Proc. of SPIE Conference on Biometric Technology for Human Identification VII, (Orlando, USA), April 2010

Visual Cryptography for Face Privacy

Arun Ross and Asem A. Othman

Lane Department of Computer Science and Electrical Engineering, West Virginia University,
Morgantown, WV 26506 USA

ABSTRACT

We discuss the problem of preserving the privacy of a digital face image stored in a central database. In the proposed scheme, a private face image is dithered into two host face images such that it can be revealed only when both host images are simultaneously available; at the same time, the individual host images do not reveal the identity of the original image. In order to accomplish this, we appeal to the field of Visual Cryptography. Experimental results confirm the following: (a) the possibility of hiding a private face image in two unrelated host face images; (b) the successful matching of face images that are reconstructed by superimposing the host images; and (c) the inability of the host images, known as sheets, to reveal the identity of the secret face image.

Keywords: Visual Cryptography, Privacy Protection, Face Registration, Active Appearance Model, Private Face Image

1. INTRODUCTION

Biometrics is defined as 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 a person or to verify a claimed identity. The template data in the database is generated during enrollment and is often stored along with the original raw data. In some instances, this data may have to be transmitted across a network. This has heightened the need to accord privacy to the subject by adequately protecting the contents of the database.

For privacy protection, 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] Ratha et al.[3] suggested transforming the stored biometric template using a set of different distortion parameters based on the application. Further, the distortion parameters could be changed to generate a new template if the original template data is deemed to be compromised. They also suggested storing the transformation parameters and biometric template in different database servers in order to guarantee security.

For preserving the privacy of a face, Newton et al.[4] and Gross et al.[5] introduced a face de-identification algorithm that minimized the probability of automatic face recognition while preserving details of the face such as expression, gender and age. Bitouk et al.[6] proposed a face swapping technique which protects identity by automatically substituting faces in an image with replacements taken from a large library of face images. However, in the case of face swapping and de-identification the original face image can be lost.

In this paper, we investigate the possibility of protecting an individual's private face image by decomposing it into two independent public host images, such that the original face image can be reconstructed only when both the public images are available. The public images hosting the private face image are referred to as sheets. In this scenario, the private image can be viewed as being encrypted using two public face images as shown in Figure 1. The two public face images can then be stored independently in different on-line servers such that the identity of the private image is not revealed to either server. When the private face image has to be matched,

Arun Ross: arun.ross@mail.wvu.edu
Asem Othman: asem.othman@mail.wvu.edu (contact author)
This project was funded by US National Science Foundation CAREER Grant No. IIS 0642554

the two public images can be retrieved and overlaid (i.e., superimposed) in order to reconstruct the original face image. We demonstrate that the reconstructed face image can be successfully used in the matching stage of a biometric system. Further, we show that different pairs of public images can be used to encrypt different samples of the same face.

Additionally, the proposed approach addresses the following template protection requirements:[7–9]
Diversity and Revocability: Different applications can employ different public datasets for host image selection. Therefore, the hosts selected for encrypting a private face image can differ across applications. Consecutively, cross-matching across databases will not be feasible. Moreover, it is straightforward to revoke the stored sheets and reissue new sheets for a private face image by changing the hosts.
Security and Performance: It is computationally hard to obtain the original face image from the individual stored sheets due to the use of visual cryptography which will be explained in detail in the following section. Furthermore, as will be shown in the experiments section, the recognition performance is not degraded when the private face image is reconstructed from the component sheets.

The rest of the paper is organized as follows. In Section 2 a basic introduction to visual cryptography and its extensions are presented. Section 3 discusses the proposed approach. Section 4 reports the experimental results and section 5 concludes the paper.

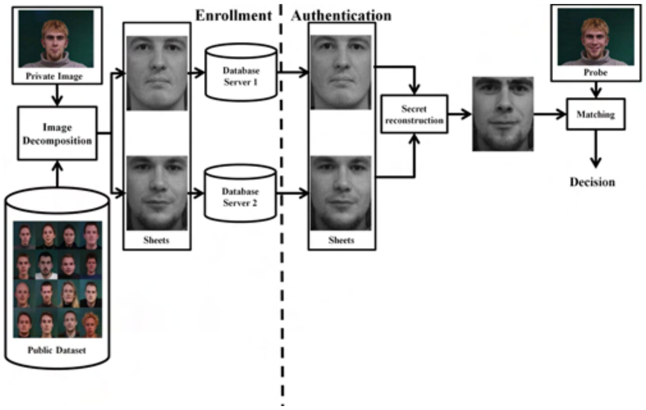


Figure 1. Illustration for the proposed approach

2. VISUAL CRYPTOGRAPHY

One of the best known techniques to protect data such as biometric templates[10, 11] 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[12] introduced the Visual Cryptography Scheme (VCS) as a simple and secure way to allow the secret sharing of images without any cryptographic computations. It is a cryptographic technique that allows the encryption of visual information such that decryption can be performed using the human visual system. We utilize this scheme in our approach. The basic scheme is referred to as the k-out-of-n visual cryptography scheme which is denoted as (k, n) VCS.[12] Given an original binary image T, it is encrypted in n images, such that:

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

where $\oplus$ is a boolean operation, S_{h_i} , $h_i \in 1, 2, ..., k$ 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.[12] 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 as two sub-pixels called shares. Figure 2 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 sub-pixels; if it is a white pixel, we get one black sub-pixel and one white sub-pixel. Therefore, the reconstructed image will be twice the width of the original secret image and there will be a 50% loss in contrast.[12] However, the original image will be visible.

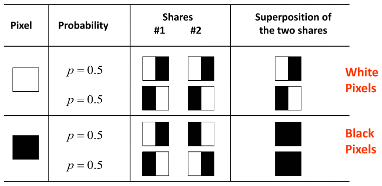


Figure 2. Illustration of a 2-out-of-2 VCS scheme with 2 sub-pixels construction

In 2002, Nakajima and Yamaguchi[13] presented a 2-out-of-2 Extended Visual Cryptography Scheme for natural images. They suggested a theoretical framework for encoding a natural image in innocuous images as illustrated in Figure 3. This is known as the Gray-level Extended Visual Cryptography Scheme (GEVCS).

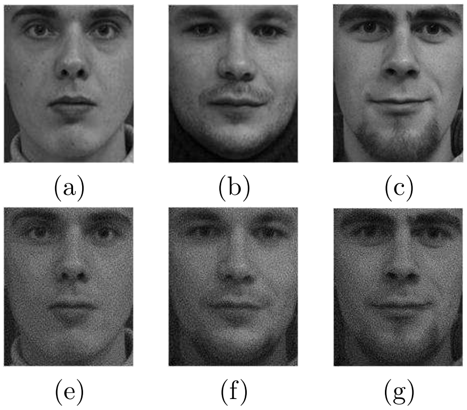


Figure 3. Encryption of a private face image in two public face images. (a) and (b) are two public images. (c) is a private face image. (e) and (f) are the public images after visual encryption. (g) is the result of overlaying (e) and (f)

In this work, we suggest an approach to protect the privacy of a specific face data set, known as a private data set, by encrypting its face images using face images from another set, known as a public data set. Each private face image will be encrypted by using two host images from the public data set via the GEVCS method. The basic Visual Cryptography scheme and its extension (GEVCS) are discussed in detail below.

2.1 Visual Cryptography Scheme Model

There are a few basic definitions which need to be explained before we formally define 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 face image.
(2) **Hosts ($H's$):** These are the images which will be used to encrypt the secret image using the Gray-level Extended Visual Cryptography Scheme (GEVCS). In our application, these correspond to the face images in the public data set.
(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 image (in the case of GEVCS).

(4) **Target (T):** The image reconstructed by stacking or superimposing the sheets.
(5) **Sub-pixel:** Each pixel P is divided into a certain number of sub-pixels during the encryption process.
(6) **Pixel Expansion (m):** It is the number of sub-pixels 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 sub-pixels. These collections of sub-pixels are known as shares.
(8) **Relative Contrast (α):** It is 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 Visual Cryptography Scheme deals with the secret message as an image consisting of independent white and black pixels. Each pixel is reproduced as n shares with each share consisting of m sub-pixels. 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 j^{th} sub-pixel in the i^{th} 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 output of a visual cryptography scheme 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 sub-pixels 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 target image is still visible. In addition, the m sub-pixels 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 Figure 4. 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:

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

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

This 2-out-of-2 visual cryptography scheme 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, we randomly pick the same pattern of four pixels for both shares which is equivalent to randomly selecting a boolean matrix B from the collection C_0. If the pixel of the original image is black, we randomly pick a complementary pair of patterns or select a boolean matrix B from the collection C_1. Condition (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 values.

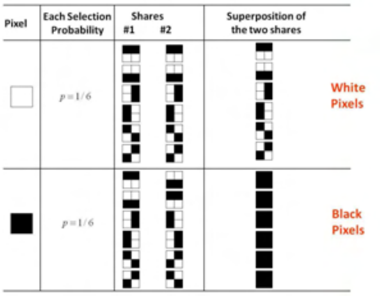


Figure 4. Illustration of a 2-out-of-2 scheme with 4 sub-pixel construction

2.2 Gray-level Extended Visual Cryptography Scheme (GEVCS)

VCS allows us to encode a secret image into n sheet images (i.e., host 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.[12] Ateniese et al.[14] introduced such a framework known as the Extended Visual Cryptography scheme. Nakajima and Yamaguchi[13] proposed a theoretical framework to apply Extended Visual Cryptography on gray level images (GEVCS) and also introduced a method to enhance the contrast of the target images. Moreover, they extended their work to increase the number of sub-pixels for each share resulting in an increase in the number of gray levels.

The Gray-level Extended Visual Cryptography Scheme (GEVCS) operates 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.

2.2.1 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.[15] 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[16] 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, the images are quantized to a number of levels equalling the number of sub-pixels per share, m. During the dithering process at the pixel level, any continuous tone pixel is expanded to a matrix of black and white sub-pixels defined by the gray level of the original pixel. The proportion of white sub-pixels in this matrix is referred to as pixel transparency.

2.2.2 Encryption

The encryption process is applied on a pixel-by-pixel basis for the three halftoned images (the two hosts and the original image). The arrangement of the sub-pixels in the shares of both the hosts has to be controlled such that the required transparency (the number of white sub-pixels) 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 sub-pixel region for share 1, share 2 and the target, respectively.

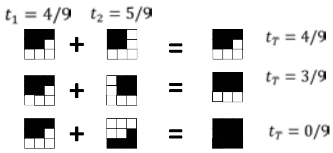


Figure 5. Examples of sub-pixel arrangement

The security of the scheme is also important. Therefore, during encryption, a Boolean matrix B is randomly selected from a set of 2 x 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 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.[13]

However, as shown in Figure 6, there are cases when the required transparency for the corresponding pixel in the target image cannot be obtained, no matter how the shared sub-pixels are rearranged. So it is essential to detect and rectify such instances. A pixel transparency can be represented as a pie chart as shown in Figure 7. The white region and shaded region correspond to the transparent and opaque sub-pixels, respectively. This figure shows that there is a specific range for the target transparency, t_T, for a given combination of share 1 and share 2 transparencies, (t_1, t_2). Therefore, to determine if it is possible to obtain the target transparency by rearranging the transparent (white) sub-pixels in the shares, the target transparency must be within the following range (condition (T1)):[13]

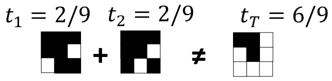
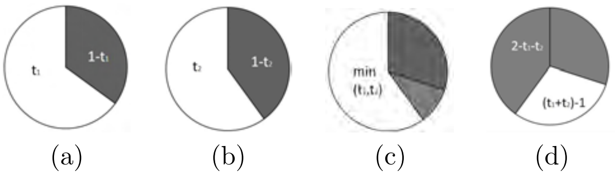


Figure 6. Example of impossible arrangements

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

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 target, respectively. The range of each of these transparencies for the entire image corresponds to the dynamic range of the pixel intensities of the 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):[13]

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



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

Figure 7. The range of target transparency, t_T, for a given t_1 and t_2. (a) The transparent area in share 1. (b) The transparent area in share 2. (c) and (d) The maximum and minimum areas, respectively, that can be achieved by stacking the shares. Adapted from Nakajima and Yamaguchi[13]

Nakajima and Yamaguchi[13] 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.[13] 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 $3D$-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 (Figure 5) 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, we will replace p' 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 Figure 8.

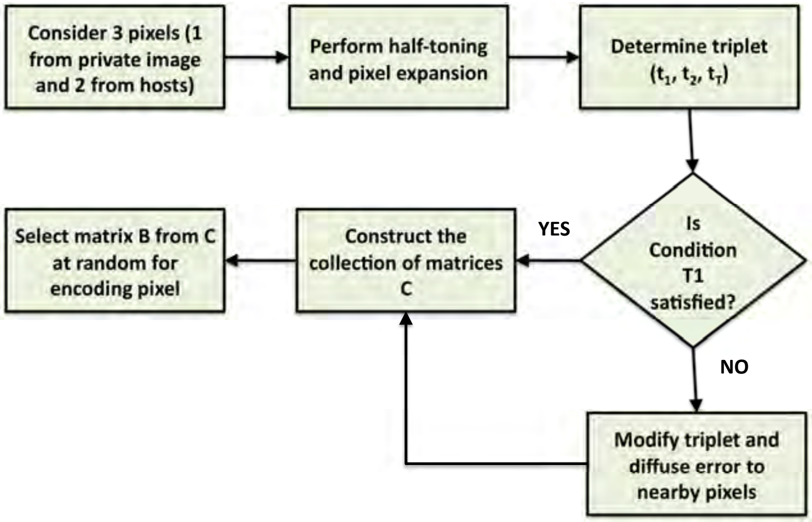

Consider 3 pixels (1 from private image and 2 from hosts)
Perform half-toning and pixel expansion
Determine triplet (t_1, t_2, t_T)
Is Condition T1 satisfied?
YES
NO
Construct the collection of matrices C
Select matrix B from C at random for encoding pixel
Modify triplet and diffuse error to nearby pixels

Figure 8. Flowchart for illustrating GEVCS at the pixel-level

Note that if there are several violated triplets, it may cause a part of the target information to appear on the sheets and the proposed extended visual cryptography scheme will not be perfectly secure.[13,17] Therefore, the Constraint Fulfillment Rate (CFR) - which is defined as the ratio of triplets which satisfy condition (T1) to the triplets in the entire image - is used to determine the effect of the target image on the sheets. Nakajima and Yamaguchi[13] found that when the CFR is below 0.6, such target violations could be perceived by the human visual system.

3. THE PROPOSED APPROACH

In this work, we attempt to secure a face image in a private dataset by using GEVCS to decompose it into two different face images taken from a public dataset. Let $\mathbf{P} = \mathbf{H_1}, \mathbf{H_2}, \ldots, \mathbf{H_N}$ 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 $\mathbf{P}$. 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 target image on the sheet images and vice versa can become perceptible. This issue can be mitigated if the host images for a particular private image are carefully chosen. Figure 9 shows the block diagram that illustrates the key steps of our approach. These steps will be explained in more detail in the following sections.

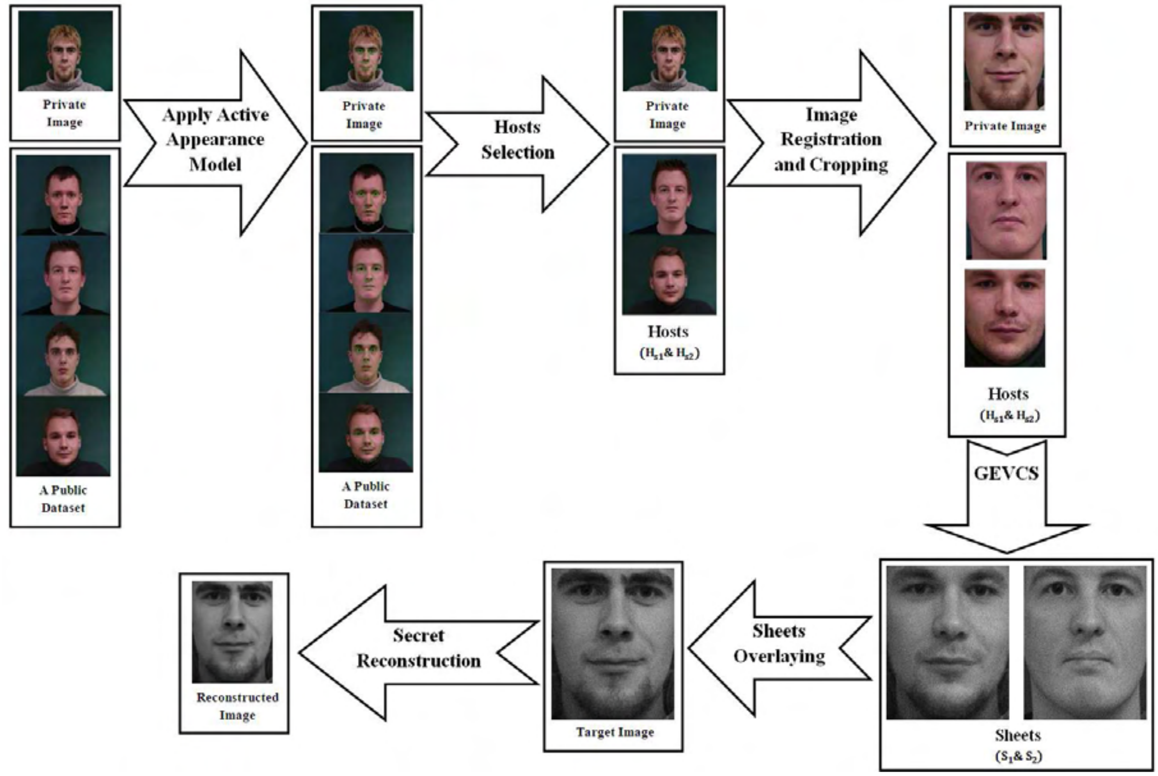


Figure 9. Block diagram of the proposed approach

3.1 Active Appearance Model

Our approach essentially selects host images that are most likely to be compatible with the private image based on geometry and appearance. Therefore, the Active Appearance Model (AAM)[18] that characterizes the shape and texture of the face is used to determine the similarity between the private face image and candidate host images (Figure 9). The steps for building the AAM and using it for detecting and annotating landmarks on face features is discussed in detail in Stegmann's work.[19]

3.2 Selection of Hosts

For selecting compatible hosts, the cost of registering (aligning) each public face image with the private image is computed and sorted in order to locate two public face images, H_{s1} and H_{s2}, with the minimum registration cost. The cost F_c of each registration is the weighted sum of the transformation cost T_c and the appearance cost A_c.

3.2.1 Transformation Cost T_c

This cost measures the amount of geometric transformation necessary to align the two images based on the annotated set of points 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, we use the thin plate spline (TPS) model which has been widely used as a non-rigid transformation model for image alignment and shape matching.[20] 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.

3.2.2 Appearance Cost A_c

The annotated set of points pertaining to the face feature of the original image (O) and that of the host image (H) are normalized by warping them to a mean shape resulting in transformed images O' and H'. Next, O' and H' are projected onto a texture space using the Principal Component Analysis (PCA) technique resulting in a set of weights that denotes the feature vector of an image. The appearance cost, A_c, is defined as the Manhattan distance between the vectors corresponding to O' and H'.

3.3 Image Registration and Cropping

In this step, the global affine transformation component of the thin plate spline model[20] is used to align the two selected host images (H_{s1} ,H_{s2}) with the secret image (O) and the annotated points are used to crop the face images.

3.4 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.

4. EXPERIMENTS AND RESULTS

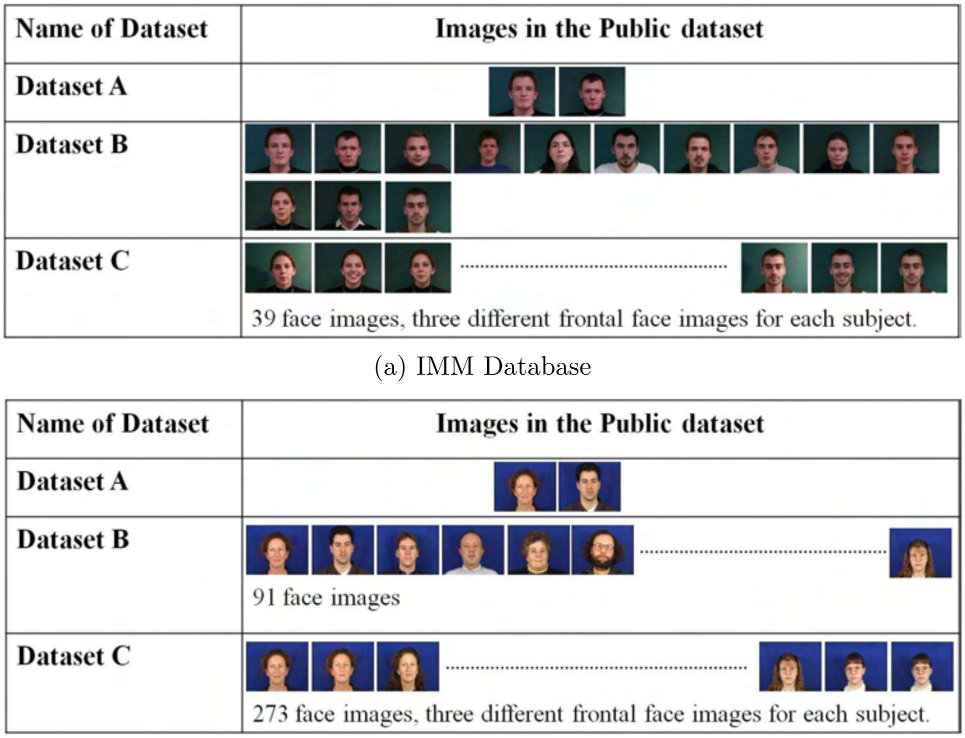
The performance of the proposed approach was tested on two different databases. The first database is the IMM Face Database[21] which is an annotated database containing 6 face images each of 40 different subjects; 3 of the frontal face images per subject were used in our experiments. 27 subjects were used to construct the private dataset and the remaining 13 were placed in the public dataset. The second database is the XM2VTS frontal image database.[22] It consists of 8 frontal face images each of 295 subjects. For our experiments, we selected 192 subjects to construct the private dataset and 91 subjects to construct the pubic datasets. 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 Figure 10. Figure 11 shows examples of the proposed approach when dataset B in Figure 10 is used as the public dataset (here $[L = 0, K = 0.75]$ and the pixel expansion value m is 36).

In the following experiments, the match scores were generated using the Verilook SDK*. In order to establish a baseline, the images in the private database were first matched against each other. This resulted in an EER (Equal Error Rate) of $\sim$ 6% for the IMM database and an EER of $\sim$ 2% for the XM2VTS database.

4.1 Experiment 1

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, we used the public dataset A in Figure 10 consisting of two fixed face images as hosts. For each subject in the private dataset, one frontal face image with neutral expression and diffuse light was selected as the secret image to be encrypted by the two public face images. The visual cryptography scheme 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 ~ 0 % in the case of the IMM database and 0.5 % in the case of the XM2VTS database.

*http://www.neurotechnology.com



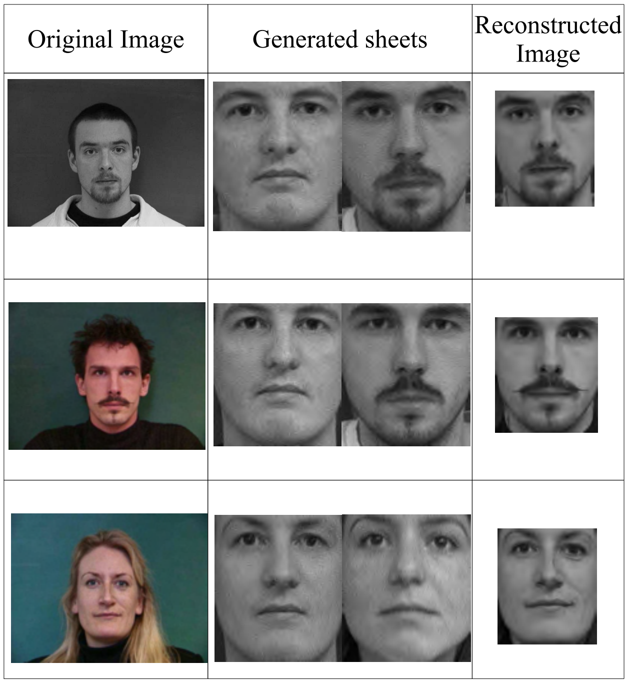
Name of Dataset	Images in the Public dataset
Dataset A	
Dataset B	
Dataset C	.... 39 face images, three different frontal face images for each subject.

(a) IMM Database

Name of Dataset	Images in the Public dataset
Dataset A	
Dataset B	.... 91 face images
Dataset C	.... 273 face images, three different frontal face images for each subject.

(b) XM2VTS Database

Figure 10. Images in the public datasets for both the IMM and XM2VTS databases



Original Image	Generated sheets	Reconstructed Image

Figure 11. Illustration of the proposed approach using images from the IMM Database

4.2 Experiment 2

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 1. To establish this, for each subject in the reconstructed dataset, N frontal face images were randomly chosen from the private database to assemble a gallery database ($N = 2$ for IMM and $N = 3$ for XM2VTS). The matching experiment consisted of comparing the reconstructed faces against these gallery images. An EER of $\sim$ 2% was obtained for the IMM database. This performance is 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 and the 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 comparing the original images only.

4.3 Experiment 3

In this experiment, we investigated the possibility of exposing the identity of the secret image by using the sheet images in the matching process. For this experiment, we computed the sheet images for 3 different face samples of the same subject. Next, the reconstructed images and the corresponding sheets are independently used in the matching process (e.g., sheet image 1 of all the private images are matched against each other; a similar matching process is conducted for sheet 2 and the reconstructed images). Figure 12 shows that each subject in the private dataset has three reconstructed images. The public datasets used in this experiments were datasets A, B and C. This experiment resulted in three ROC curves: the first is a result of using the reconstructed target images for matching, the second and the third curves are a result of using the first sheets and second sheets, respectively, for matching. As shown in Figure 13, the last two curves in each graph confirm the difficulty of exposing the identity of the secret face image by using the sheets alone. Notice that when we used the reconstructed images for matching ($m = 36$ and $K = 0.875$), the resulting performance was approximately the same as that of using the original images (Figure 13).

Note that experiment 3 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 Figure 12 where the selected host images (sheets) and the secret image are observed to have compatible expressions.

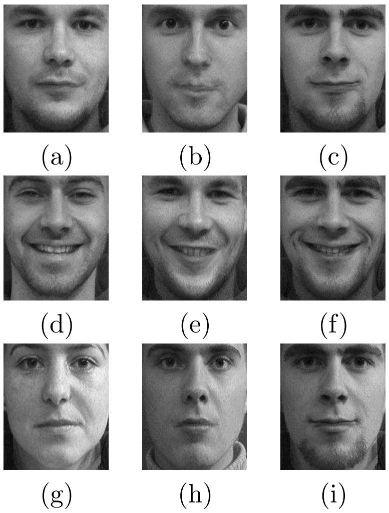
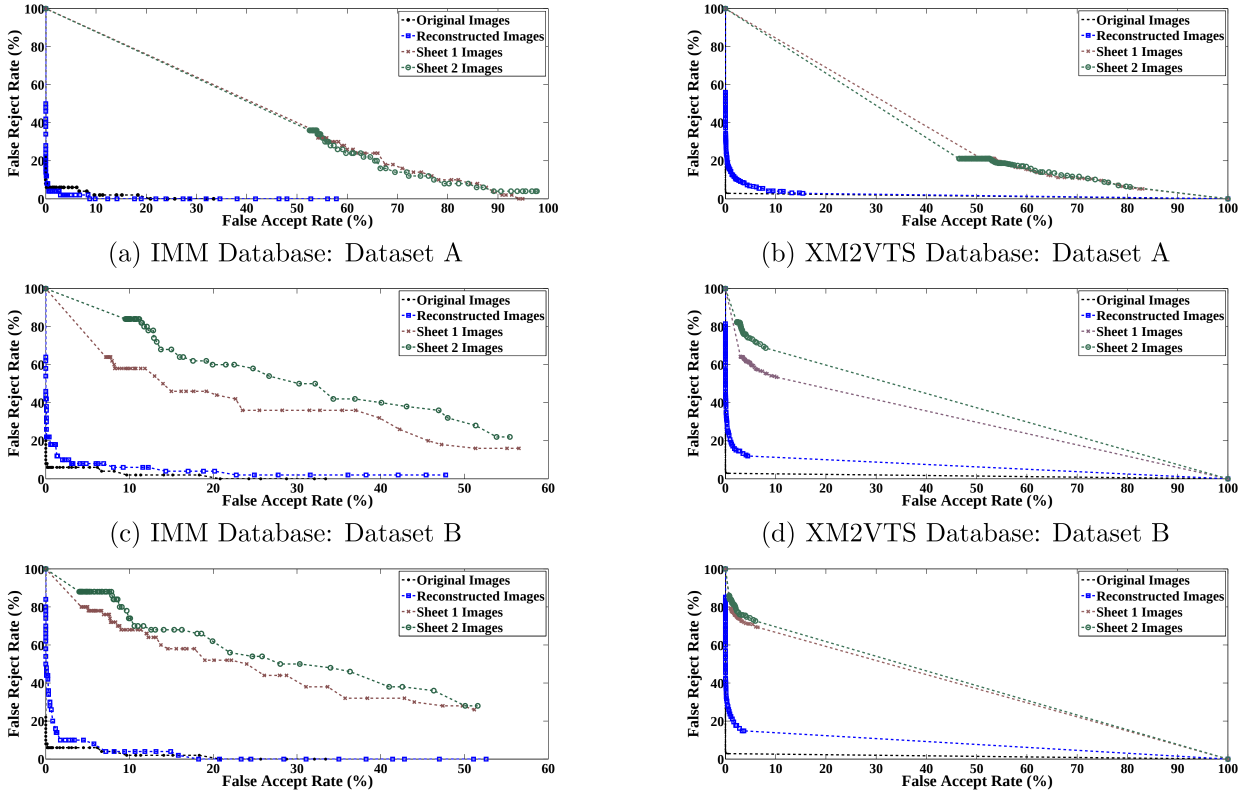


Figure 12. Examples from experiment 3 where (a), (d) and (g) are the first sheets and (b), (e) and (h) are the second sheets. (c), (f) and (i) are the corresponding reconstructed face images

5. CONCLUSION AND DISCUSSION

The contribution of this work is a novel approach to protect the privacy of face images dataset by decomposing an input private face image into two independent public face images such that the original face image can be



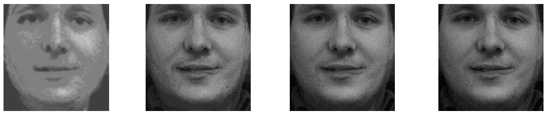
(a) IMM Database: Dataset A (b) XM2VTS Database: Dataset A

(c) IMM Database: Dataset B (d) XM2VTS Database: Dataset B

(e) IMM Database: Dataset C (f) XM2VTS Database: Dataset C

Figure 13. ROC curves for the different public datasets used in experiment 3. Experiments confirm that the sheet images cannot be used to reveal the secret image

reconstructed only when both the public images are available. The proposed algorithm first 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 hide the secret image in the selected host images. Two face databases were used to evaluate the proposed approach. Indeed, it is observed that the reconstructed images are similar to the original secret image with $m = 36$, $K = 0.875$ and a public dataset consisting of only two host face images. We investigated the effect of various parameters (K and m) on matching performance. Sheet images could be created with different contrast values, K. The performance is improved with $K = 0.875$ 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. The effect of pixel expansion, m, on the final reconstructed image was also tested. This parameter affects the number of gray-levels in the reconstructed image, and this impacts the amount of detail appearing in it. Figure 14 suggests that arbitrarily increasing m may increase the effect of the sheets on the final image. Finally, our experimental results demonstrate the difficulty of exposing the identity of the secret image by using only one of the sheets in the matching process.



(a) m=4 (b) m=16 (e) m=36 (f) m=100

Figure 14. Examples of the reconstructed image with different values for the pixel expansion factor, m

We intend to improve our host selection technique in order to build a system that could protect the privacy of faces in a larger database consisting of different pose, lighting , facial expressions and image resolution. In their face swapping process, Bitouk et al.[6] introduced a method to blend candidate faces in the original photograph. We plan to extend our work to encrypt the background of the face images as well. This would allow GEVCS to reconstruct the whole face image in the context of the original background.

REFERENCES

[1] A. Jain, P. Flynn, and A. Ross, *Handbook of Biometrics*, Springer, 2007.

[2] G. I. Davida, Y. Frankel, and B. J. Matt, "On enabling secure applications through off-line biometricidentification," in *IEEE Symposium on Security and Privacy*, pp. 148–157, 1998.

[3] N. Ratha, J. Connell, and R. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Systems Journal* **40**(3), pp. 614–634, 2001.

[4] E. Newton, L. Sweeney, and B. Malin, "Preserving privacy by de-identifying face images," *IEEE Transactions on Knowledge and Data Engineering* , pp. 232–243, 2005.

[5] R. Gross, L. Sweeney, F. De la Torre, and S. Baker, "Model-based face de-identification," in *IEEE Workshop on Privacy Research in Vision*, 2006.

[6] D. Bitouk, N. Kumar, S. Dhillon, P. Belhumeur, and S. Nayar, "Face swapping: automatically replacing faces in photographs," *ACM Transactions on Graphics* , August 2008.

[7] D. Maltoni, D. Maio, A. Jain, and S. Prabhakar, *Handbook of fingerprint recognition*, Springer-Verlag New York, Inc. Secaucus, NJ, USA, 2003.

[8] A. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP Journal on Advances in Signal Processing* , pp. 1–17, 2008.

[9] S. Prabhakar, S. Pankanti, and A. Jain, "Biometric recognition: Security and privacy concerns," *IEEE Security & Privacy* **1**, pp. 33–42, March-April 2003.

[10] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, and B. Kumar, "Biometric encryption using image processing," in *Proceedings of SPIE*, **3314**, pp. 178–188, 1998.

[11] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, and B. Kumar, "Biometric encryption," *ICSA Guide to Cryptography* , 1999.

[12] M. Naor and A. Shamir, "Visual cryptography," in *EUROCRYPT*, pp. 1–12, 1994.

[13] M. Nakajima and Y. Yamaguchi, "Extended visual cryptography for natural images," *Journal of WSCG* **10**(2), pp. 303–310, 2002.

[14] G. Ateniese, C. Blundo, A. Santis, and D. Stinson, "Extended capabilities for visual cryptography," *Theoretical Computer Science* **250**(1-2), pp. 143–161, 2001.

[15] S. Shevell, *The science of color*, Elsevier Science Ltd., 2003.

[16] R. Floyd and L. Steinberg, "An adaptive algorithm for spatial greyscale," *SPIE Milestone Series* **154**, pp. 281–283, 1999.

[17] M. Nakajima and Y. Yamaguchi, "Enhancing registration tolerance of extended visual cryptography for natural images," *Journal of Electronic Imaging* **13**, pp. 654–662, 2004.

[18] T. Cootes, G. Edwards, C. Taylor, *et al.*, "Active appearance models," *IEEE Transactions on Pattern Analysis and Machine Intelligence* **23**(6), pp. 681–685, 2001.

[19] M. B. Stegmann, "Active appearance models: Theory, extensions and cases," Master's Thesis, Informatics and Mathematical Modelling, Technical University of Denmark, DTU, August 2000.

[20] F. Bookstein, "Principal warps: Thin-plate splines and the decomposition of deformations," *IEEE Transactions on Pattern Analysis and Machine Intelligence* **11**(6), pp. 567–585, 1989.

[21] M. B. Stegmann, B. K. Ersbøll, and R. Larsen, "FAME – a flexible appearance modelling environment," *IEEE Trans. on Medical Imaging* **22**(10), pp. 1319–1331, 2003.

[22] K. Messer, J. Matas, J. Kittler, J. Luettin, and G. Maitre, "XM2VTSDB: The extended M2VTS database," in *Second International Conference on Audio and Video-based Biometric Person Authentication*, **964**, pp. 965–966, 1999.