a random set of pixels, they may pique the curiosity of an interceptor by suggesting the existence of a secret image. To mitigate this concern, the sheets could be reformulated as natural images as stated by Naor and Shamir [17]. Ateniese *et al.* [19] introduced such a framework known as the extended VCS. Nakajima and Yamaguchi [18] proposed a theoretical framework to apply extended visual cryptography on grayscale images (GEVCS) and also introduced a method to enhance the contrast of the target images. The GEVCSoperates by changing the dynamic range of the original and host images, transforming the gray-level images into meaningful binary images (also known as halftoned images) and then applying a Boolean operation on the halftoned pixels of the two hosts and the original image. However, some of these pixels (in the host and the original) have to be further modified. This is explained in more detail below.

1) Digital Halftoning and Pixel Expansion: Digital halftoning is a technique for transforming a digital gray-scale image to an array of binary values represented as dots in the printing process [20]. Error diffusion is a type of halftoning technique in which the quantization error of a pixel is distributed to neighboring pixels which have not yet been processed. Floyd and Steinberg [21] described a system for performing error diffusion on digital images based on a simple kernel. Their algorithm could also be used to produce output images with more than two levels. So, rather than using a single threshold to produce a binary output, the closest permitted level is determined and the error, if any, is diffused to the neighboring pixels according to the chosen kernel. Therefore, grayscale images are quantized to a number of levels equalling the number of subpixels per share, m. During the dithering process at the pixel level, any continuous tone pixel is expanded to a matrix of black and white subpixels defined by the gray level of the original pixel. The proportion of white subpixels in this matrix is referred to as pixel transparency. In our application, the host images used for encrypting a private face image and the private image itself are converted to halftoned images.

2) Encryption: The encryption process is applied on a pixel-by-pixel basis using the three halftoned images (the two hosts and the original image). The arrangement of the subpixels in the shares of both the hosts has to be controlled such that the required transparency (the number of white subpixels) of the target pixel is obtained. The arrangement is determined based on the pixel transparencies triplet (t_1, t_2, t_T). t_1, t_2, and t_T are transparencies of the entire subpixel region for share 1, share 2, and the target, respectively.

The security of the scheme is also important. Therefore, during encryption, a Boolean matrix B is randomly selected from a set of $2 \times m$ Boolean matrices $C_{t_T}^{t_1,t_2}$ for every pixel in the original image. This is the primary difference between this scheme and Naor-Shamir's scheme: in the latter, only a

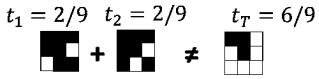

Fig. 7. Example of an impossible arrangement.

single collection of matrices is required which depends on the number of hosts and the pixel expansion (m). Nakajima and Yamaguchi describe in detail the method to compute this collection of Boolean matrices [18].

However, as shown in Fig. 7, there are cases when the required transparency for the corresponding pixel in the target image cannot be obtained, no matter how the shared subpixels are rearranged. Therefore, to determine if it is possible to obtain the target transparency by rearranging the transparent (white) subpixels in the shares, the target transparency must be within the following range [condition (T1)] [18]:

$$t_T \in [\max(0, (t_1 + t_2 - 1)), \min(t_1, t_2)] \tag{2}$$

where t_1, t_2, and $t_T (\in [0, 1])$ are the transparencies of the entire pixel region for share 1, share 2, and the target, respectively. The range of each of these transparencies for the entire image corresponds to the dynamic range of the pixel intensities of the respective images. Assuming that the dynamic ranges of the transparencies of the two sheets are the same, $[L, U] \subseteq [0, 1]$, all the triplets, (t_1, t_2, t_T), would satisfy condition (T1) if and only if the dynamic range of the target fulfils condition (T2) [18]

$$t_T \in [\max(0, (2U - 1)), L]. \tag{3}$$

Nakajima and Yamaguchi [18] described a method to enhance the image quality (contrast) and decrease the number of violated triplets by performing an adaptive dynamic range compression. In their method, the dynamic range of the sheets and the target are modified as $t_1, t_2 \in [L, L + K] \subseteq [0, 1]$, and $t_T \in [0, K] \subseteq [0, 1]$, respectively, where L denotes the lower bound of the sheets' dynamic range and K is a fixed value. It is clear that 0 is the most appropriate value for the lower bound of the target to ensure that the target is darker than both sheets [18]. However, after enhancing the contrast, it is necessary to consider condition (T1) again before encryption. Thus, if a triplet violates condition (T1), the gray levels of the conflicting triplets are adjusted and the resulting errors diffused to the nearby pixels. Consequently, both halftoning and encryption are done simultaneously to facilitate this adjustment.

To perform this adjustment, a 3-D space is defined using the transparencies of the pixels in the three images: the x-axis represents the transparencies of the pixels in share 1, the y-axis represents the transparencies of the pixels in share 2, and the z-axis represents the transparencies of the pixels in the target image. Any point in this space is characterized by a triplet representing transparencies in the three images. The volume corresponding to the points for which reconstruction is possible (Fig. 8) is determined. Every point outside this volume is adjusted. Assume a point $p' (t'_1, t'_2, t'_T)$ outside the determined volume. To encrypt this triplet without degrading the images, p' will be replaced with p'' where $p'' (t''_1, t''_2, t''_T)$ is the closest point to p' in the constructed volume. Thus, the transparencies of the corresponding pixels in share 1, share 2, and target will become t''_1, t''_2, and t''_T, respectively. If condition (T1) is violated, the errors are calculated and diffused using an error-diffusion algorithm to the nearby pixels. These steps are summarized in Fig. 9.

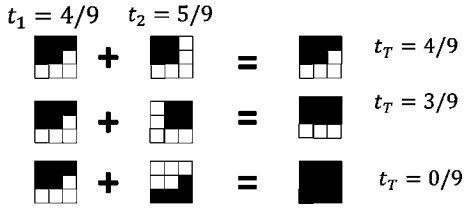

Fig. 8. Examples of subpixel arrangements.

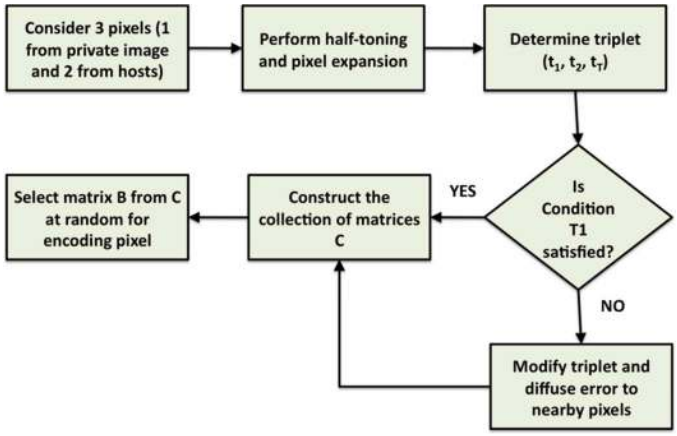

Fig. 9. Flowchart for illustrating GEVCS at the pixel-level.

III. Securing Iris and Fingerprint Templates

The use of basic visual cryptography for securing fingerprint and iris templates was suggested in [22] and [23], respectively; however, no experimental results were reported to demonstrate its efficacy. Moreover, basic VCS leads to the degradation in the quality of the decoded images, which makes it unsuitable for matching process, as shown in Fig. 10(a), where the white background of the original image becomes gray in the decrypted (target) image. The overlaying or superimposing operation in visual cryptography is computationally modeled as the binary OR operation which causes the contrast level of the target image to be lowered. Loss in contrast in target images could be addressed by simply substituting the OR operator with the XOR operator [24]. Furthermore, the target image can be down-sampled by reconstructing just one pixel from every 2×2 block. Thus, the reconstructed image will be visually appealing while requiring less storage space. Fig. 10 shows the difference in quality between the secret images recovered using the OR and XOR operations. It is clearly evident that the contrast of the original image is restored in the latter.

IV. Securing Private Face Images

Let $P = \{H_1, H_2, \ldots, H_N\}$ be the public dataset containing a set of candidate host images that can hide the assigned private face image O. The first task is to select two host images H_i and H_j, $i \neq j$ and $i, j = 1, 2, \ldots, N$ from P. Note that due to variations in face geometry and texture between the images in the public dataset and the private face image, the impact of the

(a) (b)

Fig. 10. Reconstructed fingerprint image when using the (a) OR and (b) XOR operators.

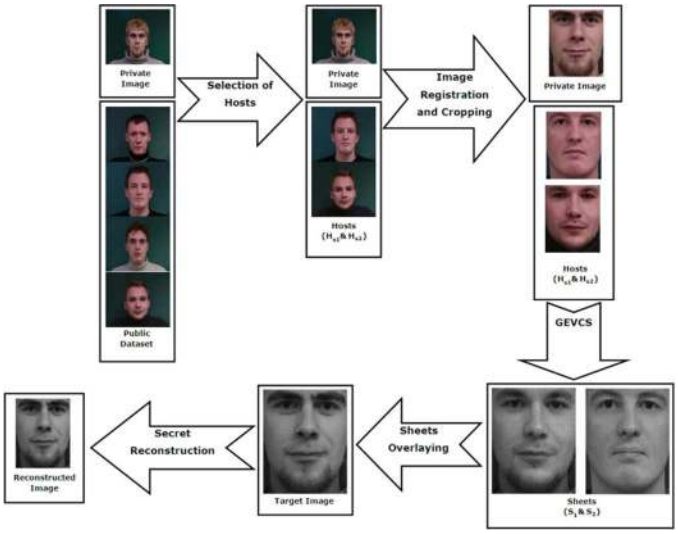

Fig. 11. Block diagram of the proposed approach for storing and matching face images.

Fig. 12. Example of an annotated face.

target image on the sheet images and vice versa may become perceptible. This issue can be mitigated if the host images for a particular private image are carefully chosen. Fig. 11 shows the block diagram that illustrates the key steps of the proposed approach. These steps will be explained in more detail in the following subsections.

A. Active Appearance Model

The proposed approach essentially selects host images that are most likely to be compatible with the private image based on geometry and appearance. Therefore, an active appearance model (AAM) [25] that characterizes the shape and texture of the face is utilized to determine the similarity between the private face image and candidate host images (Fig. 11). The steps for building the AAM and using it for locating predefined landmarks on face features, as shown in Fig. 12, is discussed in detail in [26] and [25] and is summarized below.

1) Building the AAM: Four steps are needed for building a basic AAM from a set of training images.

a) Annotate the Training Set: First, for each face image in the training dataset, its face features are annotated manually by landmarks of a predefined shape. Each shape X_j is stored in a vector format, where $j \in 1, \ldots, s$ and s is the number of training images. This representation does not include any information about the connection between landmarks. Thus,

$$X_j = [x_{1j}, x_{2j}, x_{3j}, \ldots, x_{nj}, y_{1j}, y_{2j}, y_{3j}, \ldots y_{nj}]^T \quad (4)$$

where n is the number of landmarks used to locate and annotate face features.

b) Building the Shape Model: A shape alignment process is performed to remove the effects of affine transformations (translation, scaling, and rotation). Then the principle component analysis (PCA) is used to construct a simple linear model of shape variability across the training images

$$\mathbf{X} = \bar{\mathbf{X}} + \Phi_s \mathbf{b_s}. \quad (5)$$

Here, $\bar{\mathbf{X}}$ is the mean shape vector, Φ_s is a matrix describing the modes of variation derived from the training set, and $\mathbf{b_s}$ is the shape model parameters vector.

c) Building the Texture Model: All images in the training set are warped to the mean shape by utilizing the annotated landmarks. Next, the pixel values in each warped image is consolidated to create a texture vector. Then, a photometric normalization is used to minimize the effects of lighting changes on the texture vector. The normalized texture vector is $\mathbf{g}$

$$\mathbf{g} = [g_1, g_2, g_3 \ldots g_m]^T \quad (6)$$

where m is the number of pixels within the image. Then, PCA is used to linearly model the texture vectors as in (7)

$$\mathbf{g} = \bar{\mathbf{g}} + \mathbf{\Phi}_g \mathbf{b_g}. \quad (7)$$

Here, $\bar{\mathbf{g}}$ is the mean texture vector, Φ_g is the modes of variation matrix, and $\mathbf{b_g}$ is the texture model parameter vector.

d) Building the Combined AAM: Shape and texture are often correlated [26] and, so, PCA is once again used to construct a compact model from $\mathbf{X}$ and $\mathbf{g}$ resulting in a set of combined parameters C. This helps in synthesizing an image with a given shape $\mathbf{X}$ and texture $\mathbf{g}$ using one set of parameters $\mathbf{C}$ as shown below

$$\mathbf{X} = \bar{\mathbf{X}} + \mathbf{\Phi}_s \mathbf{C} \quad (8)$$

$$\mathbf{g} = \bar{\mathbf{g}} + \mathbf{\Phi}_g \mathbf{C}. \quad (9)$$

2) Annotating an Image: A randomly selected template model is initially generated and an image based on the corresponding model parameters is synthesized. The error between the input image (I_{image}, that has to be annotated) and the synthesized image ($I_{\text{synthesized}}$) needs to be minimized. The solution is found by varying two sets of parameters: the combined model parameters $\mathbf{C}$ and the pose parameters (translation, scaling, and rotation).

Fig. 13. Shape-free image of annotated face image in Fig. 12.

B. Selection of Hosts

For selecting compatible hosts, the cost of registering (aligning) each image in the public dataset with the private image is computed as T_c. These costs are sorted in order to locate two host images, H_{s1} and H_{s2}, which have the smallest registration cost. However, as will be shown in the experiments section, this cost alone is not sufficient. So the texture is used as an additional criteria and the cost associated with this is denoted as A_c. Therefore, the final cost F_c, which is associated with each host image, is the sum of the normalized transformation cost T_c and the normalized appearance cost A_c. The simple minimum–maximum normalization technique is used to normalize both costs.

1) Transformation Cost T_C: This cost measures the amount of geometric transformation necessary to align two images based on the annotated landmarks generated by the AAM. Given the set of correspondences between these finite sets of points on two face images, a transformation $T : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ can be estimated to map any point from one set to the other. While there are several choices for modeling this geometric transformation, the thin plate spline (TPS) model is used [27]. The transformation cost T_c is the measure of how much transformation is needed to align the two face images by utilizing the thin plate spline model, which is the bending energy necessary to perform the transformation.

2) Appearance Cost A_C: First, the private face image (O) and the host image (H) are normalized by warping them to the mean shape, $\bar{\mathbf{X}}$, resulting in shape-free texture images O' and H'. Fig. 13 shows an example of a shape-free image for a private face image. This normalization step uses the mean shape computed during the AAM training phase. Each shape-free image is represented as a texture vector (6).

Both O' and H' can be expressed by the texture model parameter vector, $\mathbf{b_g}$. In order to get these basis vectors, each image is projected onto the texture space by using the stored modes of variation Φ_g

$$\mathbf{b_g} = \Phi_g^{-1} \cdot \{\mathbf{g} - \bar{\mathbf{g}}\}. \tag{10}$$

The appearance cost A_c is defined as the Manhattan distance between the basis vectors corresponding to O' and H'.

C. Image Registration and Cropping

In this step, the global affine transformation component of the thin plate spline model is used to align the two selected host images (H_{s1}, H_{s2}) with the secret image (O). Next, the aligned hosts and the secret image are cropped to capture only the facial features which have been located by AAM as illustrated in Fig. 12.

D. Secret Encryption and Reconstruction

GEVCS is used to hide the secret image O in the two host images H_{s1} and H_{s2} resulting in two sheets denoted as S_1 and S_2, respectively. S_1 and S_2 are superimposed in order to reveal the secret private image. The final target image is obtained by the reconstruction process that reverses the pixel expansion step to retain the original image size.

V. Experiments and Results

A. Securing Iris and Fingerprint Images

In the case of iris, the performance of the proposed technique was tested on a subset of the MBGC database containing NIR-iris videos. The left iris videos of 110 subjects were used in the experiments. Five frames were manually selected from each of these videos. Every frame was manually segmented and normalized to separate the iris region from the eye image. An open source Matlab implementation [28] based on Daugman's approach [29] was used to encode and match the normalized irides. There were five iris codes per subject: one of these was used as a probe and the rest were added to the gallery. The probe iris codes were encrypted and reconstructed using the (2, 2) VCS. The experiment consisted of matching the probes against the gallery entries. The equal error rate (EER) was used to observe the matching performance of the original as well as the reconstructed probes. In both cases, the EER was the same ($\sim$6.3%). Next, the possibility of exposing the identity by using the sheet images as probes and the original iris codes as gallery was investigated. However, this resulted in an EER of 50% suggesting the difficulty in using individual sheets to reveal the original iris code.

In the case of fingerprints, the performance of the proposed technique was tested on the NIST-4 fingerprint database[2] containing inked fingerprints exhibiting large variations in quality. The database consists of the grayscale images of 2000 fingers with two impressions per finger. One of these impressions was used as a probe image and the other was added to the gallery. Since the proposed technique was devised for binary fingerprint images, a threshold value was used to generate the binary image for each probe. Each binary image was then decomposed into two sheets using (2, 2) VCS. The sheets were superimposed to get the target image, as shown in Fig. 1. The reconstructed as well as the original grayscale fingerprint probes were matched against the impressions in the gallery. Using the original fingerprint images as probes resulted in an EER of $\sim$8%.[3] Table I shows the result of using the reconstructed fingerprints as probes; the performance is reported as a function of the different threshold values used to binarize the original probe images. It is observed that a threshold of 180 results in an EER of $\sim$9.13%. These experiments suggest the possibility of decomposing and storing fingerprint images.

B. Securing Private Face Images

In the case of faces, the performance of the proposed technique was tested on two different databases: the IMM and

[2]http://www.nist.gov/data/WebGuide/SD_4/FingerprintDB_4.htm

[3]No attempt was made to optimize the performance of the fingerprint matcher (VeriFinger SDK) on this dataset.

TABLE I
EQUAL ERROR RATES (%) AT DIFFERENT THRESHOLD VALUES TH

TH	EER
128	35.3
150	13.7
180	9.13

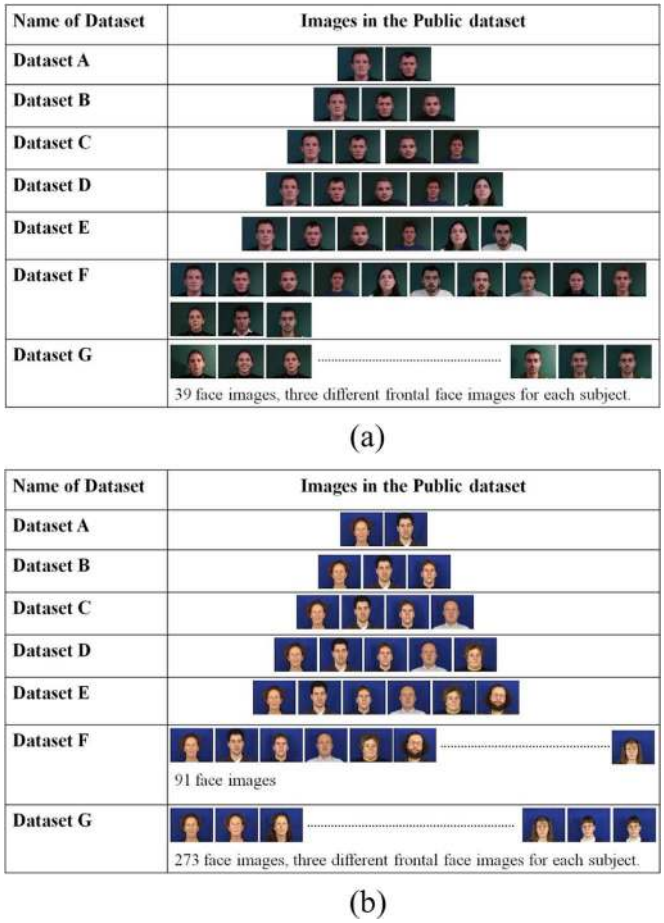

Fig. 14. Images in the public datasets for both the (a) IMM and (b) XM2VTS databases.

XM2VTS databases. These databases were used since the facial landmarks of individual images were annotated and available online. These annotations were necessary for the AAM scheme. The IMM Face Database [30] is an annotated database containing 6 face images each of 40 different subjects; 3 of the frontal face images per subject were used in the experiments. Twenty-seven subjects were used to construct the private dataset and the remaining 13 were used as the public dataset. The XM2VTS frontal image database [31] consists of 8 frontal face images each of 295 subjects. One hundred ninety-two of these subjects were used to construct the private dataset and 91 subjects were used to construct the pubic dataset. The remaining subjects were excluded because several of their face images could not be processed by the commercial matcher. The composition of the public dataset is shown in Fig. 14. The AAM for each database was constructed using the face images (one per subject) from the public dataset. Fig. 15 shows examples of

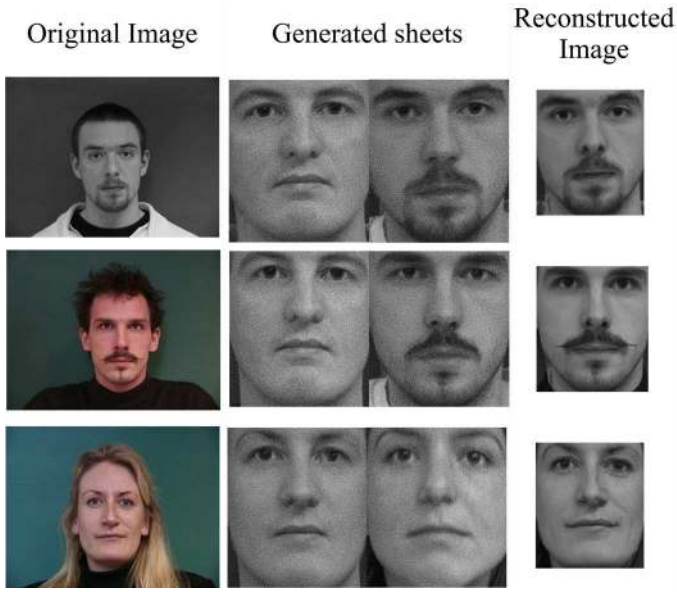

Fig. 15. Illustration of the proposed approach using images from the IMM database.

TABLE II
EQUAL ERROR RATES (%) WHEN USING DIFFERENT PUBLIC DATASETS WITH $K = 0.567$ AND $m = 16$

Dataset	IMM Database	XM2VTS Database
A	9.7	21.9
B	7.7	21.8
C	6.3	21.7
D	5.6	21.4
E	11.4	22

TABLE III
EQUAL ERROR RATES (%) WHEN USING DIFFERENT PUBLIC DATASETS WITH $K = 0.875$ AND $m = 36$

Dataset	IMM Database	XM2VTS Database
A	2.2	6.4
B	2.1	6.4
C	2	6.2
D	2	6
E	3.4	10.2

the proposed approach when dataset D in Fig. 14(a) is used as the public dataset (here $L = 0,\ K = 0.75,\ m = 36$).

In the following experiments, the match scores were generated using the Verilook SDK.[4] In order to establish a baseline, the images in the private database were first matched against each other. This resulted in an EER of ∼6% for the IMM database and ∼2% for the XM2VTS database.

1) Experiment 1: In this experiment, the impact of varying the number of images in the public dataset was investigated (datasets A, B, C, D, and E were used). The selection of hosts from the public dataset was based only on the transformation cost. The experiment consisted of matching the reconstructed private images against each other. EERs using the five public datasets are shown in Tables II and III. For the IMM database in Table II, it is clear that adding more images to the public dataset

[4]Available: http://www.neurotechnology.com

TABLE IV
EQUAL ERROR RATES (%) WHEN DIFFERENT SELECTION CRITERIA ARE USED WITH $K = 0.567$ AND $m = 16$

Selection Criteria	IMM Database	XM2VTS Database
T_c	11.4	22
$T_c + A_c$	8	21

TABLE V
EQUAL ERROR RATES (%) WHEN DIFFERENT SELECTION CRITERIA ARE USED WITH $K = 0.875$ AND $m = 36$

Selection Criteria	IMM Database	XM2VTS Database
T_c	3.4	10.2
$T_c + A_c$	2	6

TABLE VI
EQUAL ERROR RATES (%) FOR DIFFERENT VALUES OF K AND $m = 16$. THE CHOICE OF K IS BASED ON [18]

K	IMM Database	XM2VTS Database
0.567	10.7	21.4
0.6888	6.5	17.5
0.75	7.8	16
0.875	5.9	15

(a) (b) (c) (d)

Fig. 16. Examples of reconstructed images for a subject with different values for the pixel expansion factor, m. (a) $m = 4$; (b) $m = 16$; (c) $m = 36$; (d) $m = 100$.

TABLE VII
EQUAL ERROR RATES (%) FOR DIFFERENT VALUES OF K AND $m = 36$. THE CHOICE OF K IS BASED ON [18]

K	IMM Database	XM2VTS Database
0.567	5.3	12.6
0.6888	5	6.5
0.75	4	6.3
0.875	2	6

initially improves the result. However, Dataset E results in the worst EER with respect to the other datasets. This drop in performance could be attributed to the inclusion of an individual with a beard in the public dataset: the absence of the appearance cost led to the selection of this host image even for those private face images that did not possess a beard, thereby affecting the reconstructed images.

2) Experiment 2: In this experiment, the appearance cost was added to the criterion to select the host images and it is clear that this solves the problem encountered in Experiment 1. Dataset E is used in this experiment to select the hosts (H_1, H_2). Tables IV and V show the EERs of the reconstructed images when host images are selected using (a) the transformation cost T_c only and (b) the sum of the normalized transformation cost T_c and appearance cost A_c.

From both the above experiments it is also apparent that $K = 0.875$ and $m = 36$ results in better matching performance.

3) Experiment 3: The purpose of this experiment was to determine if the encrypted face images upon reconstruction could be successfully matched against the original private face images. To evaluate this, the public Dataset A in Fig. 14, consisting of two fixed face images as hosts, was used. For each subject in the private dataset, one frontal face image was selected[5] as the secret image to be encrypted by the two host face images. The VCS was invoked with contrast $K = 0.875$ and a pixel expansion factor of $m = 36$. The reconstructed images were observed to match very well with the original images resulting in an EER of $\sim$0% in the case of the IMM database and 0.5% in the case of the XM2VTS database. On other hand, when either of the sheets were matched against the original images, the resultant EERs were greater than 45%.

4) Experiment 4: The purpose of this experiment was to determine if the reconstructed face images could be successfully matched against those images in the private dataset that were not used in Experiment 3. To establish this, for each subject in the reconstructed dataset, N frontal face images were chosen from the private database to assemble the gallery ($N = 2$ for IMM and $N = 3$ for XM2VTS). The matching exercise consisted of comparing the reconstructed face images (from Experiment 1) against these gallery images (not used in Experiment 1). An EER of $\sim$2% was obtained for the IMM database. This performance, in this case, was even better than that of the original images (EER $\sim 6\%$). The improvement could be due to the contrast enhancement of the private face images that occurs when increasing the dynamic range of the sheets resulting in improved quality of the reconstructed secret image. For the XM2VTS database, the obtained EER was $\sim$6% which is still comparable with the 2% obtained when matching the original images.

5) Experiment 5: By using public Dataset D and $m = 16$ and 36, sheet images were created with different contrast values: $K = 0.567, 0.6888, 0.75, 0.875$. Tables VI and VII report the EERs for these different values of K. Here, the matching procedure was the same as that of Experiment 4. For both databases, $K = 0.875$ results in better performance than the other values. This improvement could be due to the contrast enhancement of the target images that occurs by increasing the dynamic range of the sheets and, consequently, the quality of the target image.

6) Experiment 6: Next, the effect of pixel expansion on the final reconstructed image was tested. Fig. 16 shows that details of the sheets can appear on the final image for higher values of m. The impact of m on matching performance is shown in Table VIII. Here, the matching procedure was the same as that of Experiment 4. The host images were selected from Dataset D with $K = 0.567$. As shown in Fig. 16, the pixel expansion value affects the number of gray-levels in the reconstructed image, and this impacts the amount of detail appearing in it. Therefore, when m is 100, the visual details of the sheet images appear on the reconstructed image resulting in a drop in overall performance.

7) Experiment 7: In this experiment, the possibility of exposing the identity of the secret image by using the sheet images in the matching process is investigated. For this experiment, the sheet images for three different face samples of the

[5]In the case of IMM database, the face sample exhibiting neutral expression and diffuse light was selected

TABLE VIII
EQUAL ERROR RATES FOR DIFFERENT VALUES OF $m(\%)$

m	IMM Database	XM2VTS Database
4	23.5	41
16	10.7	21.4
36	5.3	12.6
100	8	11

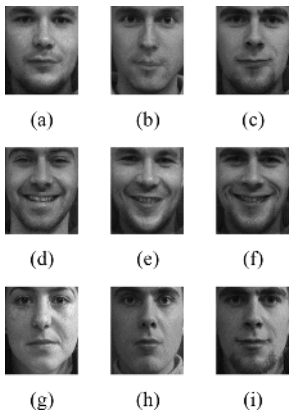

Fig. 17. Examples from experiment 7 where (a), (d), and (g) are the first sheets and (b), (e), and (h) are the second sheets. (c), (f), and (i) are the corresponding reconstructed face images.

same subject were first computed. Next, the reconstructed images and the corresponding sheets were independently used in the matching process (i.e., sheet image 1 of all the private images were matched against each other; sheet image 2 of all the private images were matched against each other; reconstructed images of all the private images were matched against each other). Fig. 17 shows that each subject in the private dataset has three reconstructed images. The public datasets used in this experiments were datasets A, F, and G. This experiment resulted in three EERs: the first was a result of using the reconstructed target images for matching, while the second and the third EERs were a result of using the first sheet and second sheet, respectively, for matching. The results in Table IX confirm the difficulty of exposing the identity of the secret face image by using the sheets alone.

Note that Experiment 7 involves automatic host selection from the public dataset based on the registration cost F_c described earlier. The positive impact of automatic host selection is seen in Fig. 17 where the selected host images (sheets) and the secret image are observed to have compatible expressions.

8) Experiment 8: Different applications may employ different public datasets for host image selection. Thus, the hosts selected for encrypting an individual's face image can differ across applications. This experiment seeks to confirm that cross-matching of the stored sheets across applications (and inferring identities) will not be feasible. To demonstrate this, the possibility of using host images from *different* public databases for encrypting the same identity (i.e., face image) was investigated. The experiment was set up as follows. Two face samples of each of the 192 subjects in the XM2VTS private dataset were randomly selected. For an arbitrary subject, let O_1 and O_2 denote the two face samples that were selected. Further, let O_1 be encrypted into sheets S_1^{IMM} and S_2^{IMM} using a public

TABLE IX
EQUAL ERROR RATES (%) FOR EXPERIMENT 7. EXPERIMENTS CONFIRM THE DIFFICULTY OF USING INDIVIDUAL SHEET IMAGES TO REVEAL THE SECRET IMAGE

	EER (%)
Reconstructed vs Reconstructed	2.4
Sheet 1 vs Sheet 1	44.7
Sheet 2 vs Sheet 2	44.2

(a) IMM Database: Dataset A

	EER (%)
Reconstructed vs Reconstructed	6.2
Sheet 1 vs Sheet 1	36.0
Sheet 2 vs Sheet 2	33.8

(b) XM2VTS Database: Dataset A

	EER (%)
Reconstructed vs Reconstructed	7.4
Sheet 1 vs Sheet 1	35.7
Sheet 2 vs Sheet 2	40

(c) IMM Database: Dataset F

	EER (%)
Reconstructed vs Reconstructed	8.2
Sheet 1 vs Sheet 1	31.7
Sheet 2 vs Sheet 2	38.3

(d) XM2VTS Database: Dataset F

	EER (%)
Reconstructed vs Reconstructed	6.8
Sheet 1 vs Sheet 1	33.8
Sheet 2 vs Sheet 2	39.5

(e) IMM Database: Dataset G

	EER (%)
Reconstructed vs Reconstructed	9.2
Sheet 1 vs Sheet 1	37.8
Sheet 2 vs Sheet 2	39.3

(f) XM2VTS Database: Dataset G

dataset from the IMM database. Similarly, let O_2 be encrypted into sheets S_1^{XM2VTS} and S_2^{XM2VTS} using a public dataset from the XM2VTS database. Let T_1 and T_2 denote the reconstructed face images pertaining to O_1 and O_2, respectively. The following matching exercises were conducted: (a) S_1^{IMM} against S_1^{XM2VTS}; (b) S_1^{IMM} against S_2^{XM2VTS}; (c) S_2^{IMM} against S_1^{XM2VTS}; (d) S_2^{IMM} against S_2^{XM2VTS}; (e) T_1 against T_2. The public datasets used in this experiment was the same as Experiment 7 (i.e., Datasets A, F, and G). Table X shows the EERs for these matching experiments and it is clear that it is difficult to perform cross-matching across different applications. However, when the corresponding reconstructed images ($m = 36$ and $K = 0.875$) are compared, the resulting EER suggests the possibility of successful matching.

VI. CONCLUSION AND DISCUSSION

This paper explored the possibility of using visual cryptography for imparting privacy to biometric templates. In the case of fingerprints and iris, the templates are decomposed into two noise-like images using (2, 2) VCS, and since the spatial arrangement of the pixels in these images varies from block to block, it is impossible to recover the original template without accessing both the shares. The XOR operator is used to superimpose the two noisy images and fully recover the original template. In addition, the contribution of this paper includes a methodology to protect the privacy of a face database by decomposing an input private face image into two independent sheet images such that the private face image can

TABLE X
EQUAL ERROR RATES (%) FOR EXPERIMENT 8

Matching	EER (%)
S_1^{IMM} vs S_1^{XM2VTS}	47.4
S_1^{IMM} vs S_2^{XM2VTS}	48.2
S_2^{IMM} vs S_1^{XM2VTS}	50
S_2^{IMM} vs S_2^{XM2VTS}	46.3
T_1 vs T_2	13.6

(a) Datasets A

Matching	EER (%)
S_1^{IMM} vs S_1^{XM2VTS}	49
S_1^{IMM} vs S_2^{XM2VTS}	49.5
S_2^{IMM} vs S_1^{XM2VTS}	49
S_2^{IMM} vs S_2^{XM2VTS}	48.5
T_1 vs T_2	4.4

(b) Datasets F

Matching	EER (%)
S_1^{IMM} vs S_1^{XM2VTS}	48.3
S_1^{IMM} vs S_2^{XM2VTS}	50
S_2^{IMM} vs S_1^{XM2VTS}	48.6
S_2^{IMM} vs S_2^{XM2VTS}	50
T_1 vs T_2	4.8

(c) Datasets G

be reconstructed only when both sheets are simultaneously available. The proposed algorithm selects the host images that are most likely to be compatible with the secret image based on geometry and appearance. GEVCS is then used to encrypt the private image in the selected host images. It is observed that the reconstructed images are similar to the original private image. The study on the effect of various parameters (K and m) on the matching performance suggests that there is indeed a relation between the quality of the reconstructed secret and these parameters. Finally, experimental results demonstrate the difficulty of exposing the identity of the secret image by using only one of the sheets; further individual sheets cannot be used to perform cross-matching between different applications.

Increasing the pixel expansion factor m can lead to an increase in the storage requirements for the sheets. In the recent literature there have been some efforts to develop a VCS without pixel expansion [32], [33]. But no such scheme currently exists for generating sheets that are not random noisy images. Thus, more work is necessary to handle this problem.

ACKNOWLEDGMENT

The authors are grateful to R. Jillela for his assistance with the iris experiments.

REFERENCES

[1] A. Jain, P. Flynn, and A. Ross, *Handbook of Biometrics*. New York: Springer, 2007.
[2] G. I. Davida, Y. Frankel, and B. J. Matt, "On enabling secure applications through off-line biometric identification," in *Proc. IEEE Symp. Security and Privacy*, 1998, pp. 148–157.
[3] N. Ratha, J. Connell, and R. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Syst. J.*, vol. 40, no. 3, pp. 614–634, 2001.
[4] Y. Feng, P. Yuen, and A. Jain, "A hybrid approach for face template protection," in *Proc. SPIE Conf. Biometric Technology for Human Identification*, Orlando, FL, 2008, vol. 6944.
[5] A. Jain and U. Uludag, "Hiding biometric data," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 25, no. 11, pp. 1494–1498, Nov. 2003.
[6] J. Dong and T. Tan, "Effects of watermarking on iris recognition performance," in *Proc. 10th Int. Conf. Control, Automation, Robotics and Vision, 2008 (ICARCV 2008)*, 2008, pp. 1156–1161.
[7] N. Agrawal and M. Savvides, "Biometric data hiding: A 3 factor authentication approach to verify identity with a single image using steganography, encryption and matching," in *Proc. Computer Vision and Pattern Recognition Workshop*, 2009, vol. 0, pp. 85–92.
[8] E. M. Newton, L. Sweeney, and B. Malin, "Preserving privacy by de-identifying face images," *IEEE Trans. Knowl. Data Eng.*, vol. 17, no. 2, pp. 232–243, Feb. 2005.
[9] R. Gross, L. Sweeney, F. De la Torre, and S. Baker, "Model-based face de-identification," in *IEEE Workshop on Privacy Research in Vision*, Los Alamitos, CA, 2006.
[10] D. Bitouk, N. Kumar, S. Dhillon, P. Belhumeur, and S. K. Nayar, "Face swapping: Automatically replacing faces in photographs," *ACM Trans. Graph.*, vol. 27, no. 3, pp. 1–8, 2008.
[11] B. Moskovich and M. Osadchy, "Illumination invariant representation for privacy preserving face identification," in *Proc. IEEE Computer Society and IEEE Biometrics Council Workshop on Biometrics*, San Francisco, CA, Jun. 2010, pp. 154–161.
[12] A. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP J. Advances Signal Process.*, pp. 1–17, 2008.
[13] D. Maltoni, D. Maio, A. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*. Secaucus, NJ: Springer-Verlag New York, Inc., 2003.
[14] S. Prabhakar, S. Pankanti, and A. Jain, "Biometric recognition: Security and privacy concerns," *IEEE Security Privacy*, vol. 1, no. 2, pp. 33–42, Mar./Apr. 2003.
[15] B. Thuraisingham and W. Ford, "Security constraint processing in a multilevel secure distributed database management system," *IEEE Trans. Knowl. Data Eng.*, vol. 7, no. 2, pp. 274–293, Apr. 1995.
[16] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, and B. Kumar, "Biometric encryption," in *ICSA Guide to Cryptography*. New York: McGraw-Hill, 1999.
[17] M. Naor and A. Shamir, "Visual cryptography," in *Proc. EUROCRYPT*, 1994, pp. 1–12.
[18] M. Nakajima and Y. Yamaguchi, "Extended visual cryptography for natural images," *J. WSCG*, vol. 10, no. 2, pp. 303–310, 2002.
[19] G. Ateniese, C. Blundo, A. Santis, and D. Stinson, "Extended capabilities for visual cryptography," *Theor. Comput. Sci.*, vol. 250, no. 1–2, pp. 143–161, 2001.
[20] S. Shevell, *The Science of Color*. Amsterdam, The Netherlands: Elsevier Science Ltd., 2003.
[21] R. Floyd and L. Steinberg, "An adaptive algorithm for spatial greyscale," *SPIE Milestone Series*, vol. 154, pp. 281–283, 1999.
[22] Y. Rao, Y. Sukonkina, C. Bhagwati, and U. Singh, "Fingerprint based authentication application using visual cryptography methods (improved id card)," in *Proc. IEEE Region 10 Conf.*, Nov. 2008, pp. 1–5.
[23] P. Revenkar, A. Anjum, and W. Gandhare, "Secure iris authentication using visual cryptography," *Int. J. Comput. Sci. (IJCSIS)*, vol. 7, no. 3, pp. 217–221, Mar. 2010.
[24] D. Jin, W.-Q. Yan, and M. S. Kankanhalli, "Progressive color visual cryptography," *J. Electron. Imag.* vol. 14, no. 3, p. 033019, 2005 [Online]. Available: http://link.aip.org/link/?JEI/14/033019/1
[25] T. Cootes *et al.*, "Active appearance models," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 23, no. 6, pp. 681–685, Jun. 2001.
[26] M. B. Stegmann, "Active Appearance Models: Theory, Extensions and Cases," Master's thesis, Informatics and Mathematical Modelling, Technical University of Denmark, DTU, Kgs. Lyngby, Aug. 2, 2000 [Online]. Available: http://www.imm.dtu.dk/aam/main/
[27] F. Bookstein, "Principal warps: Thin-plate splines and the decomposition of deformations," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 11, no. 6, pp. 567–585, Jun. 1989.
[28] L. Masek and P. Kovesi, *Matlab Source Code for a Biometric Identification System Based on Iris Patterns*. Perth, Australia: Dept. of Computer Science and Software Engineering, The University of Western Australia, 2003.
[29] J. Daugman, "Demodulation by complex-valued wavelets for stochastic pattern recognition," *Int. J. Wavelets, Multiresolution Inf. Process.*, vol. 1, no. 1, pp. 1–17, 2003.
[30] M. B. Stegmann, B. K. Ersbøll, and R. Larsen, "FAME—A flexible appearance modelling environment," *IEEE Trans. Med. Imag.*, vol. 22, no. 10, pp. 1319–1331, Oct. 2003.
[31] K. Messer, J. Matas, J. Kittler, J. Luettin, and G. Maitre, "XM2VTSDB: The extended M2VTS database," in *Proc. 2nd Int. Conf. Audio and Video-Based Biometric Person Authentication*, 1999, pp. 965–966.
[32] Y. Chen, Y. Chan, C. Huang, M. Tsai, and Y. Chu, "A multiple-level visual secret-sharing scheme without image size expansion," *Inf. Sci.*, vol. 177, no. 21, pp. 4696–4710, 2007.

[33] T. Lin, S. Horng, K. Lee, P. Chiu, T. Kao, Y. Chen, R. Run, J. Lai, and R. Chen, "A novel visual secret sharing scheme for multiple secrets without pixel expansion," *Expert Systems With Applications*, vol. 37, no. 12, pp. 7858–7869, 2010.

[34] A. Ross and A. A. Othman, "Visual cryptography for face privacy," in *Proc. SPIE Biometric Technology for Human Identification VII*, Orlando, FL, 2010, vol. 7667.

Arun Abraham Ross (S'00–M'03) received the B.E. (Hons.) degree in computer science from the Birla Institute of Technology and Science, Pilani, India, in 1996, and the M.S. and Ph.D. degrees in computer science and engineering from Michigan State University, East Lansing, in 1999 and 2003, respectively.

Between 1996 and 1997, he was with the Design and Development Group of Tata Elxsi (India) Ltd., Bangalore, India. He also spent three summers (2000–2002) with the Imaging and Visualization Group of Siemens Corporate Research, Inc., Princeton, NJ, working on fingerprint recognition algorithms. He is currently a Robert C. Byrd Associate Professor in the Lane Department of Computer Science and Electrical Engineering, West Virginia University, Morgantown. His research interests include pattern recognition, classifier fusion, machine learning, computer vision, and biometrics. He is actively involved in the development of biometrics and pattern recognition curricula at West Virginia University. He is the coauthor of *Handbook of Multibiometrics* and coeditor of *Handbook of Biometrics*.

Dr. Ross is a recipient of NSF's CAREER Award and was designated a Kavli Frontier Fellow by the National Academy of Sciences in 2006. He is an Associate Editor of the IEEE TRANSACTIONS ON IMAGE PROCESSING and the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY.

Asem Othman (S'09) received the B.Sc. (Hons.) and M.Sc. degrees in systems and biomedical engineering from Cairo University, Cairo, Egypt, in 2004 and 2008, respectively. He is currently working toward the Ph.D. degree in the Lane Department of Computer Science and Electrical Engineering, West Virginia University, Morgantown.

His current research interests are image processing, computer vision, and biometrics.